Optimal Control of Mobile Malware Epidemics

MHR. Khouzani

University of Pennsylvania, khouzani@seas.upenn.edu

Follow this and additional works at: http://repository.upenn.edu/edissertations

Recommended Citation
http://repository.upenn.edu/edissertations/444

This paper is posted at ScholarlyCommons. http://repository.upenn.edu/edissertations/444
For more information, please contact libraryrepository@pobox.upenn.edu.
Optimal Control of Mobile Malware Epidemics

Abstract
Malware attacks constitute a serious security risk that threatens our ever-expanding wireless networks. Developing reliable security measures against outbreaks of malware facilitate the proliferation of wireless technologies.

The first step toward this goal is to investigate potential attack strategies and the extent of damage they can incur. Given the flexibility that software-based operation provides, it is reasonable to expect that new malware will not demonstrate a fixed behavior over time. Instead, malware can dynamically change the parameters of their infective hosts in response to the dynamics of the network, in order to maximize their overall damage.

We first consider propagation of malware in a battery-constrained mobile wireless network by an epidemic model in which the worm can dynamically control the transmission ranges and/or the media scanning rates of the infective nodes. The malware at each infective node may seek to contact more susceptible nodes by amplifying the transmission range and the media scanning rate and thereby accelerate its spread. This may however lead to (a) easier detection of the malware and thus more effective counter-measure by the network, and (b) faster depletion of the battery which may in turn thwart further spread of the infection and/or exploitation of that node. We prove, using Pontryagin Maximum Principle from optimal control theory, that the maximum damage in this case can be attained using simple three-phase strategies: in the first phase, infective nodes use maximum transmission ranges and media access rates to amass infective nodes. In the next phase, infective nodes reduce their access attempts and enter a stealth-mode to preserve their battery and hide from detection. In the last phase, they once again use maximum transmission attempts with largest rates but this time the primary effect is killing the infective nodes by draining their batteries.

In an alternative attack scenario, we consider the case in which the malware can control the rate of killing the infective nodes as an independent parameter of control. At each moment of time the worm at each node faces the following decisions: (i) choosing the transmission ranges and media scanning rates so as to maximize the spread of infection subject to not exhausting its batteries by the end of the operation interval; and (ii) whether to kill the node to inflict a large cost on the network, however at the expense of losing the chance of infecting more susceptible nodes at later times. We establish structural properties of the optimal strategy of the attacker over time. Specifically, we prove that it is optimal for the attacker to defer killing of the infective nodes in the propagation phase until reaching a certain time and then start the slaughter with maximum effort. We also show that in the optimal attack policy, the battery resources are used according to a decreasing function of time, i.e., most aggressively during the initial phase of the outbreak.

Upon detection of a malware outbreak, the network manager can counter the propagation of the malware by reducing the communication rates of the nodes and patching. We in turn investigate the optimal defense policies of rate reduction and patching.

We introduce quarantining the malware by reducing the reception gain of nodes as a defense mechanism. In applying this counter-measure we confront a trade-off: reducing the communication range suppresses the spread of the malware, however, it also deteriorates the network performance by introducing delay. Using Pontryagin’s Maximum Principle, we derive structural characteristics of the optimal communication range as a function of time for a wide class of cost functions. In both of the defense controls, our numerical computations reveal that the dynamic optimal controls significantly outperform static choices and is also robust to errors in estimation of the network and attack parameters.

This dissertation is available at ScholarlyCommons: http://repository.upenn.edu/edissertations/444
The distribution of patches consumes bandwidth which is specially scarce in wireless networks, and must therefore be judiciously controlled in order to attain desired trade-offs between security risks and bandwidth consumption. We consider both non-replicative and replicative dissemination of patches: a pre-determined set of dispatcher nodes distribute the patches in the former, whereas the dispatcher set continually grows in the latter as the nodes that receive the patch become dispatchers themselves. In each case, the desired trade-offs can be attained by activating at any given time only fractions of dispatchers and selecting their packet transmission rates. We formulate the above trade-offs as optimal control problems that seek to minimize the aggregate network costs that depend on security risks and the overall extra energy and bandwidth used in the network for dissemination of the security patches. We prove that the dynamic control strategies have simple structures: when the cost function associated with the energy/bandwidth consumed in patching is concave, the control strategies are bang-bang with at most one jump from the maximum to the minimum value, i.e., maximum patching rates until a certain threshold and then stop. When the cost function is strictly convex, the above transition is strict but continuous. We compare the efficacy of different dispatch models and also those of the optimum dynamic and static controls using numerical computations.

Next, we consider the case in which both malware and network can dynamically vary their parameters over time in response to the changes of the state of the system and also to each other’s controls. The infinite dimension of freedom introduced by variation over time and antagonistic and strategic optimization of malware and network against each other demand new attempts for modeling and analysis. We develop a zero-sum dynamic game model and investigate the structural properties of the saddle-point strategies. We specifically show that saddle-point strategies are still simple threshold-based policies and hence, a robust dynamic defense is practicable. Finally, we develop a unified mathematical framework for calculating optimal controls of systems governed by epidemic evolution using Pontryagin’s Maximum Principle, and we demonstrate how it can be applied to contexts beyond network security. Specifically, we show how our framework can be specialized for marketing, dissemination of messages in DTN or p2p networks, health-care, etc. This dissertation in part demonstrates how using simple real analysis arguments, one can extract substantial information about the structure of optimal policies for nonlinear systems in the absence a closed-form solution.

**Degree Type**
Dissertation

**Degree Name**
Doctor of Philosophy (PhD)

**Graduate Group**
Electrical & Systems Engineering

**First Advisor**
Saswati Sarkar

**Keywords**
Optimal Control, Dynamic Games, Mean Field, Delay Tolerant Networks, Worms, Security, Wireless, Mobile Networks

This dissertation is available at ScholarlyCommons: [http://repository.upenn.edu/edissertations/444](http://repository.upenn.edu/edissertations/444)
OPTIMAL CONTROL OF MOBILE MALWARE EPIDEMICS

MHR. Khouzani

A DISSERTATION
in
Electrical and Systems Engineering

Presented to the Faculties of the University of Pennsylvania
in
Partial Fulfillment of the Requirements for the
Degree of Doctor of Philosophy

2011

Saswati Sarkar
Supervisor of Dissertation

Roch Guérin
Graduate Group Chairperson

DISSERTATION COMMITTEE
Roch Guérin, Professor, ESE, UPenn
Ali Jadbabaie, Professor, ESE, UPenn
Tara Javidi, Associate Professor, ECE, UCSD
Tamer Başar, Professor, ECE, UIUC
Dedication

I dedicate this work to all the people who have the courage to be unselfish.

Because as Bertolt Brecht puts it, “It is the simple, which is so difficult”.
Acknowledgments

This piece of work could not have come into existence without the continuous support of my advisor, Professor Saswati Sarkar. I immensely value her unremitting guidance and her sound advice, which are imprinted throughout this work. I will be indefinitely indebted to her – even if only for the fact that she graciously tried to foster in me the skill of critical thinking and analytical integrity.

I would like to also thank my dissertation committee: Professor Jadabaie, Professor Guerin, Professor Javidi and Professor Başar for their support and their insightful guidance. Special thanks to Professor Eitan Altman as he sparked the direction that became this thesis, and intellectually encouraged me throughout the journey.

I wish to express my most heartfelt appreciation to my parents, Effat and Jaffar, and my brother, Arash, who enriched me the art of magnanimous love and meaningful living.
ABSTRACT

OPTIMAL CONTROL OF MOBILE MALWARE EPIDEMICS

MHR. Khouzani
Saswati Sarkar, Advisor

Malware attacks constitute a serious security risk that threatens our ever-expanding wireless networks. Developing reliable security measures against outbreaks of malware facilitate the proliferation of wireless technologies. The first step toward this goal is to investigate potential attack strategies and the extent of damage they can incur. Given the flexibility that software-based operation provides, it is reasonable to expect that new malware will not demonstrate a fixed behavior over time. Instead, malware can dynamically change the parameters of their infective hosts in response to the dynamics of the network, in order to maximize their overall damage.

We first consider propagation of malware in a battery-constrained mobile wireless network by an epidemic model in which the worm can dynamically control the transmission ranges and/or the media scanning rates of the infective nodes. The malware at each infective node may seek to contact more susceptible nodes by amplifying the transmission range and the media scanning rate and thereby accelerate its spread. This may however lead to (a) easier detection of the malware and thus more effective counter-measure by the network, and (b) faster depletion of the battery which may in turn thwart further spread of the infection and/or exploitation of that node. We prove, using Pontryagin Maximum Principle from optimal control theory, that the maximum damage in this case can be attained using simple three-phase strategies: in the first phase, infective nodes use maximum transmission ranges and media access rates to amass infective nodes. In the next phase, infective nodes reduce their access attempts and enter a stealth-mode to preserve their battery and hide from detection. In the last phase, they once again use maximum transmission attempts with largest rates but this time the primary effect is killing the infective
nodes by draining their batteries.

In an alternative attack scenario, we consider the case in which the malware can control the rate of killing the infective nodes as an independent parameter of control. At each moment of time the worm at each node faces the following decisions: (i) choosing the transmission ranges and media scanning rates so as to maximize the spread of infection subject to not exhausting its batteries by the end of the operation interval; and (ii) whether to kill the node to inflict a large cost on the network, however at the expense of losing the chance of infecting more susceptible nodes at later times. We establish structural properties of the optimal strategy of the attacker over time. Specifically, we prove that it is optimal for the attacker to defer killing of the infective nodes in the propagation phase until reaching a certain time and then start the slaughter with maximum effort. We also show that in the optimal attack policy, the battery resources are used according to a decreasing function of time, i.e., most aggressively during the initial phase of the outbreak.

Upon detection of a malware outbreak, the network manager can counter the propagation of the malware by reducing the communication rates of the nodes and patching. We in turn investigate the optimal defense policies of rate reduction and patching.

We introduce quarantining the malware by reducing the reception gain of nodes as a defense mechanism. In applying this counter-measure we confront a trade-off: reducing the communication range suppresses the spread of the malware, however, it also deteriorates the network performance by introducing delay. Using Pontryagin’s Maximum Principle, we derive structural characteristics of the optimal communication range as a function of time for a wide class of cost functions. In both of the defense controls, our numerical computations reveal that the dynamic optimal controls significantly outperforms static choices and is also robust to errors in estimation of the network and attack parameters.

The distribution of patches consumes bandwidth which is specially scarce in wireless networks, and must therefore be judiciously controlled in order to attain desired trade-offs between
security risks and bandwidth consumption. We consider both non-replicative and replicative dissemination of patches: a pre-determined set of dispatcher nodes distribute the patches in the former, whereas the dispatcher set continually grows in the latter as the nodes that receive the patch become dispatchers themselves. In each case, the desired trade-offs can be attained by activating at any given time only fractions of dispatchers and selecting their packet transmission rates. We formulate the above trade-offs as optimal control problems that seek to minimize the aggregate network costs that depend on security risks and the overall extra energy and bandwidth used in the network for dissemination of the security patches. We prove that the dynamic control strategies have simple structures: when the cost function associated with the energy/bandwidth consumed in patching is concave, the control strategies are bang-bang with at most one jump from the maximum to the minimum value, i.e., maximum patching rates until a certain threshold and then stop. When the cost function is strictly convex, the above transition is strict but continuous. We compare the efficacy of different dispatch models and also those of the optimum dynamic and static controls using numerical computations.

Next, we consider the case in which both malware and network can dynamically vary their parameters over time in response to the changes of the state of the system and also to each other’s controls. The infinite dimension of freedom introduced by variation over time and antagonistic and strategic optimization of malware and network against each other demand new attempts for modeling and analysis. We develop a zero-sum dynamic game model and investigate the structural properties of the saddle-point strategies. We specifically show that saddle-point strategies are still simple threshold-based policies and hence, a robust dynamic defense is practicable.

Finally, we develop a unified mathematical framework for calculating optimal controls of systems governed by epidemic evolution using Pontryagin’s Maximum Principle, and we demonstrate how it can be applied to contexts beyond network security. Specifically, we show how our framework can be specialized for marketing, dissemination of messages in DTN or p2p networks, health-care, etc. This dissertation in part demonstrates how using simple real analysis
arguments, one can extract substantial information about the structure of optimal policies for nonlinear systems in the absence a closed-form solution.
Contents

1 Overview .................................................. 1
   1.1 Motivation ........................................... 1
   1.2 System state evolution ............................... 3
   1.3 Decision problems of the attackers ............... 4
   1.4 Decision problems of the defense ................. 5
   1.5 Summary of the contributions ....................... 7
       1.5.1 Formulation of maximum damage attack ....... 7
       1.5.2 Formulation of the maximum efficacy countermeasure .... 9
       1.5.3 Dynamic game of defense v.s. attack .......... 10
       1.5.4 A unified framework and further applications ... 11
   1.6 Related literature .................................... 11

2 Notations and Assumptions ............................... 16

I Attack .................................................. 21

3 Battery Depletion Attack ................................. 22
   3.1 System model ........................................ 23
       3.1.1 Dynamics of state evolution .................. 23
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1.2</td>
<td>Maximum damage battery depletion attack</td>
<td>26</td>
</tr>
<tr>
<td>3.2</td>
<td>Malware’s optimal control</td>
<td>28</td>
</tr>
<tr>
<td>3.3</td>
<td>Structural properties of optimum $u(t)$</td>
<td>30</td>
</tr>
<tr>
<td>3.4</td>
<td>Numerical computations</td>
<td>35</td>
</tr>
<tr>
<td>4</td>
<td>Seek and Destroy Attack</td>
<td>40</td>
</tr>
<tr>
<td>4.1</td>
<td>System model</td>
<td>41</td>
</tr>
<tr>
<td>4.1.1</td>
<td>Dynamics of state evolution</td>
<td>41</td>
</tr>
<tr>
<td>4.1.2</td>
<td>Maximum damage seek and destroy attack</td>
<td>43</td>
</tr>
<tr>
<td>4.2</td>
<td>Worm’s optimal control</td>
<td>47</td>
</tr>
<tr>
<td>4.3</td>
<td>Structure of the maximum damage attack</td>
<td>52</td>
</tr>
<tr>
<td>4.4</td>
<td>Proofs of Theorems 4.3.1 and 4.3.2</td>
<td>55</td>
</tr>
<tr>
<td>4.4.1</td>
<td>Proof of Theorem 4.3.1: optimal rate of killing</td>
<td>57</td>
</tr>
<tr>
<td>4.4.2</td>
<td>Proof of Theorem 4.3.2: optimal scanning rate/Tx range</td>
<td>60</td>
</tr>
<tr>
<td>4.5</td>
<td>Numerical computations</td>
<td>62</td>
</tr>
<tr>
<td>II</td>
<td>Defense</td>
<td>70</td>
</tr>
<tr>
<td>5</td>
<td>Rate Reduction</td>
<td>71</td>
</tr>
<tr>
<td>5.1</td>
<td>System model</td>
<td>72</td>
</tr>
<tr>
<td>5.2</td>
<td>Optimal reception gain control</td>
<td>77</td>
</tr>
<tr>
<td>5.3</td>
<td>Structural results</td>
<td>80</td>
</tr>
<tr>
<td>5.3.1</td>
<td>Concave $h(u)$:</td>
<td>80</td>
</tr>
<tr>
<td>5.3.2</td>
<td>Strictly convex $h(u)$:</td>
<td>85</td>
</tr>
<tr>
<td>5.4</td>
<td>Distribution of patches through the underlying network</td>
<td>88</td>
</tr>
<tr>
<td>5.5</td>
<td>Implementation and practical issues</td>
<td>90</td>
</tr>
<tr>
<td>5.6</td>
<td>Numerical computations</td>
<td>91</td>
</tr>
</tbody>
</table>
6  Patching

6.1 System model ................................................. 101
  6.1.1 Non-replicative dispatch ................................. 101
  6.1.2 Replicative dispatch .................................... 106
  6.1.3 Remarks ................................................. 108

6.2 Optimal non-replicative dispatch ............................... 108
  6.2.1 Numerical framework .................................... 109
  6.2.2 Structure of an optimal non-replicative dispatch ........ 110

6.3 Optimal replicative dispatch ................................ 115
  6.3.1 Numerical framework .................................... 115
  6.3.2 Structure of optimal replicative dispatch ............. 116

6.4 Implementation and practical issues ........................... 123

6.5 Numerical computations ....................................... 125

III  Game

7.1 System model ................................................. 137

7.2 Network-malware dynamic game ............................... 140
  7.2.1 Formulation ............................................. 140
  7.2.2 A framework for computation of the saddle-point strategies 143
  7.2.3 Structural properties of saddle-point defense strategy ............ 145
  7.2.4 Structure of the saddle-point attack strategy ............... 149

7.3 Performance evaluation ....................................... 151

IV  Generalization and Applications ................................. 156

8.1 Introduction ................................................. 157

8.2 System model ................................................. 160
8.2.1 Dynamics of non-replicative dispatch .......................... 160
8.2.2 Dynamics of replicative dispatch ............................... 162
8.2.3 Motivation of the models and instantiation .................... 165
8.2.4 The objective function ........................................ 165
8.3 Optimal non-replicative dispatch .................................. 168
  8.3.1 Structure of the optimal non-replicative dispatch .............. 169
  8.3.2 Proof of lemma 8.3.2 ..................................... 172
8.4 Optimal replicative dispatch ........................................ 175
  8.4.1 Structure of the optimal replicative dispatch ................. 175
  8.4.2 Proof of lemma 8.4.2 ..................................... 177

9 Summary and Future Research ......................................... 180

A Model Verification ..................................................... 184

Bibliography ............................................................. 198
List of Tables

2.1  List of notations of measures. ................................. 17

4.1  Control variables of the worm. ............................... 44
List of Figures

3.1 State transitions: $S, I, R, D$ respectively represent susceptible, infective, recovered, dead states. Here, $u(t)$ is product of the transmission range and media scanning rate of infectives at time $t$. The parameters $\beta, \rho$ and functions $B(\cdot), Q(\cdot)$ will be defined in Section 3.1.1. ................................. 26

3.2 Optimal controls and the corresponding levels of infection for different $\beta, I_0, \pi$. In figs (a) and (b), $I_0 = 0.1$, and in figs (b), (c), $\beta = 0.446$. In each, the plots that are always below 0.4 represent $I(\cdot)$. In figs (a), (b) ((c), (d), resp.) the higher infection levels are for the larger $\beta$’s ($I_0$’s, resp.). ................................. 37

3.3 Optimal controls and the corresponding levels of infection for different $\beta, \pi$ for strictly convex $Q, B$. Here, $I_0 = 0.1$. The plots that are always below 0.4 represent $I(\cdot)$. The higher infection levels are for the larger $\beta$’s. ................................. 37

3.4 Comparison of the damages for optimal dynamic and static policies for different $\beta, \pi$. Here $I_0 = 0.1$. ................................................................. 38

3.5 Comparison of the damages for optimal dynamic and static policies for different $I_0, \pi$. Here $\beta = 0.446$. ................................................................. 38

3.6 Reduction in the aggregate damage due to incorrect estimations of network parameters by the malware. The real values of the parameters are $I_0 = 0.1, \beta = 0.446$, $Q(u) = 0.0446 + qu, B(u) = 0.0446\pi + bu, q = b = 0.0223$. ................................. 39
4.1 Transitions. $S$, $I$, $R$, $D$ respectively represent fraction of the susceptible, infective, recovered and dead. $u(t)$ and $\nu(t)$ are the control parameters of the malware.

4.2 Evaluation of the optimal controllers and the according states as functions of time.

Here, $h(u) = u^2$, $\beta = 0.9$, $u_{\text{max}} = 1$, $\gamma = 0.2$, and $\pi = 0$ in left and $\pi = 1$ in right. Thus $\beta u_{\text{max}} = 0.9 > 0.4 \geq (\gamma + \pi \gamma)$. Therefore, the fast-healing regime does not hold. However, as we can see, the pattern for optimal $u$ is consistent with statement of by theorem 4.3.2 and strictly convex $h(u)$.

4.3 Jump points of optimal $\nu$ (starting time of the slaughter period) versus $\gamma$ for both $\pi = 0$ and $\pi = 1$. Note that for $\pi = 1$ and for $\gamma \geq 0.30$, malware starts killing the infectives from time zero.

4.4 The optimal $u$ (media scanning rate times the transmission rates of infectives) for different values of $\gamma$ for both $\pi = 0$ (left) and $\pi = 1$ (right).

4.5 varying $\beta$.

4.6 varying $I_0$.

4.7 varying $\gamma$.

4.8 varying $C$.

4.9 varying $\nu_{\text{max}}$.

4.11 Robustness of the dynamic attack strategy with respect to clock drifts.

4.12 System cost (malware’s damage + the cost of patching) versus $\gamma$ (rate of patching).

4.13 System cost (malware’s damage + the cost of quarantining) versus $\beta$.

5.1 $u(t)$ is the reception gain of the susceptible nodes at time $t$.

5.2 Optimal $u$, varying $K$. The $h(u)$ functions used for concave and convex cases are $0.5(1-u)$ and $(1-u)^{1.2}$, respectively. Other parameters are $u_{\text{min}} = 0.1$, $\gamma = 0.2$, $\beta = 0.4$, $R_0 = 0$ and $C = 1$. Other parameters are $u_{\text{min}} = 0.1$, $\gamma = 0.2$, $\beta = 0.4$, $R_0 = 0$ and $C = 1$. Other parameters are $u_{\text{min}} = 0.1$, $\gamma = 0.2$, $\beta = 0.4$, $R_0 = 0$ and $C = 1$.
5.3 Optimal $u$, varying $\beta$. Here, $I_0 = 0.1, K = 50$, and other parameters are as in fig. 5.2. ................................................................. 93

5.4 Optimal $u$, varying $\gamma$. Here, $I_0 = 0.1, K = 50$, and other parameters are as in fig. 5.2. ................................................................. 94

5.5 Optimal $u$, varying $C$. Here, $I_0 = 0.1, K = 50$, and other parameters are as in fig. 5.2. ................................................................. 95

5.6 An optimal $u$ with two jumps. Here, $h(u) = 1 - u, u_{\min} = 0.1, \gamma = 0.22, \beta = 0.4, I_0 = 0.05, R_0 = 0, C = 0.8$ and $K = 60$. ................................................................. 96

5.7 Cost comparison: optimum dynamic versus the static policies. The parameters are $T = 25, u_{\max} = 1, u_{\min} = 0.1 \gamma = 0.2, I_0 = 0.2, C = 5 K = 50$ and $h(u) = 1 - u$. .................................................. 97

5.8 Comparison of the costs achieved by our dynamic optimal control and a heuristic control that uses (noisy) local state information. ................................................. 97

5.9 The first two figures respectively demonstrate the robustness with respect to $\beta$ and $I_0$ respectively for $h(u) = 1 - u$. The last two figures demonstrate robustness with respect to quantization in the control for $h(u) = (1 - u)^{1.5}$. In the last figure, the $x$-axis represents the number of levels available for $u$, and the control is rounded to the level closest to the optimal value, e.g., $x = 2$ means the output is rounded to $u_{\min}$ and 1. The other parameters for all the figures are $\beta = 0.5, I_0 = 0.2, R_0 = 0, \gamma = 0.2, u_{\min} \approx 0, u_{\max} = 1, C = 10, T = 20$. .................................................. 98

6.1 The top figures represent the optimal controls and the bottom figures the corresponding system states as functions of time for non-replicative dispatch with concave $h(.)$. Here, $f(I) = 10I^2, g(D) = 20D^2, T = 100, \beta_0 = \beta_1 = 0.2, \delta = 0.005$, $I_0 = R_0 = 0.1, h(\varphi) = 10R_0\varphi$. Also, Left: $\pi = 0$, Right: $\pi = 1$. .................................................. 107
6.2 The optimal control and the corresponding system states as functions of time for non-replicative dispatch. The parameters are the same as in fig. 6.1, except that
\[ h(\vartheta) = 10(R_0 \vartheta)^2, \] hence a strictly convex function. Also, Left: \( \pi = 0 \), Right: \( \pi = 1 \).

6.3 The jump point of the bang-bang optimum control for replicative and non-replicative dispatch. Here, \( f(I) = 10I^2 \), \( g(D) = 20D^2 \), \( h(x) = K_u x \), and \( T = 100 \), \( \delta = 0.005 \), \( \beta_0 = \beta_1 = \beta \).

6.4 (Continuation of) the jump point of the bang-bang optimum control for replicative and non-replicative dispatch. Refer to fig. 6.3 for the parameters of choice.

6.5 (Continuation of) the jump point of the bang-bang optimum control for replicative and non-replicative dispatch. Refer to fig. 6.3 for the parameters of choice.

6.6 varying \( \beta \). Here, \( R_0 = 0.1 \), \( K_u = 10 \), \( \delta = 0.005 \) and \( I_0 = 0.1 \).

6.7 varying \( R_0 \). Here, \( \beta = 0.20 \), \( K_u = 10 \), \( \delta = 0.005 \) and \( I_0 = 0.1 \).

6.8 varying \( K_u \). Here, \( \beta = 0.20 \), \( R_0 = 0.1 \), \( \delta = 0.005 \) and \( I_0 = 0.1 \).

6.9 varying \( I_0 \). Here, \( \beta = 0.20 \), \( R_0 = 0.1 \), \( \delta = 0.005 \) and \( K_u = 10 \).

6.10 varying \( \delta \). Here, \( \beta = 0.20 \), \( R_0 = 0.1 \), \( K_u = 10 \), \( I_0 = 0.1 \).

6.12 Robustness of the patching with respect to clock drift. The increase in the overall cost is less than 15%.

7.13 State transitions. \( u^{N_i}(t) \) and \( u^{N_r}(t) \) are the control parameters of the network while \( u^M(t) \) is the control parameter of the malware.

7.14 State evolution and saddle-point strategies. The parameters of the game are as follows: \( \kappa_I = 10 \), \( \kappa_D = 13 \), \( \kappa_u = 10 \), \( \kappa_r = 5 \), \( K_I = K_D = 0 \), \( \beta_2 = \beta_1 = \beta_0 = 4.47 \), \( \pi = 1 \), and initial fractions \( I_0 = 0.15 \), \( R_0 = 0.1 \), \( D_0 = 0 \), and \( T = 4 \).

7.15 Saddle-point defense and attack strategies for the game considered in §7.3. Here, \( \kappa_I = 10 \), \( \kappa_D = 20 \), \( \kappa_u = 10 \), \( \kappa_r = 15 \), \( \beta_1 = \beta_0 = 0.109 \), \( \beta_2 = K_I = K_D = 0 \), and initial fractions \( I_0 = 0.1 \), \( R_0 = 0.1 \), \( D_0 = 0 \), and \( T = 4 \).
7.18 Comparison of the maximum damage for the best static choice of defense parameters and dynamic saddle-point defense strategies. ................................................................. 155

8.19 State transitions for non-replicative case. The only difference in the replicative case is that transition rates from $S$ to $R$ is at rate $\beta_1 \varepsilon u RS$ and from $I$ to $R$ at rate $\pi \beta_1 \varepsilon u RI$ instead. ................................................................. 162

A.1 The top two figures compare the simulated (averaged over 100 runs) and the calculated (from the epidemic model) state trajectories for a network of $N = 500$ nodes, and the bottom two figures compare the simulated and calculated damages for different values of $N$. The inter-contact times are exponentially distributed. In all the figures the dashed and the solid lines respectively represent the calculated values and the simulation results. The error-bars represent the standard deviations. The dashed and solid lines mostly overlap, and the deviations diminish as $N$ increases. 190

A.2 Comparison of the simulated (averaged over 100 runs) damages and calculated (from the epidemic model) damages under power-law distributed inter-contact times for different value of $I_0$. ................................................................. 191

A.3 Simulated and calculated trajectories of the states for a network of 41 nodes with exponential inter-contact times. The solid lines represent the trajectories obtained from the epidemic model (calculated trajectories), and the dashed lines are the averages of the trajectories over 100 simulation runs. ................................................................. 192

A.4 Comparison of the simulated and calculated costs for a network of 41 nodes with exponentially distributed inter-contact times. The solid lines represent the cost derived from the epidemic model (calculated cost), and the dashed lines are the averages over 100 simulation runs for different values of $I_0$. ................................................................. 193
A.5 Simulated and calculated trajectories of the states for a network of 400 nodes with exponential inter-contact times. The solid lines represent the trajectories obtained from the epidemic model (calculated trajectories), and the dashed lines are the averages of the trajectories over 100 simulation runs.

A.6 Comparison of the simulated and calculated costs for a network of 400 nodes with exponentially distributed inter-contact times. The solid lines represent the cost derived from the epidemic model (calculated cost), and the dashed lines are the averages over 100 simulation runs for different values of $I_0$.

A.7 Simulated and calculated trajectories (i.e., sample paths) of the states for a network of 41 nodes with truncated power-law inter-contact times. The solid lines represent the trajectories obtained from the epidemic model (calculated trajectories), and the dashed lines are the averages of the trajectories over 100 simulation runs.

A.8 Comparison of the simulated and calculated costs for a network with power-law distributed inter-contact times. The solid lines represent the cost derived from the epidemic model (calculated cost), and the dashed lines are the averages over 100 simulation runs.

A.9 Robustness of the saddle-point strategy with respect to clock drift. The increase in the overall cost is less than 9%.

A.10 Optional caption for list of figures

A.11 Optional caption for list of figures
Chapter 1

Overview

1.1 Motivation

Malicious self-replicating codes, known as malware, pose substantial threat to the wireless computing infrastructure. Malware can be used to launch attacks that vary from the less intrusive confidentiality or privacy attacks, such as traffic analysis and eavesdropping, to the more intrusive methods that either disrupt the nodes normal functions such as those in relaying data and establishing end-to-end routes (e.g., sinkhole attacks [37]), or even alter the network traffic and hence destroy the integrity of the information, such as unauthorized access and session hijacking attacks [82], [32]. Malware outbreaks like those of Slammer [54] and Code Red [88] worms in wired Internet have already inflicted expenses of billions of dollars in repair after the viruses rapidly infected thousands of hosts within few hours. New investments have increasingly been directed toward wireless infrastructure thanks to the rapid growth of consumer demands and advancements in wireless technologies. The economic viability of these investments is, however, contingent on the design of effective security countermeasures.

The first step in devising efficient countermeasures is to anticipate malware hazards, and understand the threats they pose, before they emerge in the hands of the attackers [26]. Recognizing
the above, specific attacks such as the wormhole [34], sinkhole [37], and Sybil [22], that utilize vulnerabilities in the routing protocols in a wireless sensor network, and their counter-measures, have been investigated before they were actually launched. The first questions addressed in this dissertation are (i) quantifying fundamental limits on the damages that the attackers can inflict by intelligently choosing their actions, and (ii) identifying the optimal actions that inflict the maximum damage on the network. Such quantification is motivated by the fact that while attackers can pose serious threats by exploiting the fundamental limitations of wireless network, such as limited energy, unreliable communication, constant changes in topology owing to mobility [80], their capabilities may well be limited by the above as well since they rely on the same network for propagating the malware.

Our next step is to characterize maximum efficacy defense, attained by intelligent and dynamic choice of counter-measure parameters such as immunization rates and reception gains of nodes that are yet to be infected. This is motivated by the fact that the choice of counter-measure parameters is constrained by the inherent resource limitations in the network. We also seek to identify the optimal counter-measures that maximally limit the damage imposed by the attacker. The answers in both cases depend on the network parameters such as communication ranges of the nodes, mobility parameters, and also the counter-measure parameters such as the rates of updates of security patches, etc.

Given the flexibility that software-based operation provides, it is reasonable to expect that new malware will not demonstrate a fixed behavior over time. Instead, malware can dynamically change its modus operandi in response to the dynamics of the network, in order to maximize the overall damage it inflicts. However, in return, the network can also dynamically change its counter-measure policy to more effectively oppose the spread of the infection. The infinite dimension of freedom introduced by variation over time and antagonistic optimization of malware and network against each other demand new attempts for modeling and analysis of their confrontation. This dissertation also investigates such confrontations and identifies maximum
damage dynamic strategies of attack and devises robust dynamic defense.

1.2 System state evolution

Worms spread during data or control message transmission from nodes that are infected (infec-
tives) and those that are vulnerable, but not yet infected (susceptibles). We consider a pernicious worm that may (i) eavesdrop, (ii) analyze, (iii) alter or destroy traffic and (iv) disrupt the infective host’s normal functions (such as relaying data or establishing routes), and even kill the host, that is, render it completely dysfunctional (dead). This killing process may be triggered by performing a code which inflicts irretrievable hardware damage. For instance, Chernobyl virus [57] could reflash the BIOS, corrupting the bootstrap program required to initialize the system. The worm can determine the time to kill, or equivalently the rate of killing the hosts, by regulating the rate at which it triggers such codes.

Counter-measures can be launched by installing security patches that either immunize susceptible nodes against future attacks, by rectifying their underlying vulnerability, or heal the infectives of the infection and render them robust against future attacks. For instance, for SQL-Slammer worms [54], while StackGuard programs [17] immunize the susceptibles by removing the buffer overflow vulnerability that the worms exploit, specialized security patches [71] are required to remove the worm from (and thereby heal) the infectives. Nodes that have been immunized or healed are denoted as recovered. Thus, depending on whether the worm kills the infective before it fetches a security-patch, the state of an infective changes to dead or recovered. States of susceptible nodes change to infective or recovered depending on whether they communicate with infectives before installing the security-patches. Note that the counter-measures incur costs, since the patches must be obtained through the bandwidth-limited wireless media involving energy-expensive communications, and different patches potentially incur different costs depending on whether they treat susceptibles or infectives. Thus, such counter-measures
must be resorted to, selectively and judiciously.

1.3 Decision problems of the attackers

The goal of the attacker is to infect as many nodes as possible, and use the worms to disrupt the hosts as well as the network functions, while being cognizant of the countermeasures [81]. We consider two different attack settings in Chapters 3 and 4, which we respectively refer to as battery depletion and seek and destroy attacks.

In the battery depletion attack setting, the malware decides the rate at which an infective node accesses the media in search of new susceptible nodes. At any given time, the infectives can accelerate the rate of spread of the worm by increasing their contact rates with susceptibles by selecting higher transmission gains and media scanning rates. Such a choice however depletes their energy reserves which are limited as those of any other nodes in wireless networks. Depending on whether the malware drains an infective’s battery before the node fetches the security patch, its state changes to dead or recovered. Killing an infective host by draining its battery sooner rather than later disrupts its functions and thereby inflicts damage on the network right away, but also prevents it from propagating the infection in the network and performing its other baleful activities such as eavesdropping, traffic destruction, etc. Deferral of killing, on the other hand, may allow the host to be healed of the infection before it can be killed, or infect other hosts. Moreover, the elevated media access rate and battery usage might also expose the malware to anomaly detection tools and hence lead to higher overall recovery rates. Recognizing all these inter-twined trade-offs, it is therefore interesting to determine the instantaneous rate of media access rates that maximizes the aggregate damage inflicted by the worm.

In the seek and destroy attack setting, similar to the battery depletion attack, the malware can use an infective node as long as is battery is not completely drained. However, the malware enjoys an extra feature that the battery depletion attack did not have: it can kill an infective node
whenever it wishes by invoking specific codes that inflicts irretrievable hardware or software
damage in the node and make it completely dysfunctional. In the battery depletion model, mal-
ware could only deplete the battery to impair an infective node, which is more benign compared
to the seek and destroy attack where the malware can permanently extirpate the node. Thus in
the seek and destroy attack, the malware selects the transmission gains and media access rates
so that the battery reserves last during the period of the infection in order to utilize the infective
nodes and exterminate them as an independent decision with time. We consider the transmission
range of the infective nodes and the rate of killing as distinct dynamic control functions of the
worm which are jointly optimized in order to inflict the maximum damage.

1.4 Decision problems of the defense

The counter-measure focuses on the containment of infection in a mobile wireless network. Sev-
eral wireless properties enhance the severity of the infection. However, these unique features
can also be utilized to contrive new counter-measures against the spread of the infection. An
infected node can transmit its infection to another node only if they are in communication range
of each other. We propose to quarantine an infection by regulating the communication range of
the nodes. Specifically, the reception gain of the healthy nodes can be reduced to abate the fre-
quency of contacts between the mobile nodes and thus suppress the spread of the infection. This
is achieved, however, at an expense: reducing the communication range of nodes can deteriorate
the QoS offered by the network, as the overall badwidth decreases and end-to-end communica-
tion delays increase. The defense needs to choose the reception gain of the nodes (that is, for the
nodes whose reception gains the defense can control - the ones that are yet to be infected) so as
to optimize the trade-off between QoS and damage due to infection.

The susceptible nodes can be immunized and infectives can be healed through installation of
security patches. However, the distribution of the patch relies on the transmission resources in
the network. Hence, the propagation and dispatching of a security patch, if not carefully con-
trolled, can become a menace itself which threatens to deteriorate the function of the network
by taxing the limited transmission and processing resources such as spectrum and energy. An
example of such a predicament in wired networks was experienced in the case of the outbreak
of Welchia [14, 62]. Welchia, a variant of Blaster worm itself, was designed as a counter-worm to
defeat Blaster, but its uncontrolled propagation proved even more disruptive in terms of crash-
ing and slowing systems. This threat is but more dire in a wireless setting since due to media
being common and the channels being unreliable, the bandwidth can be a more restrictive con-
straint. Also, mobile nodes are limited in their energy resources. An important decision problem
of the counter-measure is to decide the rate at which such security patches should be propa-
gated in the system. We consider two different settings for dispatching and distribution of the
security patches in a mobile wireless network. In the first model, a number of mobile (or sta-
tionary) agents pre-loaded with the security patch deliver the security patch upon a contact with
a functioning node which has not received the security patch yet. In the second scenario, the
receptors of the security patch themselves propagate the security patch by forwarding it to other
susceptible or infective nodes. We respectively refer to these two models as non-replicative and
replicative patchings. The decision of the defense policy is that at each given time, what portion
of the dispatchers are activated, and at which rates they should transmit the security patches,
without knowing the instantaneous state of the system. Activation of more of such nodes and
increase of their rates of transmission accelerate the spread of the security patch, however, at the
expense of consuming more of the underlying resources of the mobile wireless network such as
the ever-demanded bandwidth, battery and processing time of the nodes.
1.5 Summary of the contributions

1.5.1 Formulation of maximum damage attack

In part I, we hold the perspective of an attacker, assuming the defense parameters are fixed over time. For both battery depletion (Chapter 3) and seek and destroy (Chapter 4) attack settings, we develop mathematical frameworks which cogently model the effect of the decisions of the attackers on the state dynamics and their resulting trade-offs through a combination of epidemic models and damage functions. Specifically, we assume that the damage inflicted by the worm is a cumulative function increasing in the number of infected and dead hosts, both of which change with time. The worm seeks to maximize the damage subject to satisfying certain constraints on the energy and power consumption of its hosts by dynamically selecting its control parameters while assuming full knowledge of the network parameters and the counter-measures. The maximum value of the damage function then quantifies the fundamental limits on the efficacy of the worm, particularly, since we assume that the worm has complete knowledge of all the contributing factors, and uses optimal dynamic strategies. The damage maximization problem is cast as optimal control problems which can be solved numerically by applying Pontryagin’s Maximum Principle [24, 47, 63].

Second, we answer the natural next question of whether in practice the worm can indeed inflict the damage quantified above, or the above quantifications constitute only theoretical upper bounds. Specifically, if the optimal policies that inflict the above maximum damage are complex to execute, then the worm may not be able to execute them since they are limited by the capabilities of their resource constrained hosts as well. Towards this end, we investigate structures of the optimum policies for the worms. Our results have negative connotations from the counter-measures point of view since we show that an attacker can inflict the maximum damage by using very simple decisions. In the battery depletion attack setting, we establish (§3.3) that the malware uses the maximum power to aggressively spread itself until a threshold time, and subsequently
ceases its media access activities altogether and enters an energy-saving mode while furtively performing its malicious activities. If the malware seeks also to increase the final tally of the dead nodes, then a final slaughter phase follows the initial blitz and intermediate stealth phases. In the final slaughter phase, the malware resumes, at the maximum power, the media access activities of the infected nodes, seeking primarily to kill them by depleting their residual energy reserves. In the optimal control terminology [24, 47, 63], we have shown that the optimal strategy has a bang-bang structure, that is, at any given time, the battery usage is either at its minimum or maximum possible values, and has at most two jumps which necessarily culminates at the maximum possible value.

In the seek and destroy setting, we prove (§4.3) that the optimal killing rate has the following simple structure: until a certain time (which can be zero depending on the network and countermeasure parameters), the worm does not kill any host, and right after that, it annihilates its hosts at the maximum possible rate until the end of the optimization period. Thus the optimal killing rate is bang-bang but with at most one jump, which culminates at the maximum value. We also prove that when the energy consumption costs are strictly convex the worm’s optimal energy consumption rate is a decreasing function of time. Thus, the worm seeks to infect as many hosts as possible early on by selecting the maximum possible values of the media scanning rates and transmission ranges, and thereafter starts to behave more conservatively so as to satisfy the energy consumption constraints. When the energy consumption costs are concave, the structure is even more specific: the optimal media scanning rates and transmission ranges are not only decreasing functions of time, but also have a bang-bang nature with at most one jump from the maximum possible value to the minimum possible value. Therefore, the joint optimal controls delineate two phases to the optimal attack, the first phase is to amass the infectives and then arrives the slaughter time. The result carries a qualitative cautionary message for countermeasures as well: an apparently inoffensive malware with little disruptive behavior might well be stacking infective hosts for the imminent carnage.
1.5.2 Formulation of the maximum efficacy countermeasure

In part II, we adopt the viewpoint of the network and assuming the attack parameters do not vary over time, we formulate defense decisions based on deterministic epidemic modeling. We propose an optimal control framework to characterize the trade-off between the containment efficacy, and communication capabilities of the nodes by reducing the reception gain of the susceptibles (Chapter 5) and the extra resources used for patching (Chapter 6).

For both of the defense mechanisms, we investigate whether the optimal policies that inflict the minimum cost are complex to execute, which could turn them impractical to implement in reality. Our results are promising: we show that minimum overall cost is achieved by executing very simple strategies. In reception gain reduction, the optimal policy in general can be divided into three time phases: the first phase (which depending on the parameters of the system can have length zero) is less intense reception gain reduction. This is followed by a potentially second phase during which the rate reduction is extreme. In the last phase, which extends till the end of the optimization period, the reception gain is increased to normal. The transitions between these phases are abrupt for concave QoS costs, and is smooth for strictly convex QoS costs. In patching, in both non-replicative and replicative models, we prove that optimal policies have simple structures: for a concave bandwidth consumption cost, activate all dispatchers and choose the maximum possible transmission rate for them until a certain time; subsequently all dispatchers must be de-activated until the end of the network operation period. We have therefore shown that the optimal control is \textit{bang-bang} with at most one jump that terminates at the minimum possible value. The optimal control has a similar structure for a convex bandwidth consumption cost, except that its transition from the maximum to minimum values is (strict but) continuous rather than abrupt.
1.5.3 Dynamic game of defense v.s. attack

When both defense and attack can strategically change their parameters of control with time, we have a dynamic game setting. Then a robust counter-measure is one that seeks to minimize the damage inflicted by the malware assuming that the malware chooses its strategy so as to maximize this damage with full knowledge of the counter-measure. Due to the aforementioned trade-offs and since an optimal strategy of the malware depends on the strategy of the network and vice versa, determination of robust strategies for either is non-trivial. In part III, we propose a method to answer these questions. First, we construct a mathematical framework which cogently models the strategic confrontations between the malware and the network as a zero-sum dynamic game (§7.1). We then prove the existence of the robust (i.e., saddle-point) strategies of the network and the malware (§7.1), and compute them (§7.2.2). Existence of such strategies and also their computations are not clear a priori, since the strategy set of each player is uncountably infinite and consists of functions of time and the model is nonlinear.

We prove that the robust defense strategy has a simple two-phased structure (§7.2.3): (i) patch at the maximum possible rate until a threshold time, and then stop patching (ii) choose the minimum possible reception rate (i.e., the maximum packet drop rate at the receivers) until a threshold time and subsequently revert to the normal reception rate. The initial aggressive defense limits the spread of infection and thereby the pool of nodes that can potentially be compromised or killed; this guarantees an upper bound on the damage inflicted irrespective of the malware’s choice of annihilation strategy. Given its simple structure, the defense control can readily be implemented in resource constrained wireless devices. From a game-theoretical point of view, the structural results are somewhat surprising given the non-linear dynamics of state evolutions and the non-monotonicity of the state functions, and their proofs rely on non-standard techniques.

Our numerical computations reveal that our robust dynamic defense strategy attains substantially lower value of the maximum damage inflicted by the malware as compared to that
for heuristic static choice of defense parameters. Our dynamic strategies are shown robust to parameter estimation and clock drifts.

1.5.4 A unified framework and further applications

Epidemic models based on nonlinear differential equations have been extensively applied in a variety of systems as diverse as infectious outbreaks, marketing, diffusion of beliefs, etc., to the dissemination of messages in DTN or p2p networks. In part IV, we investigate whether our optimal control framework and structural results can be applied to setting beyond network security. In this regard, we motivate various instantiations of the model in contexts of DTN routing, marketing and health-care. We develop a unified optimal control framework based on a nonlinear deterministic epidemic model and generalized costs to capture the system dynamics and optimization objective in the above contexts. We establish that our structural results extend to the generalized formulation as well.

1.6 Related literature

Epidemic modeling based on the classic Kermack-Mckendrick model [18] has extensively been used to analyze the spread of malware in wired networks [15, 42–45, 65, 70, 79, 88, 89], etc, and more recently in wireless networks [16, 51, 72–75]. These works show, through simulations and matching with actual data, that when the number of nodes in a network is large, the deterministic epidemic models can successfully represent the dynamics of the spread of the malware.

Most of the existing work on dynamic control of parameters of the malware or the network propose heuristic dynamic policies in different contexts, and evaluate them using simulations. [13, 39–41, 59] investigate different attack mechanisms. [59] describes a vulnerability in MMS services in cellular networks that enables an attacker to drain the device batteries, and [13] proposes battery depletion through reduction of sleep cycles of sensors. We focus on managing,
rather than merely depleting, the device batteries for maximizing the overall damage inflicted on
the network which is fostered both by the spread of the infection and the battery depletion. The
closest to our attack setting are [41] and [39] which propose strategies for utilizing the infectives’
available energy so as to increase the spread of the malware; [41] proposes heuristics which do
not provide any damage guarantee, whereas [39] focuses on the static (as opposed to dynamic)
optimum choice of the malware’s parameters. [19, 64, 68, 78, 84, 85] assume the defense point
of view against malware outbreaks. Control theoretic tools have been used in [19] to propose a
feedback-based (but heuristic) strategy for containment of malware in a wired network. [64,84,85]
consider reduction of communication rates as a defense mechanism. However, [84] is based on
heuristics and simulations, and unlike our work, [85] does not propose a formal framework for at-
taining desired trade-offs, and considers only a static choice of the communication rate, whereas
we allow the communication range of the nodes to dynamically evolve over time as the infection
level fluctuates. [64] proposes to contain a worm in the initial phase of infection by limiting the
total number of distinct contacts per node over the containment cycle, and models the growth
of the worm using a stochastic branching process. However, this work only applies to the ini-
tial phase of infection and their countermeasure is ineffective once the epidemic starts. Patching
as a defense mechanism is investigated in [68,78] among others. Both of these works consider
replicative and non-replicative dispatch in wired networks. The analytical tools and the results
presented there do not however apply in our context since (i) the patching rate is assumed con-
stant in [68,78], whereas we consider dynamic patching policies and (ii) [68,78] consider the final
(maximum, resp.) number of the infective nodes as the performance metric whereas we investi-
gate more general cost functions based on the level of infection as well as the overall bandwidth
consumed by the dispatchers.

Models of propagation of malware which consider the underlying topology of the network
(hence primarily focused on static wired/social networks) are studied in [7,11,28] among others.
These works, although more accurate to model the spread of the network if the underlying topol-
ogy is known, do not consider dynamic (changing with time) policies; they focus on SIS models of treatment (where the patched nodes are again susceptible to infection) and mostly focus on the probability of having a long term level of infection and the size of such a population. [11] considers the resource limitation of patching, however, provides optimality only in long term sense and provides order results (in the number of nodes in the network). In contrast, we assume a large enough network in which the spread of malware can be approximated by its mean-field representation. At the cost of this loss of accuracy in the modeling, we achieve absolute optimality over any desired time horizon and using dynamic policies, and we characterize the nature of the optimal solutions.

Very few research works have in fact tried to adopt malware propagation models to investigate optimal dynamic attack and countermeasure responses based on a quantified damage function in wired or wireless networks. [9, 10, 86], which assume the defense point of view, constitute notable exceptions. Our defense framework differs from [9, 10, 86] in that we consider (i) reduction of reception gain of nodes as well as patching (both replicative and non-replicative), and (ii) more general network state evolution dynamics in that the counter-measure involves both immunization and healing, moreover the worm may cause mortality, and (iii) cost functions which are only assumed to be either concave or convex and therefore more general than quadratic functions in [9, 10, 86]. Also unlike [9, 10] we do not use any linearization of the system which can be very poor in the context of epidemic behavior. Moreover, we provide provable structural results for fairly general system dynamics and cost functions.

In contexts other than network security, optimal control has been extensively used to find the best deployment of resources e.g. in treating infectious epidemics [6, 83], advertising and marketing [25, 66, 67] and recently, in epidemic routing [2, 3]. An extensive overview of the existing work is beyond the scope of this article. In what follows, we mention and differentiate from some of the most related works. Formal application of optimal control theory in treatment of infectious epidemics is mostly done for systems where only vaccination or healing/quarantining is present,
the cost is linear in the treatment rate and/or there is no mortality among infectives [6, 83]. In contrast, our generalized framework integrates both vaccination and healing/quarantining, the cost of treatment is any general concave or convex function, and it depends on both infective and the deceased. Moreover, there is no equivalent of replicative immunization in the case of infectious diseases. Also, our unified framework generalizes the existing treatment of models in advertising and marketing [25, 66, 67] which mostly consider only either public advertisement or word-of-mouth advertisement with linear benefits, and optimizations are mostly with respect to the steady state behavior of the market, rather than the transitional patterns, which is the salient feature of the diffusion of new technologies. We consider a nonlinear system and general cost functions, and consider the transients of the evolution of the states as well. Interestingly, the optimal control strategies in a related context, that of epidemic forwarding of packets in an energy-constrained delay tolerant wireless network [2, 3], follow similar structures as our optimal dispatch strategies. The objective in that context is to deliver a message to its destination before a deadline through forwarding upon contact. The control variable is whether or not (and with what rate) a recipient of message should transmit it to the next node which it contacts. [2, 3] show that the forwarding decisions are bang-bang with at most one jump. But, we need a different set of analytical arguments to establish our structure results, because [2, 3] rely on some crucial assumptions that are ruled out in our context. Specifically, [2] considers only networks that use two-hop routing, and therefore, the resulting dynamics of the number of infectives (i.e., nodes that have received the packet) is not representative of an epidemic behavior which is central to the propagation of malware in wireless networks. Also, [3] investigates a monotonic epidemic model, which arises when none of the nodes that have received a desired packet loses it (i.e., the infectives do not lose their infection). By contrast, in our context, counter-measures as well as mortality may reduce the infection.

Game theory has been used in the context of security in networks as it is apt to model the interactions of attackers and defenders, e.g. in [1, 31, 36, 49, 53, 56]. [53] presents models for the
inference of the intents, objectives and strategies of a new attacker and apply it to a DDoS attack. In their work, however, the sets of actions of both the attack and the defense are finite, and structural property of Nash Equilibria or saddle-points have not been obtained; the work focuses on the modeling and numerical evaluations. Algorithmic implementations of (variations of) models in [53] are pursued in [36], [31], etc. [76] combined a deterministic worm propagation model with a game theoretic process that involves learning, in order to incorporate decisions of users about whether to install or uninstall a security patch in a wired network. We apply dynamic zero-sum games to model the strategic confrontations of a malware and the defense in a wireless network, and delve into the structural properties of the saddle-point strategies, when the attack and defense can intelligently choose the annihilation, patching and reception rates respectively. Thus, unlike most of the existing work, the defense operates also at the MAC and physical layers, as opposed to only at the routing or application layers. Indeed, we analyze not only the security risks (fraction of infectives, dead nodes), but also the QoS degradations (packet drops) and the lower layer bandwidth consumptions (in transmission of patches) associated with the tradeoffs. Also, the strategy sets of each player is uncountably infinite since the strategies are functions of continuous time with continuous ranges. The differences in the contexts and the nature of choices require a substantially different analytical approach. Our contributions complement [1], which focuses on detecting the intrusion of a worm that dynamically controls the intensity of its activity, but does not investigate subsequent defense. [49, 56] assume a network in which each user autonomously decides whether or not install a security measure, depending on his/her utility function, and they show that a pure Nash equilibrium (of these decisions) exist. They however, assume the actions of the malware, and of the users once decided, are fixed over time, and the game is between the users. In contrast, in our model, the actions of the users and the malware can dynamically and strategically vary over time and the game is between the network and the malware.
Chapter 2

Notations and Assumptions

In this chapter, we introduce common notations and model assumptions which will be used throughout the thesis. A susceptible node is a communication device that is not contaminated by the worm, yet is vulnerable to infection. A node is infective if it is contaminated by the worm. An infective spreads the worm to a susceptible node while transmitting data or control messages to it. The worm can kill an infective host, i.e., render it completely dysfunctional - such nodes are denoted dead. A functional node that is immune to the worm is referred to as recovered.

Let the total number of nodes in the network be \( N \). Let the number of susceptible, infective, recovered and dead nodes at time \( t \) be denoted by \( n_S(t) \), \( n_I(t) \), \( n_R(t) \) and \( n_D(t) \), respectively, and the corresponding fractions be \( S(t) = n_S(t)/N \), \( I(t) = n_I(t)/N \), \( R(t) = n_R(t)/N \), and \( D(t) = n_D(t)/N \) (Table 2.1) respectively. Then, \( S(t) + I(t) + R(t) + D(t) = 1 \). At the time of the outbreak of the infection, that is at time zero, some but not all nodes are infected: \( 0 < I(0) = I_0 < 1 \). For simplicity, let \( R(0) = D(0) = 0 \). Thus, \( S(0) = 1 - I_0 \).

In this thesis, we model the dynamics of the propagation of the infection using deterministic epidemic models based on the classic Kermack-Mckendrick model [18]. Experiments as well as network simulations have validated that such models provide an acceptable representation for the spread of malware in large mobile wireless networks (see e.g. [16, 73, 74]) - we also indepen-
<table>
<thead>
<tr>
<th>$S(t)$</th>
<th>fraction of the susceptible nodes</th>
</tr>
</thead>
<tbody>
<tr>
<td>$I(t)$</td>
<td>fraction of the infective nodes</td>
</tr>
<tr>
<td>$R(t)$</td>
<td>fraction of the recovered nodes</td>
</tr>
<tr>
<td>$D(t)$</td>
<td>fraction of the dead nodes</td>
</tr>
</tbody>
</table>

**Table 2.1:** List of notations of measures.

dently validate them in Appendix A. These epidemic models rely on some abstraction which we motivate and justify next. We ground our assumptions in the context of two driving applications, Delay Tolerant Networks (DTN) and Multimedia Messaging Service (MMS) in a 3G/4G network. A DTN (Delay Tolerant Network) is a mobile ad-hoc network (MANET) in which the communication range is very small compared to the roaming area. Such networks are highly mobile and continuous connectivity is rare. Application of DTN arises in the contexts of military networks, sensor-actuator networks, networks in extreme terrestrial environments, etc [23]. MMS in the context of cellular network is a service which allows users to send multimedia messages which contains elements such as pictures, audios and videos to other users in a the cellular network.

An infective initiates communication with a susceptible when it generates a valid ID of a susceptible handset in cellular networks with MMS service, or detects the presence of a susceptible node in its communication range in a DTN, and spreads the worm to the susceptible during such communications. Two nodes are said to be in *contact* whenever they communicate. An infective is equally likely to initiate communication with each node, and hence with each susceptible, say at rate $\beta$. The property that this rate is equal for each pair is often referred to as *homogeneous mixing*. Homogeneous mixing constitutes a key assumption in our models, and in what follows we justify this assumption in the context of MMS networks and DTNs.

In a 3G/4G network, homogeneous mixing property can arise when infective nodes generate the ID’s of potential susceptibles uniformly randomly from a space of valid ID’s. Note that each
pairwise communication involves two wireless hops between mobile nodes and access points or base stations, and one fast wireline backbone between the access points or base stations. The relative location of communicating nodes determines the number of hops in the fast backbone network, for which, in comparison to the wireless channel, the delays are often negligible. Thus the contact rates are not affected by the relative location of pairs.

In DTNs, an infective transmits a message to a susceptible with a given probability whenever the infective detects the presence of the susceptible in its transmission range. This probability is proportional to the rate $u_0$ at which the infective scans the media in search of susceptibles nearby, and the proportionality constant is determined by the message collision probability $\eta_1$, which is determined by the communication range of the nodes, and the overall node density ($N/A$). Under mobility models such as the random waypoint or random direction model [8], Groenevelt et al. [30] have shown that the time between consecutive arrivals of a specific pair of nodes in each others' communication ranges is nearly exponentially distributed, and the rate $\eta_2$ of this exponential process is equal to $\frac{2wE[V^*]}{A}u_1$, where $w$ is a constant factor pertaining to the specific mobility model, $E[V^*]$ is the average relative speed between two nodes, and $u_1$ is the communication range of the pair, which itself is proportional to the product of the transmission gain of the antenna of the transmitter and the reception gain of the antenna of the receiver. Note also that this rate is inversely proportional to the roaming area, i.e., $\eta_2 \propto \frac{1}{A}$. This result has been proved when the communication range of the nodes is small compared to the total area of the region and $v$ is sufficiently high and is validate through simulations. Thus, a given infective-susceptible pair contacts as per an exponential random process whose rate at any given time $t$ is $\hat{\beta}$, where $\hat{\beta} = \eta_1\eta_2u_0$, and homogeneous mixing holds.

Patches are distributed when a dispatcher communicates (i.e., contacts) with an infective or a susceptible node. If the receptor of a security patch is a susceptible node, it installs the security patch, is subsequently immunized, and its state changes to recovered. If however the receptor is an infective, the patch may fail to heal it, or, the worm may obstruct or delay its installation.
We capture the above possibility, by introducing a coefficient \(0 \leq \pi \leq 1\). \(\pi = 0\) corresponds to the case where the patch is completely unable to remove the worm from infectives, and only immunizes the susceptibles, whereas \(\pi = 1\) represents the other extreme scenario where a patch can equally well immunize and heal susceptibles and infectives, and intermediate values of \(\pi\) represent probabilistic or delayed recovery for infectives.

The details of the model for patching slightly varies between our chapters.\(^1\) Here, we provide a high-level road-map of the patching rates considered in each chapter. In part I, the patching rate is fixed over time, as the focus is on the dynamic control of the attacker. In Chapter 3 of part I (unlike in the rest of the paper), we could manage to consider the rates of recovery to also depend on the activity level of the malware, as higher power usage activity can potentially trigger abnormality detection softwares and lead to higher rates of patching. In neither one of Chapters 3 or 4, \(\pi\) (the relative efficiency of patching in healing the infectives compared to immunizing the susceptibles) has to be less than one. Indeed, we do not mention \(\pi\) in the analytical results therein. In Chapter 5 of part II, the patching rate is fixed, as the focus is on the optimization of rate reduction as the dynamic defense control. The patching is assumed to be able to only heal the infectives (no immunization is considered).\(^2\) In Chapter 6 of part II as well as in part III, the patching is dynamic and \(\pi\) is assumed to be bellow one.

Another assumption that we make in our model construction is that although controls vary with time, at a given time all node use the same control as opposed to an individual-based policy. In what follows we justify this assumption. Note that distinction between an infective node and a susceptible node is difficult a priori. Indeed, we assume that from the system’s point of view, information about whether or not a node is infective is not available to any other node. Therefore, information about the state of the nodes is either nonexistent or at best represents a statistics about the average state of the whole network. Hence, at any given time \(t\), all nodes

---

\(^1\)The analytical results in each chapter is derived assuming the specific choices. However, they may not be necessary conditions in general.

\(^2\)Our postulation is that this choice can be relaxed and relevant structural results can be strengthened.
choose identical controls, either for defense or attack. Nevertheless, the reception gain of the nodes, the fraction of activated dispatchers and the rate of dispatching can be allowed to vary with time, i.e., selected dynamically, though identically among individual nodes.

In part I, to obtain fundamental bounds on the potency of the attack, we assume that the network parameters are known to the malware. Similarly, in part II, in order to obtain fundamental bounds on the efficacy of the defense, we assume that the network computes its optimal controls assuming full knowledge of the attack parameters. However, in the numerical sections of the corresponding chapters, we investigate the effect of errors in the estimation of these parameters on the aggregate damage. We also assume that the parameters of the opponent is selected a priori and does not change them with time. In contrast, in part III, we consider the case in which the parameters of neither the attack nor the defense are fixed and rather can be selected dynamically, and hence should be taken into account in the decisions of both the attacker and the defender.
Part I

Attack
Chapter 3

Battery Depletion Attack

Introduction

One of the most critical resources in a mobile wireless network is the energy reserves of the nodes. An important decision of the malware pertains to its optimal use of the available energy of the infective nodes. The infectives, at any given time, can accelerate the rate of spread of the malware by increasing their contact rates with susceptibles by selecting higher transmission gains and media scanning rates. Such a choice, however, (a) can lead to easier detection of the malware as a deviation from the normal energy signature of the devices [46], prompting the nodes to fetch appropriate patches sooner, and (b) depletes the infectives’ energy reserves faster which in turn limits the spread of the infection and also their other malicious activities such as eavesdropping, traffic destruction, etc. Early loss of infectives due to their battery depletion may thwart the spread of the malware. The attack seeks to infect and kill as many nodes as possible, use the malware in the infectives to disrupt the hosts as well as the network functions while being cognizant of the countermeasures [81]. The challenge then is to determine the dynami-
cally changing instantaneous transmission gain and/or media access rate of the infectives that maximize the overall damage inflicted by the malware.

First, we construct a mathematical framework which cogently models the effect of the decisions of the attackers on the state dynamics and their resulting trade-offs through a combination of epidemic models and damage functions (§3.1). Next, we prove that an attacker can inflict the maximum damage by using simple decisions. Specifically, if the attacker seeks to maximize an aggregate over time of the fraction of the infective and the dead nodes but is not concerned about their final tallies, then until a certain time, each infective nodes uses the maximum power to aggressively spread itself, and subsequently it ceases its media access activities altogether and enters an energy-saving mode while furtively performing its malicious activities like eavesdropping, analyzing sensed data, sabotaging routes, changing data, etc. (theorem 3.3.2, §3.3). Thus, the attack consists of an initial blitz phase and a subsequent stealth phase. If, on the other hand, the malware seeks also to increase the final tally of the dead nodes, then a final slaughter phase follows the initial blitz and intermediate stealth phases. In the final slaughter phase, the malware resumes, at the maximum power, the media access activities of the infected nodes, seeking primarily to kill them by depleting their residual energy reserves.

3.1 System model

3.1.1 Dynamics of state evolution

We introduced the common notations and main assumptions in Chapter 2. In what follows, we specify the battery-depletion model.

Let $u$ be the product of the infective’s transmission range and its media scanning rate.\footnote{A dynamic strategy allows the decision variables to vary with time, whereas a static strategy chooses their values at $t = 0$ and does not change them subsequently.} Following MMS networks it is likely that only the media scanning rate is controllable, through the rate at which each node sends request to transmit packages. This clearly does not restrict our analysis.
lowing the homogeneous mixing property discussed in Chapter 2, the malware is thus transmitted between a given infective-susceptible pair at rate $\hat{\beta}u$, where $\hat{\beta}$ is the product of pairwise contact rates and the message delivery success upon each contact. We allow $u$ to vary over time, hence we use $u(t)$. The malware regulates the spread of the infection by controlling $u(t)$ through appropriate choice of its transmission gain and media scanning rate.

The security patches are installed at an infective (susceptible, respectively) after random delays starting from when it is infected ($t = 0$, respectively). The delays account for the time required in detection of infection, and fetching the appropriate patch, etc. We denote the immunization and healing rates respectively by $Q(u)$ and $B(u)$.

A larger transmission range and a higher scanning rate leads to faster detection of the malware [12, 46], and therefore increases the overall recovery rate. Thus, $Q(\cdot)$ and $B(\cdot)$ are non-decreasing functions of $u$. We assume that $Q(x) > 0$ if $x > 0$. In practice, the advantage of easier detection starts to saturate with increase in $u$, thus both $B(\cdot)$ and $Q(\cdot)$ are likely to be concave, though we allow them to be convex as well4. We assume that $Q(\cdot)$ and $B(\cdot)$ are differentiable functions of $u$, and also $Q(0) = B(0) = 0$, i.e., no spreading/battery drainage attempts of the malware results in zero recovery rate, though we relax this latter assumption in Remark 2. Finally, we allow $Q(\cdot), B(\cdot)$ to be different functions as different patches may be required for immunization and healing, as the former involves only rectification of the vulnerability that the malware exploits, whereas the latter involves the removal of the malware as well. For instance, while StackGuard programs [17] immunize the susceptibles by removing the buffer overflow vulnerability that the SQL-Slammer malware [54] exploits, specialized patches [71] are required to remove the malware from (and thereby heal) the infectives.

3In a more general form, the immunization and healing rates themselves can be a function of the fraction of the infectives and susceptibles in the system as well. However, we derive our analytical results in the absence of such dependencies.

4The detection may also be affected by the fraction of infected nodes, which can be incorporated by allowing $Q(\cdot), B(\cdot)$ to be functions of both $u$ and $I$. 

24
Nodes are constrained in their battery reserves. The energy consumption during normal operations (i.e., when a node is susceptible or recovered) is negligible as compared to that in media access of the infectives - the former is therefore assumed to be zero.\(^5\) Therefore, the energy depletion time of an infective’s depends on its media access activities - we assume that exhaustion rate at time \(t\) is \(\rho u(t)\), where \(\rho\) is a positive coefficient. Note that the depletion rate must be an increasing function of \(u\), we assume it to be a linear function, since \(u\) can not be large so as to avoid interference. We assume that the malware does not know the remaining energies, thus the selected \(u(t)\) at a given node at a given \(t\) is not a function of its (or others’) residual energies.

Recalling that the system has a total of \(N\) nodes, let\(^6\)
\[
\beta = \lim_{N \to \infty} N \hat{\beta}.
\] (3.1.1)

The system model is hence as follows:\(^7\)
\[
\begin{align*}
\dot{S}(t) &= -\beta u(t)I(t)S(t) - Q(u(t))S(t), \quad \text{(3.1.2a)} \\
\dot{I}(t) &= \beta u(t)I(t)S(t) - B(u(t))I(t) - \rho u(t)I(t), \quad \text{(3.1.2b)} \\
\dot{D}(t) &= \rho u(t)I(t), \quad \text{(3.1.2c)} \\
\text{with } S(0) &= 1 - I_0, I(0) = I_0, D(0) = 0, \quad \text{(3.1.2d)}
\end{align*}
\]

which should also satisfy the following constraints at all \(t\):
\[
0 \leq S(t), I(t), D(t) \text{ and } S(t) + I(t) + D(t) \leq 1. \quad \text{(3.1.3)}
\]

Fig. 3.1 illustrates the transitions between different states of nodes. Note that epidemic models as in (3.1.2) involve state dynamics that are non-linear differential equations and the state

\(^5\)The formulations presented in Sections 3.1 and 3.2 extend when this assumption is relaxed, by allowing a transition from the susceptible state to the dead state (fig. 3.1).

\(^6\)A more elaborate discussion of the existence of this limit and mean field convergence to the deterministic model is provided in Appendix A.

\(^7\)Throughout the thesis, variables with dot marks (e.g., \(\dot{S}(t)\)) represent their time derivatives (e.g., time derivative of \(S(t)\)) and the prime signs (e.g., \(q'(S)\)) designate their derivatives with respect to their argument (e.g., \(S\)).
Figure 3.1: State transitions: $S, I, R, D$ respectively represent susceptible, infective, recovered, dead states. Here, $u(t)$ is product of the transmission range and media scanning rate of infectives at time $t$. The parameters $\beta, \rho$ and functions $B(\cdot), Q(\cdot)$ will be defined in Section 3.1.1.

function $I(t)$ may not be monotonic (e.g. figures 3.2 and 3.3).

3.1.2 Maximum damage battery depletion attack

We consider a malware that seeks to inflict the maximum possible damage in a time window $[0, T]$ of its choice. The malware benefits over time from the dead and the infected hosts. The malware can use the infectives to eavesdrop, analyze, alter or destroy data sensed or relayed by the hosts. It also benefits by inflicting a large death-toll by the end of the desired time window. These motivate the following damage function:

$$J = \int_0^T \left\{ \kappa_I I(t) + \kappa_D D(t) \right\} dt + K_I I(T) + K_D D(T).$$  \hspace{1cm} (3.1.4)

where $\kappa_I > 0$ and $\kappa_D, K_I, K_D \geq 0$.

The malware seeks to maximize the damage function by appropriately regulating $u(t)$, the product of the transmission range and the scanning rate of the infectives.\(^8\) When sensors are moving fast and no sensor has any information about the location of others, each sensor is equally likely to meet any other sensor in future irrespective of the past.\(^9\) Therefore, at any given time

\(^8\)The attacker does not control any other parameter such as the susceptible’s reception gain, node mobilities, etc.

\(^9\)This assumption can be analytically established when the inter-contact times between sensors are independent and exponentially distributed.
the optimal control will be the same for all infectives. The choice of $u(t)$ is subject to:

$$0 \leq u(t) \leq u_{\max}. \quad (3.1.5)$$

The above bounds arise from the physical constraints of the transmitters and also for ensuring that the interference among simultaneous transmissions remain limited.

Any piecewise continuous function $u : [0, T] \rightarrow \mathbb{R}$ such that the left and right hand limits exist and that satisfies (3.1.5) belongs to the control region denoted by $\Omega$. Now, for any $u(\cdot) \in \Omega$, the state constraints in (3.1.3) are satisfied throughout $[0, T]$.

**Lemma 3.1.1.** For any $u(\cdot) \in \Omega$, the state functions $(S, I, D) : [0, T] \rightarrow \mathbb{R}^3$ that satisfy (3.1.2), also satisfy (3.1.3). Moreover, $S(t) \geq (1 - I_0)e^{-C_1t} > 0$, $I(t) \geq I_0 e^{-C_2t} > 0$ for $t \in [0, T]$ and some finite $C_1, C_2$.

Thus, we ignore (3.1.3) henceforth. The following proof reveals that $C_1 = \beta u_{\max} + Q(u_{\max})$ and $C_2 = \rho u_{\max} + B(u_{\max})$.

**Proof.** According to (3.1.2), $S, I, D$ are differentiable, and therefore, continuous functions of time. Note that at $t = 0$, by assumption we have $0 < I = I_0 < 1$, and also $0 < S = 1 - I_0 < 1$. Hence, from the continuity of $S, I$, it follows that $S > 0$ and $I > 0$ in an interval starting from $t = 0$. Since $D(0) = 0$ and $\dot{D} \geq 0$ in this interval, it follows that $D \geq 0$ in this interval. Next, $S + I + D = 1$ at $t = 0$, however, by summing equations (3.1.2a), (3.1.2b) and (3.1.2c) we have $\frac{d}{dt}(S + I + D) \leq 0$, and hence $S + I + D \leq 1$ throughout this interval. Now, if the lemma is not true, from the continuity of $S, I, D$, either $S = 0$ or $I = 0$ or $D < 0$ or $S + I + D > 1$ at some $t < T$. Then there exists a time $t^*$ such that $S > 0, I > 0, D \geq 0, S + I + D \leq 1$ in $[0, t^*)$ and $S(t^*) = 0$ or $I(t^*) = 0$ or $D(t^*) < 0$ or $S(t^*) + I(t^*) + D(t^*) > 1$. Note that $D(t^*) \geq 0$ and $S(t^*) + I(t^*) + D(t^*) \leq 1$ from the continuity of $S, I, D$. For $0 < t < t^*$, from (3.1.2a) we have $\dot{S} \geq -C_1 S$, where $C_1 = (\beta u_{\max} + Q(u_{\max}))$. Thus $S \geq S(0)e^{-C_1 t}$, for all $0 \leq t < t^*$ and therefore, due to continuity of $S, S(t^*) > 0$. Similarly, for $0 < t < t^*$ from (3.1.2b) we have $\dot{I} \geq -C_2 I$ where $C_2 = \rho u_{\max} + B(u_{\max})$. Thus $I(t^*) > 0$ as well. The result follows from this contradiction. \qed
Once the control \( u(\cdot) \) is selected, the system state vector \((S(\cdot), I(\cdot), D(\cdot))\) can be obtained as a solution to (3.1.2). The state and control functions pair \(((S(\cdot), I(\cdot), D(\cdot)), u(\cdot))\) is called an admissible pair and \( u(\cdot) \) is called an admissible control if (i) \( u(\cdot) \) is in \( \Omega \), and (ii) the pair satisfies (3.1.2). If for an admissible pair \(((S, I, D), u)\),

\[
J(u) \geq J(\bar{u}) \quad \text{for any admissible control } \bar{u}
\]

then \(((S, I, D), u)\) is called an optimal solution and \( u \) is called an optimal control of the problem.

### 3.2 Malware’s optimal control

We now present a framework using which the malware can determine its optimal control function \( u(\cdot) \) and also compute the maximum value of the damage function. The main challenge in computing the optimal control is that the differential equations (3.1.2) can be solved provided the control is known. But, since \( \Omega \) consists of an uncountably infinite number of such controls, an exhaustive search on \( \Omega \) is ruled out. This dilemma may however be elegantly resolved using Pontryagin’s maximum principle which we apply next.

We start with by clarifying a notation: \( u \) (and other functions without an underline) represents the optimal control (and functions corresponding to it) whereas \( \bar{u} \) represents an admissible control. Let \(((S, I, D), u)\) be an optimal solution. Consider the Hamiltonian \( H \), and the co-state or adjoint functions \( \lambda_1(t) \) to \( \lambda_3(t) \) defined as follows:

\[
H := \kappa_I I + \kappa_D D + (\lambda_2 - \lambda_1)\beta u I S - \lambda_1 Q(u) S - \lambda_2 B(u) I + (\lambda_3 - \lambda_2)\rho u I \quad (3.2.1)
\]

\[
\dot{\lambda}_1 = -\frac{\partial H}{\partial S} = -\frac{\partial \lambda_1}{\partial S} - \beta u I S + \lambda_1 Q(u)
\]

\[
\dot{\lambda}_2 = -\frac{\partial H}{\partial I} = -\kappa_I - (\lambda_2 - \lambda_1)\beta u S + \lambda_2 B(u) - (\lambda_3 - \lambda_2)\rho u 
\]

\[
\dot{\lambda}_3 = -\frac{\partial H}{\partial D} = -\kappa_D
\]

along with the final (or transversality) conditions:

\[
\lambda_1(T) = 0, \quad \lambda_2(T) = K_I, \quad \lambda_3(T) = K_D. \quad (3.2.3)
\]
Then according to Pontryagin’s maximum principle ([24, P.111 theorem 3.14]), there exists continuous and piecewise differentiable co-state functions $\lambda_1, \lambda_2$ and $\lambda_3$ that at every point $t \in [0, T]$ where $u(t)$ is continuous, satisfy (3.2.2), (3.2.3), and we have at each $t$:

$$u(t) \in \arg \max_{u(t) \in \Omega} H(\bar{x}(t), (S(t), I(t), D(t)), u(t)). \quad (3.2.4)$$

Let

$$\varphi(x) := (\lambda_2 - \lambda_1)\beta x IS - \lambda_1 Q(x)S - \lambda_2 B(x)I + (\lambda_3 - \lambda_2)\rho x I. \quad (3.2.5)$$

Note that for each $x$, $\varphi(x)$ is a continuous function of time. Maximizing the Hamiltonian as per (3.2.4), we obtain:

$$\varphi(u(t)) \geq \varphi(u(t)) \forall t, \forall \text{admissible } u.$$  

Since $u = 0$ is admissible, $\varphi(u(t)) \geq 0$ at each $t$. Following lemma 3.3.1, which will come later, $\lambda_1, \lambda_2 \geq 0$. Thus:

- concave $Q, B \Rightarrow \varphi(x)$ is convex in $x$ at each $t$;
- convex $Q, B \Rightarrow \varphi(x)$ is concave in $x$ at each $t$.

We start from the first case, i.e., concave $Q$ and $B$, which is when the sensitivity of the detection, which is equal to the (partial) derivative of $Q$ and $B$ with $u$, reduces with more intense media access activity of the malware (more aggressive scanning rates, larger transmission powers). Then, at each $t$, $\varphi(x)$ is convex in $x$, and its maxima for $x \in [0, u_{\text{max}}]$ must occur at $x = 0$ or $x = u_{\text{max}}$. Hence:

$$u(t) = \begin{cases} 
0, & \text{if } \varphi(u_{\text{max}}) < 0 \text{ at } t \\
u_{\text{max}}, & \text{if } \varphi(u_{\text{max}}) > 0 \text{ at } t. \end{cases} \quad (3.2.6)$$

If either $Q(\cdot)$ or $B(\cdot)$ is strictly concave, $\varphi(x)$ is strictly convex in $x$ at each $t$, and $u(t) \in \{0, u_{\text{max}}\}$ at each $t$.  

29
If both $Q$ and $B$ are convex, then, at each $t$, $\varphi(x)$ is concave in $x$, and its maxima for $x \in [0, u_{\max}]$ must occur either at $x = 0$, or $x = u_{\max}$, or at $x$ such that $\varphi'(x) = 0$. Let

$$\psi := (\lambda_2 - \lambda_1)\beta IS + (\lambda_3 - \lambda_2)\rho I,$$

$$C(x) := \lambda_1 Q(x) + \lambda_2 B(x).$$

Then:

$$u(t) = \begin{cases} 
0, & \text{if } \psi \leq C'(0) \text{ at } t, \\
C'^{-1}(\psi) & \text{if } C'(0) < \psi \leq C'(u_{\max}) \text{ at } t, \\
u_{\max}, & \text{if } C'(u_{\max}) < \psi \text{ at } t,
\end{cases}$$

where $C'(x) := \frac{\partial}{\partial x} C(x) = \lambda_1 Q'(x) + \lambda_2 B'(x)$.

Combining (3.1.2), (3.2.2), (3.2.3) and (3.2.6) (or (3.2.8), depending on the concavity of $Q$ and $B$), we obtain a system of (non-linear) differential equations with boundary values that involve only the state $S, I, D$ and co-state $\lambda_1, \lambda_2, \lambda_3$ functions (and not the control $u$). $S, I, D, \lambda_1, \lambda_2, \lambda_3$ can therefore be obtained using standard numerical procedures that solve differential equations [33].

Now, the optimal control $u$ can be obtained using the above solutions in (3.2.6) (or (3.2.8), accordingly).

Note that, throughout this thesis, classical optimal control techniques do not provide the optimal control in closed form since the state dynamics (as in (3.1.2)) are non-linear, and the aggregate cost functions (as in (3.1.4)) are not necessarily quadratic.

### 3.3 Structural properties of optimum $u(t)$

We show that for concave $Q(\cdot), B(\cdot)$, the optimal $u(\cdot)$ is a *bang-bang* function of time, that is, at any given time, it is either at its minimum or maximum possible values, $0, u_{\max}$ respectively (theorem 3.3.2). Moreover, the number of jumps it exhibits between the extreme values is at most two.
We first state the lemma that we will use extensively hereafter. We appealed to it in section 3.2 (after eq. (3.2.5)).

**Lemma 3.3.1.** For \( t \in [0, T) \) we have \( \lambda_1 \geq 0, \lambda_3 \geq 0 \) and \((\lambda_2 - \lambda_1) > 0\).

Thus, also, \( \lambda_2 > 0 \). The lemma is consistent with the shadow reward interpretation of co-state functions: shadow rewards associated with susceptible, infective and dead nodes are positive from the malware’s point of view. Also, the infectives fetch at least as much shadow reward as the susceptibles.

**Proof.** Referring to (3.2.3), \( \lambda_3(T) = K_D \geq 0 \), and at any \( t \) at which \( u \) is continuous, \( \dot{\lambda}_3 = -\kappa_D \leq 0 \). Also, \( u \) and \( \lambda_3 \) are piecewise continuous and continuous functions of time respectively. Hence, (e.g. by integration) \( \lambda_3 \geq 0 \).

Next, let there exist an interval \([t_1, T)\) over which \((\lambda_2 - \lambda_1) \geq 0\). Then, we show that \( \lambda_1 \geq 0 \) for \( t \in [t_1, T) \). Referring to (3.2.2), over this interval, at any \( t \) at which \( u \) is continuous, we have:

\[
\dot{\lambda}_1 \leq Q(u_{\text{max}})\lambda_1.
\]

Therefore, from the continuity of \( \lambda_1 \), over this interval, \( \lambda_1(t) \geq \lambda_1(T) e^{Q(u_{\text{max}})(t-T)} \).

The result follows since \( \lambda_1(T) = 0 \). The entire lemma therefore follows if we show that \((\lambda_2 - \lambda_1) > 0\) for \( t \in [0, T) \), which we now set to do.

**Step-1.** We show that for some \( \delta > 0 \), \( \lambda_2(t) - \lambda_1(t) > 0 \) for \( t \in [T - \delta, T) \). Following (3.2.3), \( \lambda_2(T) = (\lambda_2(T) - \lambda_1(T)) = K_I \geq 0 \). If \( K_I > 0 \), the above holds due to continuity of \( \lambda_2 - \lambda_1 \). If \( K_I = 0 \) and \( \kappa_I > 0 \), it follows because \( 10 (\dot{\lambda}_2(T^-) - \dot{\lambda}_1(T^-)) = -\kappa_I - \rho u(T) K_D < 0 \).

**Step-2.** Let \( \lambda_2 - \lambda_1 \leq 0 \) at some \( t \in [0, T) \). Then there exists \( t^* \) such that

\[
\text{for } t^* < t < T : \lambda_2(t) > \lambda_1(t), \text{ and } \lambda_2(t^*) = \lambda_1(t^*). \quad (3.3.1)
\]

Thus, \( \lambda_1 \geq 0 \) for \( t \in [t^*, T) \).

\[
(\dot{\lambda}_2(t^+) - \dot{\lambda}_1(t^+)) = -\kappa_I - \frac{\varphi(u)}{I} - \lambda_1 \frac{Q(u)S}{T} - \lambda_1 Q(u). \quad (3.3.2)
\]

\(^{10}f(t_0^+) \triangleq \lim_{t \to t_0^+} f(t) \) and \( f(t_0^-) \triangleq \lim_{t \to t_0^-} f(t) \).
Recall that $\varphi(u) \geq 0$. Thus, as $\kappa_I > 0$, it follows from lemma 3.1.1 that $\dot{\lambda}_2(t^+)-\dot{\lambda}_1(t^+) < 0$. Since $u$ is piecewise continuous, $\lambda_2(t) - \lambda_1(t)$ is differentiable in $(t^*, t^* + \delta)$ for some $\delta > 0$. Thus, $\dot{\lambda}_2(t) - \dot{\lambda}_1(t) < 0$ for all $t \in (t^*, t^* + \delta)$ for some $\delta > 0$. Referring to (3.3.1) and the continuity of $\lambda_2(t) - \lambda_1(t)$, this contradicts the Mean value theorem. Therefore, $\lambda_2 - \lambda_1 > 0$ for all $[0, T)$.

We consider concave $Q$ and $B$ functions in this section. From (3.2.6), at any $t$ at which $u$ is continuous,

$$\frac{\dot{\varphi}(u_{\text{max}})}{I} = B(u_{\text{max}})\kappa_I + \kappa_I \rho u_{\text{max}} - \kappa_D \rho u_{\text{max}}$$

$$- S\beta \kappa_I u_{\text{max}} - Q(u) S\beta \lambda_2 u_{\text{max}}$$

$$+ Q(u_{\text{max}}) S\beta \lambda_2 u - B(u) \lambda_3 \rho u_{\text{max}}$$

$$+ B(u_{\text{max}}) \lambda_3 \rho u + B(u) S\beta \lambda_1 u_{\text{max}}$$

$$- B(u_{\text{max}}) S\beta \lambda_1 u.$$  

If both $Q, B$ are linear, then

$$Q(u_{\text{max}})u - Q(u)u_{\text{max}} \equiv 0, \text{ and } B(u_{\text{max}})u - B(u)u_{\text{max}} \equiv 0.$$  

The above also holds if either $Q$ or $B$ is strictly concave as then $u(t) \in \{0, u_{\text{max}}\}$ at each $t$. Thus, at any $t$ at which $u$ is continuous,

$$\frac{\dot{\varphi}(u_{\text{max}})}{I} = \kappa_I (B(u_{\text{max}}) + \rho u_{\text{max}} - S\beta u_{\text{max}}) - \kappa_D \rho u_{\text{max}}.$$  

From (3.1.2), lemma 3.1.1 and since $S$ is a continuous function, $S$ is also a non-increasing function of time. Hence, as $\kappa_I > 0$, $\frac{\dot{\varphi}(u_{\text{max}})}{I}$ is a non-decreasing function of time, ignoring its values at the (finite number of) discontinuity points of $u$. Also, $S$ is constant in any interval in which $\dot{\varphi}(u_{\text{max}}) = 0$. Thus, from (3.1.2) and lemma 3.1.1 and since $Q(x) \neq 0$ if $x \neq 0$, $u = 0$ in any such interval except at the discontinuity points of $u$.

Also, from (3.2.5),

$$\varphi(u_{\text{max}})|_T = K_I \beta u_{\text{max}} I(T) S(T) - B(u_{\text{max}}) K_I I(T) + (K_D - K_I) \rho u_{\text{max}} I(T).$$  

(3.3.4)
We are now ready to prove the following theorem:

**Theorem 3.3.2.** Let $Q$ and $B$ be concave. Then for any optimal $u$, there exists $t_1, t_2$ such that $0 \leq t_1 \leq t_2 \leq T$, and

- $u(t) = u_{\text{max}}$ for $0 \leq t < t_1$ (blitz phase);
- $u(t) = 0$ for $t_1 < t < t_2$ (stealth phase);
- $u(t) = u_{\text{max}}$ for $t_2 < t \leq T$ (slaughter phase).

If $K_I = K_D = 0$, $t_2 = T$, i.e., the slaughter phase does not exist.

**Proof.** (a) First, in any interval in which $\varphi(u_{\text{max}}) = 0$, $\dot{\varphi}(u_{\text{max}}) = 0$, and hence $u = 0$ except at the discontinuity points of $u$. (b) Next, consider an interval in which $\varphi(u_{\text{max}}) \leq 0$. Since $\frac{\dot{\varphi}(u_{\text{max}})}{I}$ is non-decreasing (ignoring finite number of points), and since $I > 0$ (from lemma 3.1.1) either the interval can be divided in (i) two subintervals such that $\varphi(u_{\text{max}}) = 0$ in one, and $\varphi(u_{\text{max}}) < 0$ in the other, (ii) or three subintervals such that $\varphi(u_{\text{max}}) < 0$ in the intermediate and $\varphi(u_{\text{max}}) = 0$ in the boundary ones. Now, from (a) and (3.2.6), $u = 0$ throughout the interval (except at its discontinuity points) in both cases.

Now, first let $\varphi(u_{\text{max}})|_T \leq 0$. From (3.3.4), this case, for example, arises when $K_I = K_D = 0$. Again, arguing as in (b), if $\varphi(u_{\text{max}})|_{t'} > 0$, for some $t' \in (0, T)$, then $\varphi(u_{\text{max}})|_t > 0$ for all $t < t'$. The lemma now follows from (b) and (3.2.6), with $t_2 = T$ and $t_1 = \inf\{t : \varphi(u_{\text{max}})|_{t'} \leq 0 \forall t' \geq t\}$.

Next, let $\varphi(u_{\text{max}})|_T > 0$. Let $t_2 = \inf\{t : \varphi(u_{\text{max}})|_{t'} > 0 \forall t' > t\}$. If $t_2 = 0$, the lemma follows from (3.2.6), with $t_1 = 0$. Otherwise, $\varphi(u_{\text{max}})|_{t_2} = 0$. The lemma now follows arguing as in the previous case for $[0, t_2]$ rather than $[0, T]$, and with $t_1 = \inf\{t \leq t_2 : \varphi(u_{\text{max}})|_{t'} \leq 0 \forall t' \in [t, t_2]\}$. □

Thus, the malware’s activity can be divided into (at most) three distinct phases: an initial *blitz*, an intermediate *stealth* and a final *slaughter* phase. In the blitz phase, infectives use the maximum power to spread the infection as aggressively as possible. During this period, owing to the higher initial number of susceptibles the benefit of using the maximum power for spreading the...
infection prevails over its harms (higher risk of detection and battery-drainage of the infectives). Subsequently, that is, after a desired number of infectives have been amassed, and the number of susceptibles diminished accordingly, the infectives operate in the stealth mode, altogether ceasing the spreading effort, but instead furtively performing other malicious activities such as eavesdropping, analyzing and altering the sensed data, sabotaging routes, etc. The spreading effort is eschewed during this period as it merely results in easier detection and early depletion of the infective nodes’ batteries rather than substantially enhancing the infection level owing to the depletion of the susceptibles in the earlier phase. Finally, the media access activities are resumed with the maximum power in the slaughter phase, but this time the primary goal is to kill the infectives by depleting their batteries. If however the malware does not gain from enhancing the final tally of the infective and dead nodes, i.e., \( K_I = K_D = 0 \), then the final slaughter phase is eliminated.

**Remark 3.3.1.** The simplicity of the optimum attack strategies is conducive to their implementation using resource constrained devices. Before the attack is launched, the attacker estimates the network parameters (e.g., \( \beta, \rho, Q(\cdot), B(\cdot) \)), the damage coefficients (\( \kappa_I, K_I, \kappa_D, K_D \)) and the initial fraction of infectives \( I_0 \) before the immunization and healing would start. Using the above, it computes the jump points \( t_1, t_2 \) by solving a system of differential equations, as described in the last paragraph of Section 3.2. Note that existing efficient numerical algorithms [33] can solve differential equations very fast, and the computation time is constant in that it does not depend on the number of nodes. The jump points are subsequently incorporated in the code of the malware. The infected devices can execute the attack strategies without any further global coordination or information exchange.

**Theorem 3.3.3.** For concave \( Q, B \), if \( \kappa_D \geq \gamma \kappa_I \) and \( K_D \geq \gamma K_I \), where

\[
\gamma = (1 + B(u_{\text{max}})/\rho u_{\text{max}}),
\]

the optimal \( u \) is \( u_{\text{max}} \) throughout \([0, T]\).
Proof. Using the conditions in the theorem, it follows from (3.3.3) and (3.3.4) that $\dot{\phi} < 0$ at any $t$ at which $u$ is continuous and $\varphi(u_{\text{max}})|_T > 0$. This is because $I, S > 0$ (from lemma 3.1.1) and $\beta, \kappa_I > 0$. Since $u$ and $\varphi(u_{\text{max}})$ are respectively piecewise continuous and continuous functions of time, $\varphi(u_{\text{max}}) > 0$ at all $t$. The theorem follows from (3.2.6).

When $K_D \gg K_I$ and $\kappa_D \gg \kappa_I$, the malware gains significantly more from dead nodes than from infectives. Nevertheless, choosing $u = u_{\text{max}}$ facilitates detection of the malware leading to faster immunization of the susceptibles and depletes infectives’ batteries faster. Both the above may slow down the spread of the infection and thereby reduce the number of dead nodes. The optimality of this extreme choice is therefore somewhat surprising.

Remark 3.3.2. So far, we assumed that $Q(0) = B(0) = 0$. This is the case when detection based on media access activity of the infectives is crucial in the countermeasures. Using similar analysis, we can generalize theorem 3.3.2 to allow for $Q(0) > 0$, i.e., when even without any media access activity of the malware, susceptibles are immunized. Theorem 3.3.3 can also be generalized to the case in which $Q(0) > 0$ and $B(u) = \text{constant} \leq Q(0)$, i.e., the healing is not affected by the media access activity of the malware. The latter assumption ($B \leq Q(0)$) usually holds in practice as fetching more complex, and frequently larger, security patches required for healing incurs larger delays.

### 3.4 Numerical computations

We investigate the nature of the optimal dynamic attack policies and the damage they inflict for different values of network and attack parameters. We also compare the efficacy of the optimal dynamic and static controls. In a static policy, in contrast to a dynamic policy, the value of $u(t)$ is fixed throughout the period of the attack. The optimal static policy is computed by selecting the above fixed value as the one that maximizes the damage among choices in the interval $[0, 1]$. We use $\rho = 0.0892$ and the damage function in (3.1.4) with $\kappa_I = 10, \kappa_D = 0, K_I = 0$ $K_D = 50$ and
\( T = 40 \). We consider concave \( Q, B \), i.e., \( Q(u) = 0.0446 + 0.0223u \) and \( B(u) = 0.0446\pi + 0.0223u \), with \( \pi \in \{0, 1\} \), except for fig. 3.3(a) and 3.3(b) where \( Q, B \) are strictly convex: \( Q(u) = 0.0446 + 0.0223u^{3/2} \) and \( B(u) = 0.0446\pi + 0.0223u^{3/2} \).

In fig. 3.2(a) and 3.2(b), we have depicted both the optimal controls and the fraction of infectives as functions of time for different values of \( \beta \). In figures 3.2(c) and 3.2(d), we have depicted the above for different values of \( I_0 \). Note that for \( \pi = 1 \), unlike for \( \pi = 0 \), the level of infection drops during the interval of \( u = 0 \), as \( B(0) > 0 \) in the former case. Also, for both \( \pi \in \{0, 1\} \), the evolution of the level of infection indicate that the initial \( u = u_{\text{max}} \) phase is primarily aimed at the spread of the malware and the final \( u = u_{\text{max}} \) phase chiefly increases the final tally of the dead. Fig. 3.2(c) and 3.2(d) reveal that the initial phase is shorter for higher \( I_0 \), however, the final killing phase is less affected by varying \( I_0 \). The optimum control have two jumps in all the above, even for \( \pi = 1 \) and \( B(\cdot) \neq \text{constant} \). Recall that the structure of the optimal control in the latter case, as also when \( B, Q \) are strictly convex, is not predicted by any of our theorems and their generalizations, namely Remark 2. As fig. 3.3(a) and 3.3(b) reveal, the optimal controls for strictly convex \( B \) and \( Q \), are similar to those for concave \( Q \) and \( B \) (fig. 3.2(a) and 3.2(b)) except that the transitions between different phases are continuous rather than abrupt.

Fig. 3.4 and Fig. 3.5 show that the optimal dynamic attack policy yields higher damages than the optimal static choice of \( u \). The differences are significant for \( \pi = 0 \).

We have so far assumed that the malware computed the optimum attack strategies assuming full knowledge of the network parameters. However, an attacker may only have a rough estimate of the values of the parameters. Here, we investigate the impact of this inaccuracy on the efficacy of the attack. First, we derive the optimal dynamic and static controls assuming certain values for network parameters. Then we apply the same (dynamic and static, resp.) policies to a network in which the real value of one parameter (e.g., \( \beta \)) is different from the assumed value. Then we plot the amount of reduction in the total damage due to applying these sub-optimal policies as a function of the assumed (i.e., estimated) value of the parameter in question. The reduction is
Figure 3.2: Optimal controls and the corresponding levels of infection for different $\beta, I_0, \pi$. In figs (a) and (b), $I_0 = 0.1$, and in figs (b), (c), $\beta = 0.446$. In each, the plots that are always below 0.4 represent $I(\cdot)$. In figs (a), (b) ((c), (d), resp.) the higher infection levels are for the larger $\beta$’s ($I_0$’s, resp.).

Figure 3.3: Optimal controls and the corresponding levels of infection for different $\beta, \pi$ for strictly convex $Q, B$. Here, $I_0 = 0.1$. The plots that are always below 0.4 represent $I(\cdot)$. The higher infection levels are for the larger $\beta$’s.
Figure 3.4: Comparison of the damages for optimal dynamic and static policies for different $\beta, \pi$. Here $I_0 = 0.1$.

Figure 3.5: Comparison of the damages for optimal dynamic and static policies for different $I_0, \pi$. Here $\beta = 0.446$. 
the difference between the damages inflicted by the sub-optimal policy (the dynamic and static optimal control calculated based on the inaccurate estimate of the parameter under consideration) and the optimal (dynamic) policy for the accurate value of that parameter. As fig. 3.6(a) shows, the damage reduction due to inaccurate estimation of $\beta$ is insignificant for the dynamic policy. Also, the dynamic policy calculated based on the inaccurate estimate inflicts significantly higher damages than the static policy calculated using the same estimate - thus the dynamic policy retains its advantage over the static even in presence of estimation errors. Similar calculations for varying $Q$ and $B$ suggest the same behavior (figures 3.6(b) and 3.6(c) respectively). Optimal dynamic policies are therefore robust to errors in the estimation of the parameters of the network - yet another negative result from the defence point of view.

![Graphs showing reduction in aggregate damage due to incorrect estimations of network parameters](image)

(a) Incorrect estimation of $\beta$

(b) Incorrect estimation of $q$

(c) Incorrect estimation of $b$

Figure 3.6: Reduction in the aggregate damage due to incorrect estimations of network parameters by the malware. The real values of the parameters are $I_0 = 0.1, \beta = 0.446, Q(u) = 0.0446 + qu, B(u) = 0.0446\pi + bu, q = b = 0.0223$. 

39
Chapter 4

Seek and Destroy Attack

Introduction

In Chapter 3, we investigated our first attack model. In this chapter, we consider our alternative attack: seek and destroy. In this setting, similar to the battery depletion attack, the malware can use an infective node as long as its remaining battery is not exhausted. Unlike the battery depletion attack, though, the malware can kill an infective node whenever it decides to by invoking pernicious codes that inflicts irretrievable hardware or software damage and make the node completely dysfunctional. The malware thus selects the transmission gains and media access rates so that the battery reserves last during the period of the infection. Hence the transmission range of the infective nodes and the rate of killing constitute separate dynamic control functions of the worm which are then jointly optimized to inflict the maximum damage.

At each moment of time the worm at each node faces the following decisions: (i) choosing the transmission ranges and media scanning rates so as to maximize the spread of infection subject to not exhausting its batteries by the end of the operation interval; and (ii) whether to kill the node to inflict a large cost on the network, however at the expense of losing the chance of infecting more susceptible nodes at later times. We mathematically formulate the decision problems and utilize
Pontryagin Maximum Principle to investigate joint optimal strategies of the attacker over time. We prove that the optimal killing rate is bang-bang but with at most one jump, which culminates at the maximum value. In other words, until a certain time (which can be zero depending on the network and counter-measure parameters), the worm does not kill any host, and right after that, it annihilates its hosts at the maximum possible rate until the end of the optimization period. We also prove that the worm’s optimal energy consumption rate is a decreasing function of time. Thus, the worm seeks to infect as many hosts as possible early on by selecting the maximum possible values of the media scanning rates and transmission ranges, and thereafter starts to behave more conservatively so as to prevent losing the nodes due to battery depletion. The transition between the battery intensive phase and the battery-conservative phase is continuous when the energy consumption costs are strictly convex, and is abrupt when it is concave. Therefore, the joint optimal controls portray a two-phases attack, in the first phase the malware amasses the infectives and then it slaughters them in the second phase. The result carries a qualitative cautionary message for defenders: an apparently inoffensive malware with little disruptive behavior might well be stacking infective hosts for the imminent carnage.

4.1 System model

4.1.1 Dynamics of state evolution

The dynamics of the infection propagation is similar to the battery depletion attack model discussed in §3.1. Specifically, at any given time the rate of contacts between infective and susceptible nodes is linearly proportional to the media access rate of the infective nodes, $u(t)$, where $u(t)$ is a (dynamic) parameter of control of the malware. In what follows we elucidate the differences in the current setting, which are in the death and recovery processes.

In this case the worm at an infective node can kill the host (by invoking specific codes which inflicts irretrievable hardware or software damage on the host) at rate $\nu(t)$, which is an indepen-
dent dynamically controlled parameter of the worm.

The security patches are installed at an infective (susceptible, respectively) and transformed them into recovered. The rates of installation at any given time \( t \) are \( B(I(t)) \) and \( Q(S(t)) \), for infectives and susceptibles respectively, where \( B(\cdot) \), \( Q(\cdot) \) are arbitrary functions that satisfy the following mild assumptions: \(1 \lim_{x \to 0} B(x) \), \( \lim_{x \to 0} Q(x) \) are finite, and for \( 0 < x < 1 \), \( B(x) \), \( Q(x) \) are positive and differentiable, \( xB(x) \) is a concave non-decreasing function of \( x \) and \( xQ(x) \) is a non-decreasing function of \( x \). These rates are associated with delays in detection of infection and fetching the appropriate security patch, etc. These rates are associated with delays in detection of infection and fetching the appropriate security patch. Note that the functions \( B(\cdot) \) and \( Q(\cdot) \) are likely to be constants (e.g., \( B(x) = B_0 \), \( Q(x) = Q_0 \) for all \( x \)) in practice\(^2\), and any constant function satisfies all of the above properties. Nevertheless, we allow more general functions (such as \( Q(x) = x^\alpha \) for \( \alpha > -1 \) and \( B(x) = x^\alpha \) for \( -1 < \alpha < 0 \)) so as to accommodate more general scenarios.

Let

\[ \beta = \lim_{N \to \infty} N \hat{\beta}, \quad q(S) = Q(S)S, \quad b(I) = B(I)I. \]

Our discussions lead to\(^3\) the following system of differential equations representing the dynamics of the system:

\[
\begin{align*}
\dot{S}(t) &= -\beta u(t)I(t)S(t) - q(S(t)) & S(0) &= 1 - I_0 \\
\dot{I}(t) &= \beta u(I)S(t) - b(I(t)) - \nu(t)I(t) & I(0) &= I_0 \\
\dot{D}(t) &= \nu(t)I(t) & D(0) &= 0.
\end{align*}
\]

\(^1\)In a more general form, the immunization and healing rates may depend on the media access activities of the worm as well, as in the previous chapter. However, we derive our analytical results in the absence of such dependencies.

\(^2\)This is because the users are likely to receive the security patches from software stores or servers distributed in the area. In the first case, the rates are naturally constants. In the latter case, the reception rates of the patches depend on the host’s reception gains, servers’ transmission gains, etc.; and none of the above depend on the infective and susceptible fractions.

\(^3\)Refer to Appendix A for more details.
Figure 4.1: Transitions. S, I, R, D respectively represent fraction of the susceptible, infective, recovered and dead. $u(t)$ and $v(t)$ are the control parameters of the malware.

and also satisfy the following constraints at all $t$:

\begin{align}
0 &\leq S(t), I(t), D(t) & (4.1.2a) \\
S(t) + I(t) + D(t) &\leq 1. & (4.1.2b)
\end{align}

Fig. 4.1 illustrates the transitions between different states of nodes. Owing to the technical assumptions we made on $B(.)$ and $Q(.)$, the functions $b(.), q(.)$ exhibit the following properties: $b(0) = q(0) = 0$, and for $0 < I < 1, 0 < S < 1$ we have $b(I), q(S) > 0$, $b'(I) = db/dI \geq 0$, $q'(S) = dq/dS \geq 0$, and $b''(I) = d^2b/ dI^2 \leq 0$.

4.1.2 Maximum damage seek and destroy attack

As in the battery depletion attack model, we consider an attack that seeks to inflict the maximum possible damage in a time window $[0, T]$ of its choice. Although conceptually the same, we consider slightly different damage functions in this section. An attack can benefit over time from the infected hosts, by using the worms to (i) eavesdrop and analyze traffic that is generated or relayed by the infected hosts, or the traffic that traverses in the hosts’ vicinity, and (ii) alter or destroy the traffic that is generated or relayed by the infected hosts. An attacker also benefits by inflicting a large death-toll by the end of the desired time window. These motivate the following
damage function:

\[ J = \kappa D(T) + \int_0^T f(I(t)) \, dt, \]  

(4.1.3)

where \( \kappa \) is an arbitrary non-negative constant, and \( f(.) \) is an arbitrary non-decreasing, convex function such that \( f(0) = 0 \). Note that the assumptions on \( \kappa, f(.) \) are mild and natural, and a large class of functions, e.g., \( f(I) = K I^\alpha \) for \( \alpha \geq 1 \) and \( K \geq 0 \), \( f(I) = K(e^{\alpha I} - 1) \) for \( \alpha, K \geq 0 \) satisfy them. Finally, an attacker that simply seeks to maximize the final tally of the dead without any other agenda is readily representable by taking \( f \equiv 0 \).

| \( \nu(t) \) | the rate of killing the infectives |
| \( u(t) \) | the transmission range times the scanning rate of the infectives |

Table 4.1: Control variables of the worm.

The attacker seeks to maximize the aggregate damage by appropriately regulating its killing rate, \( \nu(t) \), and the product of the transmission range and the scanning rate of the infective nodes, \( u(t) \), (Table 4.1), subject to:

\[ 0 \leq \nu(t) \leq \nu_{\text{max}} \quad 0 \leq u_{\text{min}} \leq u(t) \leq u_{\text{max}} \]  

(4.1.4a)

\[ \int_0^T h(u(t)) \, dt \leq C. \]  

(4.1.4b)

The bound on \( \nu(t) \) is imposed by limitations on the worm’s speed of killing an infective host. The bounds on \( u(t) \) are dictated by the physical constraints of the transmitters and also for ensuring that the interference and hence collisions between simultaneous transmissions remain limited. The second constraint (4.1.4b) -referred to as the battery constraint- arises because enhancing \( u(t) \) depletes the infective’s battery, and the worm wants to ensure that the infective’s battery lasts and it can continue to use it and to infect susceptibles for the time period of its operation \([0, T]\) 

\[4\text{The attacker naturally does not control any other parameter such as the susceptible’s reception gain, server’s transmission gains, mobility patterns, immunization and healing rate functions, } Q(\cdot) \text{ and } B(\cdot) \text{ etc.} \]
(should it choose not to kill the host earlier). For appropriate functions, \( h(\cdot) \) (e.g., \( h(u) = K_1 u^r \), for \( r \geq 2 \)), \( \int_0^T h(u(t)) \, dt \) is the energy consumed by the host if it is infected at \( t = 0 \) and is not killed before \( t = T \) - this is therefore an upper bound on the energy consumption of any infective while it remains infected. We assume that the energy consumption in media scanning and malware transmission by the infective nodes is much larger than the energy expenditure as a result of other activities of the nodes, and therefore, the energy consumed by a host before it is infected is relatively insignificant. Thus, the worm chooses \( u(t) \) so that the above upper bound does not exceed its maximum energy reserve, \( C \).

It is natural to assume that \( h(u) \) is non-decreasing and non-negative. We allow \( h(u) \) to be either convex or concave for \( 0 \leq u \leq u_{\text{max}} \). Note that when \( h(u) \) represents power dissipation associated with \( u \), \( h(u) \) must be \( K_1 u^r \), for \( r \geq 2 \) and some non-negative \( K_1 \), and is therefore convex. But, if \( h(u) \) represents a cost associated with power dissipation, then it may be concave as well. Finally, without loss of generality, \( h(u_{\text{min}}) = 0 \), because if \( h(u_{\text{min}}) > 0 \), we can equivalently consider \( h(u_{\text{min}}) = 0 \), and reduce the bound \( C \) appropriately. Any pair of piecewise continuous functions \((\nu, u) : [0,T] \rightarrow \mathbb{R}^2\) such that the left and right hand limits exist and that satisfy the above constraints belongs to the control region denoted by \( \Omega \).

We next show that for any \((\nu, u) \in \Omega \), the state constraints in (4.1.2) are automatically satisfied throughout \((0 \ldots T]\). Thus, we ignore (4.1.2) henceforth.

**Lemma 4.1.1.** For any \((\nu, u) \in \Omega \), the state functions \((S, I, D) : [0,T] \rightarrow \mathbb{R}^3\) that satisfy the state equations and initial states in (4.1.1), also satisfy the state constraints in (4.1.2). Moreover, \( S(t) \geq (1 - I_0) e^{-K_1 t} > 0 \), \( I(t) \geq I_0 e^{-K_2 t} > 0 \) for \( t \in [0,T] \) and some finite \( K_1, K_2 \).

The proof, coming next, reveals that

\[
K_1 = \beta u_{\text{max}} + \max_{0 \leq x \leq 1} q'(x), \quad K_2 = \max_{0 \leq x \leq 1} b'(x).
\]

**Proof.** All \( S, I \) and \( D \), resulting from (4.1.1), and thus any continuous functions of them, are continuous functions of time. We first show that if there exists \( t_0 \) such that we have \( 0 < S, I \)
throughout \((0, t_0)\), then \(S(t_0) \geq S(0)e^{-K_1t_0}\), where \(K_1 = \beta u_{\max} + \max_{0 \leq x \leq 1} q'(x)\), and \(I(t_0) \geq I(0)e^{-K_2t_0}\), where \(K_2 = \max_{0 \leq x \leq 1} b'(x)\). The second statement will now follow if we can prove the first and since \(0 < S(0) = 1 - I(0) < 1\). Now, let \(0 < S, I\) throughout \((0, t_0)\). For \(0 \leq t < t_0\) from (4.1.1a) we have \(\dot{S} \geq -\beta uS - q(S) \geq -K_1 S\). Hence, \(S(t) \geq S(0)e^{-K_1t} \geq S(0)e^{-K_1t_0}\) for all \(0 \leq t < t_0\). Since \(S\) is continuous, \(S(t_0) \geq S(0)e^{-K_1t_0}\). Similarly, we can show that \(I(t_0) \geq I(0)e^{-K_2t_0}\). The result follows.

We now prove the first statement. Since \(0 < I_0 < 1\), the initial conditions in (4.1.1) ensure that the state constraints (4.1.2) are strictly met at \(t = 0\). The continuity of \(S\) and \(I\) functions ensure that there exists an interval of nonzero length starting at \(t = 0\) on which both \(S\) and \(I\) are strictly positive. Thus, from (4.1.1c) and since \(\nu(t) \geq 0\), \(\dot{D} \geq 0\) in the above interval. Thus, since \(D(0) = 0\), \(0 \leq D\) in this interval as well. Since \(\frac{d}{dt}(S + I + D)|_{t=0} = -q(S_0) - b(I_0) < 0\) and \(S(0) + I(0) + D(0) = 1\), there exists an interval after \(t = 0\) over which the constraint in (4.1.2b) is strictly met.

Suppose the first statement does not hold. Now, let \(t_0 \leq T\) be the first time after \(t = 0\) at which, at least one of the constraints of \(0 \leq S, I\) and \(S + I + D \leq 1\) becomes active, or \(0 \leq D\) becomes violated right after it. That is, at \(t_0\), we have (1) \(S = 0\) OR (2) \(I = 0\) OR (3) \(S + I + D = 1\) OR (4) there exists an \(\epsilon > 0\) such that \(D < 0\) on \((t_0 \ldots t_0 + \epsilon)\); AND throughout \((0, t_0)\), we have \(0 < S, I\) and \(S + I + D < 1\) and \(D \geq 0\). Thus, from the first para in this proof, \(S(t_0) \geq S(0)e^{-K_1t_0} > 0\), \(I(t_0) \geq I(0)e^{-K_2t_0} > 0\). Thus, since \(S(0) > 0\), \(I(0) > 0\), neither (1) nor (2) could have happened.

Let \(P_1 = S(0)e^{-K_1t_0}, P_2 = I(0)e^{-K_2t_0}\). Also, \(\frac{d}{dt}(S + I + D) = -q(S) - b(I) \leq -q(P_1) - b(P_2) < 0\) throughout \([0 \ldots t_0]\). Since \(S(0) + I(0) + D(0) = 1\) we have \((S + I + D)|_{t=t_0} < 1\), showing that (3) is impossible. Moreover, from (4.1.1a), and since \(I(t_0) > 0\), and \(I\) is continuous, there exists an \(\epsilon'\) such that \(\dot{D} \geq 0\) over \((t_0 \ldots t_0 + \epsilon')\). From continuity of \(D\), \(D(t_0) \geq 0\). Thus, \(0 \leq D\) over \((t_0 \ldots t_0 + \epsilon')\), dismissing the possibility of (4). This negates the existence of \(t_0\). Thus, the first statement holds by contradiction. □
Once the control \((\nu, u)\) is selected, the system state vector \((S, I, D)\) is specified at all \(t\) as a solution to (4.1.1) and hence the value of the damage function \(J\) is determined as well. Thus, the control \((\nu, u)\) is considered only as a function of time rather than that of the system states, and since the value of \(J\) is determined only by the selection of \((\nu, u)\), we will henceforth denote \(J\) as \(J(\nu, u)\) instead.

The state and control functions pair \(((S, I, D), (\nu, u))\) is called an admissible pair if (i) \((\nu, u)\) is in \(\Omega\), i.e. satisfies (4.1.4), (ii) \((\nu, u)\) is continuous except for possibly finite number of time epochs such that the left and right hand limits exist at the points of discontinuity, and (iii) equations in (4.1.1) hold. The function \((\nu, u)\) is then called an admissible control. Let \(((S, I, D), (\nu, u))\) be an admissible pair. If

\[
J(\nu, u) \geq J(\nu, u) \quad \text{for any admissible control } (\nu, u)
\]

then \(((S, I, D), (\nu, u))\) is called an optimal solution and \((\nu, u)\) is called an optimal control of the problem.

### 4.2 Worm’s optimal control

We now present a framework using which the worm can determine its optimal control functions \((\nu, u)\) and also compute the maximum value of the damage function.

The main challenge in computing the optimal control is that the differential equations (4.1.1) can be solved provided that the functions \((\nu, u)\) are known. Thus, the only approach seems to be that of an exhaustive search on all functions \((\nu, u)\) in \(\Omega\). This will require the evaluation of the damage function \(J(\nu, u)\) for each pair of such functions where the corresponding \((I, D)\) functions required in evaluating \(J(\nu, u)\) are obtained by solving (4.1.1) for each such pair. But, \(\Omega\) consists of an uncountably infinite number of such pairs, which rules out an exhaustive search. Pontryagin’s Maximum Principle, however, provides an elegant tool for solving this seemingly impossible problem, which we apply next.
First, we introduce a new state variable $E$ to transform the constraint in (4.1.4b) to a more treatable one:

$$\dot{E}(t) = -h(u), \quad E(0) = 0, \quad (4.2.1)$$

with the final constraint:

$$E(T) \geq -C. \quad (4.2.2)$$

Now, note that (4.2.1) and (4.2.2) are together equivalent to (4.1.4b). Thus, the optimal control problem posed in § 4.1 can now be modified to augment (4.1.1) with (4.2.1) and (4.2.2), and omit (4.1.4b), without any alterations in the set of optimal solutions and in the maximum value of the damage function. We consider this version henceforth.

Let $((S, I, D), (\nu, u))$ be an optimal solution. Consider the Hamiltonian $H$, and co-state or adjoint functions $\lambda_1(t)$ to $\lambda_4(t)$, and a scalar $\lambda_0 \geq 0$ defined as follows:

$$H := \lambda_0 f(I) + (\lambda_2 - \lambda_1)\beta u IS - \lambda_1 q(S) - \lambda_2 b(I)$$

$$+ (\lambda_3 - \lambda_2) v I - \lambda_4 h(u). \quad (4.2.3)$$

$$\dot{\lambda}_1 = -\frac{\partial H}{\partial S} = -(\lambda_2 - \lambda_1)\beta u I + \lambda_1 q'$$

$$\dot{\lambda}_2 = -\frac{\partial H}{\partial I} = -\lambda_0 f' - (\lambda_2 - \lambda_1)\beta u S + \lambda_2 b' - (\lambda_3 - \lambda_2) v$$

$$\dot{\lambda}_3 = -\frac{\partial H}{\partial D} = 0$$

$$\dot{\lambda}_4 = -\frac{\partial H}{\partial E} = 0. \quad (4.2.4)$$

along with the transversality conditions:

$$\lambda_1(T) = 0, \quad \lambda_2(T) = 0, \quad \lambda_3(T) = \lambda_0 \kappa \quad (4.2.5a)$$

$$\lambda_4(T) \geq 0 \quad (4.2.5b)$$

$$\lambda_4(T)(E(T) + C) = 0. \quad (4.2.5c)$$

Then according to Pontryagin’s Maximum Principle With Terminal Constraints ([24, P.111 theorem 3.14]), there exist continuous and piecewise continuously differentiable co-state functions...
\( \lambda_1, \lambda_2, \lambda_3 \) and \( \lambda_4 \), and constant \( \lambda_0 \geq 0 \) that at every point \( t \in [0 \ldots T] \) where \((\nu(.),u(.))\) is continuous, satisfy (4.2.4) and the transversality conditions (4.2.5), and we have:

\[
\vec{\lambda} \not\equiv \vec{0} \quad (4.2.6a)
\]

\[
(\nu,u) \in \arg \max_{(\vec{\nu},\vec{u}) \in \Omega} H(\vec{\lambda},(S,I,D),(\nu,u)) \quad (4.2.6b)
\]

Referring to (4.2.4), \( \dot{\lambda}_4 = 0 \) and thus, \( \lambda_4 \) is a constant, which, according to (4.2.5), is nonnegative. Now assume that \( \lambda_4 > 0 \), then by scaling the Hamiltonian and the co-states by \( 1/\lambda_4 \), the equations are still satisfied with \( \lambda_4 = 1 \). Thus if \( \lambda_4 > 0 \), we can take \( \lambda_4 = 1 \) without loss of generality. The case for \( \lambda_4 = 0 \) can be handled very easily and is discussed in sections 4.4.1,4.4.2 as remarks.

Here, we show that \( \lambda_0 = \text{constant} > 0 \). This is because if otherwise \( \lambda_0 = 0 \) then (4.2.4) for \((\lambda_1,\lambda_2,\lambda_3)\) constitutes a linear autonomous ODE with the final constraint of \((\lambda_1,\lambda_2,\lambda_3)(T) = \vec{0} \) which from vector space theory [33], has the unique solution of \((\lambda_1,\lambda_2,\lambda_3)(t) = \vec{0} \). Also, from (4.2.4) and (4.2.5b), \( \lambda_4 \) is a non-negative constant. Thus, either \( \lambda_4 = 0 \) or \( \lambda_4 = \text{constant} > 0 \) for all \( t \). The case of \( \lambda_4 = 0 \) contradicts the necessary condition of \( \vec{\lambda} \not\equiv \vec{0} \) of (4.2.6a). Now consider the case of \( \lambda_4 = \text{constant} > 0 \) for all \( t \). The Hamiltonian in (4.2.3) reduces to \( H = -\lambda_4 h(u) \). Thus maximization of Hamiltonian leads to \( u(t) = u_{\text{min}} \) for all \( 0 \leq t \leq T \). This means \( \int_0^T h(u) \, dt < C \) or \( E(T) > -C \), and thus \( \lambda_4(T)(E(T) + C) > 0 \), which contradicts (4.2.5c). Therefore, \( \lambda_0 \) cannot be zero.

Define the switching function \( \varphi \) as follows:

\[
\varphi := (\lambda_3 - \lambda_2)I \quad (4.2.7)
\]

which is a continuous and piecewise continuously differential function of time and referring to (4.2.5), has the following final value:

\[
\varphi(T) = \lambda_0 \kappa I(T) > 0. \quad (4.2.8)
\]

The positivity comes from the facts \( \lambda_0 > 0, \kappa > 0 \), and \( I > 0 \) according to lemma 4.1.1. Also let \( \psi \)
be defined as follows:

$$\psi := (\lambda_2 - \lambda_1)\beta IS$$  \hfill (4.2.9)

which too is a continuous and differential function of time and according to (4.2.5) has zero final value:

$$\psi(T) = 0.$$  \hfill (4.2.10)

Introduction of \(\varphi\) and \(\psi\), along with \(\lambda_1 = 1\) allow us to rewrite the Hamiltonian in (4.2.3) as follows:

$$H = \lambda_0 f(I) - h(u) + \psi u - \lambda_1 q - \lambda_2 b + \varphi \nu.$$  \hfill (4.2.11)

According to Pontryagin’s Maximum Principle in (4.2.6b), we have:

$$H(S, I, D, \nu, u, \lambda_1, \lambda_2, \lambda_3) \geq H(S, I, D, \nu, u, \lambda_1, \lambda_2, \lambda_3)$$  \hfill (4.2.12)

over all admissible \(\nu, u\).

Hence, the optimal \(\nu\) satisfies \(\varphi \nu \geq \varphi \nu\), where \(\nu\) is any admissible controller, \(i.e., \nu \in [0 \ldots \nu_{\text{max}}]\).

Thus, to find the optimal controller, one needs to maximize the linear function \(\varphi \nu\) over the admissible set \(\nu \in [0 \ldots \nu_{\text{max}}]\), which yields:

$$\nu = \begin{cases} 
0, & \varphi < 0 \\
\nu_{\text{max}}, & \varphi > 0, 
\end{cases}$$  \hfill (4.2.13)

hence, the name switching function. An immediate observation of the above property is the following important property:

$$\varphi \nu \geq 0.$$  \hfill (4.2.14)

Also note that according to (4.2.8), \(\varphi(T) > 0\) and thus by continuity of \(\varphi\) and following (4.2.13), \(\nu = \nu_{\text{max}}\) over an interval of nonzero length toward the end of \((0 \ldots T)\) interval which extends until time \(T\).

Again, from (4.2.11) and according to (4.2.12), the optimal \(u\) satisfies \(\psi u - h(u) \geq \psi u - h(u)\), where \(u\) is any admissible controller, \(i.e., u \in [u_{\text{min}} \ldots u_{\text{max}}]\). Thus, to find the optimal \(u\), one
needs to maximize the function \( \psi u - h(u) \) over the admissible set \( u \in [0 \ldots u_{\text{max}}] \). We separately consider the cases of strictly convex \( h(\cdot) \) and concave \( h(\cdot) \):

**Strictly Convex** \( h(u) \) For a strictly convex \( h(u) \) we have \( \frac{d^2(\psi u - h(u))}{du^2} = -h''(u) < 0 \), thus the function \( \psi u - h(u) \) is strictly concave in \( u \) over the admissible interval and the maximizer is found by comparing the values of three candidates of \( u_{\min}, u_{\max} \) and the \( u \in (u_{\min} \ldots u_{\max}) \) at which the derivative of this expression becomes zero. This yields:

\[
\begin{align*}
u &= \begin{cases} 
  u_{\min}, & \psi \leq h'(u_{\min}) \\
  h^{-1}(\psi), & h'(u_{\min}) < \psi \leq h'(u_{\max}) \\
  u_{\max}, & h'(u_{\max}) < \psi. 
\end{cases}
\end{align*}
\]

(4.2.15)

This shows that \( u \) is a continuous function of \( \psi \), and thus according to the continuity of the \( \psi \), \( u \) is a continuous function of time. Therefore, the co-state functions are differentiable at every point at which the other control, \( i.e. \nu \), is continuous.

**Concave** \( h(u) \) For this case, \( \psi u - h(u) \) is convex in \( u \) and a maximizer \( u \) is found by comparing the only two candidates \( u_{\min} \) and \( u_{\max} \). This readily yields the following:

\[
u = \begin{cases} 
  u_{\min}, & \psi < \rho \\
  u_{\max}, & \psi > \rho. 
\end{cases}
\]

(4.2.16)

where

\[
\rho := \frac{h(u_{\max})}{u_{\max} - u_{\min}} \geq 0.
\]

For both strictly convex and concave \( h(u) \), referring to (4.2.10) and following (4.2.15)/(4.2.16), we have \( u(T) = u_{\min} \).

Implementing (4.2.13), (4.2.15)/(4.2.16) into (4.1.1), (4.2.4) and (4.2.5), we obtain a system of (non-linear) differential equations with specified initial or final values that involve only the state and co-state functions (and not the control \((\nu, u)\)). Functions \( \lambda_1 \) to \( \lambda_4 \) and scalar \( \lambda_0 \) that satisfy
the above differential equations and boundary values, can therefore be obtained using standard numerical procedures that solve differential equations [33]. Now, the optimal control \((\nu, u)\) can be obtained using the above solutions in (4.2.13) and (4.2.15)/(4.2.16).

### 4.3 Structure of the maximum damage attack

Whether in practice the worm can indeed inflict the maximum damages developed in this chapter depends on implementability of the optimal strategies. Specifically, if the optimal policies that inflict the maximum damage are complex to execute, then the worm may not be able to perform them since they are limited by the capabilities of their resource constrained hosts as well. Inauspiciously though, we show that optimal attack strategies follow simple structures (theorems 4.3.1,4.3.2) which make them conducive to implementation. Fig. 4.2 provides visualization of the theorems.

Recall that one of the basic trade-offs that the attacker were dynamically faced with was the perfect timing to kill an infective node. Specifically, should an attacker kill a node as soon as it is infected so as to have claimed a casualty and secured a large damage on the network? Theorem 4.3.1 states the opposite:

**Theorem 4.3.1.** Consider an optimal solution pair \((\nu, u)\) that jointly maximizes the worm’s damage function in (4.1.3) subject to the constraints in (4.1.4a) and (4.1.4b); then \(\nu(t)\) has the following characteristics:

\[\exists t_1 \in [0 \ldots T) \text{ such that } \nu(t) = 0 \text{ for } 0 < t < t_1 \text{ and } \nu(t) = \nu_{\text{max}} \text{ for } t_1 < t < T.\]

In words, an optimal \(\nu(\cdot)\) is of **bang-bang** form, that is, it possesses only two possible values \(\nu_{\text{max}}\) and 0, and switches abruptly between them. It has at most one such jump, which necessarily culminates at \(\nu_{\text{max}}\). Thus, the theorem says that although killing a node early on would ensure partial damage, the overall damage is more if this decision is deferred until toward the end of the attacking period despite the risk of recovery of the infective node by the system. Specifically, at the start of the outbreak, number of susceptibles is high and infective nodes can be used to further
propagate the infection. As time passes by, the level of susceptibles drops due to both spread of infection and immunization effort by the system. At a certain threshold, the risk of recovery of the infective nodes in the remaining time outweigh the potential benefit by spreading the infection. At this point, whose exact value depends on the parameters of the case, the malware starts killing the nodes with maximum possible rate. This will ensure that an infective nodes are maximally used for spread of the infection and for attacker’s malicious activities.

In order to present the result for optimal $u$, we need to introduce an extra assumption. Recall that both $b(I)$ and $q(S)$ satisfy $b(0) = q(0) = 0$, and $b(I), q(S)$ are increasing functions of $I, S$ for $I, S \in [0, 1]$. Assume further that there exist positive constants $\hat{b}$ and $\hat{q}$ such that

$$\forall I, S \in [0, 1], \quad b(I) \geq \hat{b}I \quad \text{and} \quad q(S) \geq \hat{q}S. \quad (4.3.1)$$

Now, considering the supremum of such constants, we assume to have:

$$\hat{b} + \hat{q} \geq \beta u_{\text{max}} \quad (4.3.2)$$

$\beta u_{\text{max}}$ is the maximum rate of the spread of the infection, and intuitively, the above condition describes the scenario in which the recovery rate (healing + immunization) is larger than the maximum rate of the spread of the infection. We will refer to this assumption as fast-recovery regime assumption.

**Theorem 4.3.2.** Assuming fast-recovery regime, any optimal $u(t)$ for the case of strictly convex $h(u)$ consists of the following phases:

1. $u = u_{\text{max}}$ on $0 < t \leq t_0 < T$ for some $t_0 \geq 0$;

2. $u$ strictly and continually decreases on $t_0 < t \leq t_1 < T$ for some $t_1 \geq t_0$;

3. $u = u_{\text{min}}$ on $t_1 < t \leq T$.

For the case of a concave $h(u)$, any optimal $u$ consists of only phase 1 followed by phase 2, i.e., $u = u_{\text{max}}$ until time $t_0$ and subsequently $u = u_{\text{min}}$.
Although theorem 4.3.2 is presented assuming fast-recovery regime, our numerical results show that these structural results hold even when this assumption is relaxed (§4.5).

According to theorem 4.3.2, optimal media scanning rate and malware transmission rates is always a non-increasing function of time. Specifically, the most intense (battery-consuming) spreading effort of malware should take place at the start of the outbreak. Intuitively, this is because initially the number of susceptibles is high, and hence an infective contacts more susceptibles by using the same $u$ initially than later. Moreover, if a node is infected earlier, it will have more time to further propagate the infection. Subsequently, owing to the overall energy limitations, as the level of susceptibles as potential preys drop, infectives should reduce their media scanning rates so as not to exhaust their spreading battery budget. The structure of an optimal $u$ turns out to subtly depend on whether the $h$ function is strictly convex or concave. We can have an intuitive explanation for this phenomenon: a slight reduction in the value of $u$ results in a higher decrease in the instantaneous power for a strictly convex $h(u)$ than for a concave $h(u)$. Therefore, in the case of strictly convex $h(u)$, it is beneficial to reduce $u$ continuously (instead of keeping $u$ at $u_{\text{max}}$ before a threshold time) and prolong the battery lifetime for malicious activities of the malware.

In summary, theorems 4.3.1 and 4.3.2 provide the joint optimal attack as follows: initially, the highest effort of the malware is focused on spreading the malware and amassing infectives without killing any. Subsequently, the reverse course of action is taken: battery is used at lower rates, and at a threshold time, the amassed nodes are slaughtered at the highest rate which lasts till the end of the interval.

Note that the optimal killing policy ($\nu$), as well as the media scanning rate of the infectives ($u$) for the case of concave $h(u)$, are completely specified by the (only possible) jump points. Also, the optimal media scanning strategy ($u$) for a strictly convex $h$ can be simply divided into at most three phases, characterized by at most two time epochs. Therefore, no continuous global coordination of attack is necessary. In particular, the threshold times can be computed once an
estimate of the parameters of the network \( (\beta, q(S), b(I), C) \) is made, and can be subsequently incorporated into the code of the malware. Given the flexibility provided by software-driven devices, the infective nodes can subsequently execute these strategies without coordinating any further among themselves or with any central entity. The transition times can be determined by solving a system of differential equations, as described in previous sections. Such systems can be solved very fast due to the existence of efficient numerical algorithms for solving differential equations, and the computation time is constant in that it does not depend on the number of nodes \( N \). Note also that our algorithms do not require any local or global information as time progresses and only the initial information is sufficient to determine the decision of infective nodes for the entire interval.

In practice, due to the drifts in local clocks, different infectives may slow down their transmission rates and start the killing at slightly different times. Our simulations presented in \( \S 4.5 \) reveal that the overall damages are robust to clock drifts for our dynamic optimal policies, yet another unfavorable news from the defense point of view. In the next section we provide the proofs for both of the theorems.

### 4.4 Proofs of Theorems 4.3.1 and 4.3.2

We first obtain some properties of the Hamiltonian and system states which we subsequently use to establish theorems 4.3.1 and 4.3.2.

**Lemma 4.4.1.** \( H = constant > 0 \).

**Proof.** First, the system is autonomous, i.e., the Hamiltonian and the control region do not have an explicit dependency on the independent variable \( t \). Hence, ( \( \{47, P.236\} \)):

\[
H(S(t), I(t), D(t), \nu(t), u(t), \lambda_1(t), \lambda_2(t), \lambda_3(t)) \equiv constant. \tag{4.4.1}
\]
Therefore, from (4.2.11):

\[ H = H(T) = \lambda_0 f(I(T)) + \lambda_0 \kappa \nu I(T) \quad (4.4.2) \]

We showed (after (4.2.6)) that \( \lambda_0 > 0 \), and following lemma 4.1.1, \( I(T) > 0 \); also \( \nu(T) = \nu_{\text{max}} > 0 \), as we argued after (4.2.13). Thus, \( H(T) > 0 \).

The second observation is that \( I \) satisfies the following condition:

**Lemma 4.4.2.** \((f'(I)I - f(I)) \geq 0\) and \((b(I) - b'(I)I) \geq 0\) for all \( t \in [0 \ldots T] \).

**Proof.** By lemma 4.1.1, \( I \) and \( S \) are nonnegative. Define \( \xi(I) = f'(I)I - f(I) \). Since \( f(0) = 0 \), we have \( \xi(0) = 0 \). Also,

\[
\frac{d}{dt} \xi(I) = \xi' = f''(I)I + f'(I) - f'(I) = f''(I)I.
\]

Following lemma 4.1.1 and properties of \( f \), we observe that \( \xi' \geq 0 \) for all \( t \in [0 \ldots T] \). Thus, since \( \xi(0) = 0, \xi(I) = f'(I) - f(I)I \geq 0 \) for all \( t \in [0 \ldots T] \). Likewise for \( b \).

We will also use the following key lemma in the sequel.

**Lemma 4.4.3.** For all \( t \in (0 \ldots T) \), we have \( \lambda_1 \geq 0 \) and \( (\lambda_2 - \lambda_1) > 0 \).

**Proof.** **Step-1.** Following (4.2.5), \( \lambda_2(T) = (\lambda_2(T) - \lambda_1(T)) = 0 \) and from (4.2.4) and (4.2.5) and the discussion following (4.2.15), \( (\lambda_2(T) - \lambda_1(T)) = -\lambda_0 f'(I(T)) - \kappa \nu(T) \), which is strictly negative. Thus, there exists an \( \epsilon_1 > 0 \) such that on the interval of \((T - \epsilon_1 \ldots T)\), we have \( (\lambda_2 - \lambda_1) > 0 \). Also recall from (4.2.5) that \( \lambda_1(T) = 0 \).

**Step-2.** Proof by contradiction. Let \( t^* \) be defined as follows:

\[
t^* := \inf_{0 \leq t \leq T} \{ t | \lambda_1(t) \geq 0 \text{ and } (\lambda_2(t) - \lambda_1(t)) > 0 \text{ on the interval } (t \ldots T) \}\]

If \( t^* = 0 \) then we are done. Suppose \( t^* > 0 \). According to the continuity of \( \lambda_1 \) and \( \lambda_2 \), and following step-1, we must have:

\[
\lambda_2(t^*) - \lambda_1(t^*) = 0 \quad \text{OR} \quad \lambda_1(t^*) = 0
\]

56
• Case 1: $\lambda_2(t^*) - \lambda_1(t^*) = 0$. From the continuity of $\lambda_1$, $\lambda_1(t^*) \geq 0$. We have:

$$\frac{d}{dt}(\lambda_2 - \lambda_1)(t^+) = \frac{d}{dt}(\lambda_2 - \lambda_1)(t^-) = -\lambda_0 f' + \lambda_2 b' - \frac{\varphi}{T} \nu - \lambda_1 q' \quad [: (4.2.4)]$$

$$= -\lambda_0 f' + \lambda_2 b' - \frac{\varphi}{T} \nu - \lambda_1 q' - \frac{H}{T} + \lambda_0 \frac{f}{T} - \lambda_1 q' - \frac{\lambda_2 b}{T} + \frac{\varphi}{T} \nu - \frac{h}{T} \quad [: (4.2.11)]$$

$$= \frac{\lambda_0}{T} [f' - (f' I)] + \frac{\lambda_2}{T} [b' I - b] - \lambda_1 q' - \frac{\lambda_1 q}{I} - \frac{H}{I} - \frac{h}{I} \quad (4.4.3)$$

From lemma 4.4.2, $[f - f'I] \leq 0$ and $[b'I - b] \leq 0$. Also in this case, $\lambda_2(t^*) = \lambda_1(t^*)$ (by assumption of the case), and $\lambda_1(t^*) \geq 0$. Now following lemmas 4.1.1 and 4.4.1, and eq. (4.4.3) and properties of $q(S)$, we observe that $\left[ \frac{d}{dt}(\lambda_2 - \lambda_1)(t^+) \right] = \frac{d}{dt}(\lambda_2 - \lambda_1)(t^-) < 0$. According to property 1, this is a contradiction. Thus, case 1 could not occur.

• Case 2: $\lambda_2(t^*) - \lambda_1(t^*) > 0$, and $\lambda_1(t^*) = 0$, and $\forall \delta > 0$, there exists $t_1 \in (t^* - \delta \ldots t^*)$ such that $\lambda_1(t_1) < 0$. From continuity of $\lambda_1$ and $\lambda_2$, $\exists \epsilon > 0$ such that on $(t^* - \epsilon \ldots t^*)$, $\lambda_2 - \lambda_1 > 0$, and hence according to (4.2.4) and lemma 4.1.1, wherever $(\nu, u)$ is continuous, $\dot{\lambda}_1 \leq \lambda_1 q'$. Now consider a $\delta < \epsilon$, and define $\hat{t}$ to be the point which has the lowest value of $\lambda_1$ on the interval of $[t^* - \delta \ldots t^*]$. According to the assumption of case 2, $\lambda_1(\hat{t})$ is strictly negative. Thus, $\dot{\lambda}_1(\hat{t}^+) \leq \lambda_1(\hat{t}^+) q'(S(\hat{t}^+)) < 0$. This, along with continuity of $\lambda_1$, imply that in the right neighborhood of $\hat{t}$, $\lambda_1$ has lower values than $\lambda_1(\hat{t})$. This contradicts the definition of $\hat{t}$.

Therefore, none of the two cases could occur, which is a contradiction with existence of $t^*$. Hence, the lemma.

We are now ready to proceed to the proofs of the theorems.

### 4.4.1 Proof of Theorem 4.3.1: optimal rate of killing

**Proof.** To establish the statement of the theorem, we will show that the switching function $\varphi$ is equal to zero at at most one time epoch. The theorem subsequently follows from the relation between $\varphi$ and $\nu$ given by (4.2.13).
Let us begin by studying two simple real analysis properties.

**Property 1.** Let \( f(t) \) be a continuous and piecewise continuously differentiable function of \( t \). Assume \( f(t_0) > L \). Now if \( f(t_1) = L \) for the first time before \( t_0 \), i.e., \( f(t_1) = L \) and \( f(t) > L \) for all \( t \in (t_1 \ldots t_0) \), then \( \dot{f}(t_1^+) \geq 0 \).\(^5\)

**Proof.** Proof by contradiction. Suppose that Property 1 did not hold, thus

\[
\begin{align*}
&f(t_1) = L, \quad \dot{f}(t_1^+) < 0 \\
\Rightarrow &\exists \delta_1 \in (0 \ldots t_0) \text{ such that } f(t_1 + \delta_1) < L.
\end{align*}
\]

However, by the Intermediate Value Theorem (IVT), there must exist a time \( t_1 + \delta_1 < \tau < t_0 \) such that \( f(\tau) = L \). This contradicts the assumption that \( f(t) \neq L \) for all \( t_1 < t < t_0 \). \( \square \)

**Property 2.** Let \( f(t) \) be a continuous and piecewise continuously differentiable function of \( t \). Assume \( t_1 \) and \( t_2 \) to be its two consecutive \( L \)-crossing points, that is, \( f(t_1) = f(t_2) = L \) and \( f(t) \neq L \) for all \( t_1 < t < t_2 \). Now if \( \dot{f}(t_1^+) \neq 0 \) and \( \dot{f}(t_2^-) \neq 0 \), then \( \dot{f}(t_1^+) \) and \( \dot{f}(t_2^-) \) must have opposite signs.

**Proof.** We prove the property for \( \dot{f}(t_1^+) > 0 \). The proof follows similarly if \( \dot{f}(t_1^+) < 0 \). We have,

\[
\begin{align*}
&f(t_1) = L, \quad \dot{f}(t_1^+) > 0 \\
\Rightarrow &\exists \delta_1 \in (0 \ldots \frac{1}{2}(t_2 - t_1)) \text{ such that } f(t_1 + \delta_1) > L.
\end{align*}
\]

Suppose that Property 2 did not hold, and \( \dot{f}(t_2^-) > 0 \). Then,

\[
\begin{align*}
&f(t_2) = L, \quad \dot{f}(t_2^-) > 0 \\
\Rightarrow &\exists \delta_2 \in (0 \ldots \frac{1}{2}(t_2 - t_1)) \text{ such that } f(t_2 - \delta_2) < L.
\end{align*}
\]

But now, by the Intermediate Value Theorem (IVT), there must exist a time \( t_1 + \delta_1 < \tau < t_2 - \delta_2 \) such that \( f(\tau) = L \). This contradicts the assumption that \( f(t) \neq L \) for all \( t_1 < t < t_2 \). \( \square \)

\(^5\)For a general function \( f(x) \), the notations \( f(x_0^+) \) and \( f(x_0^-) \) are defined as \( \lim_{x \to x_0^+} f(x) \) and \( \lim_{x \to x_0^-} f(x) \), respectively. We denote \( \dot{f}(t^+) \) as the right-side time derivative of \( f \) at time \( t \).
Now, we proceed with the proof of the theorem. Let us calculate the time derivative of the \( \varphi \) function wherever \((\nu, u)\) is continuous:

\[
\dot{\varphi} = (\lambda_3 - \lambda_2) I \dot{I} + \dot{I} \dot{\varphi} / I \quad \text{[\:(4.2.7):]} \\
= (\lambda_0 f' + (\lambda_2 - \lambda_1) \beta u S - \lambda_2 b' + (\lambda_3 - \lambda_2) \nu) I \dot{I} + \dot{I} \dot{\varphi} / I \quad \text{[\:(4.2.4):]} \\
= \lambda_0 f' I + \psi u - \lambda_2 b' I + \varphi \nu + \dot{I} \dot{\varphi} / I \\
+ (H - \lambda_0 f - \psi u + \lambda_1 q + \lambda_2 b - \varphi \nu + h(u)) \quad \text{[\:(4.2.11):]} \\
= H + \lambda_1 q + \lambda_0 (f' I - f) + \lambda_2 (b - b' I) + h(u) + \dot{I} \dot{\varphi} / I. \quad (4.4.4)
\]

Let a time at which \( \varphi = 0 \) be denoted by \( \tau \). From (4.4.4) we obtain:

\[
\dot{\varphi}(\tau^+) = \dot{\varphi}(\tau^-) = H + \lambda_1 q + \lambda_0 (f' I - f) + \lambda_2 (b - b' I) + h(u) \quad (4.4.5)
\]

Equation (4.4.5), positivity of \( \lambda_0 \) and lemmas 4.1.1, 4.4.1, 4.4.2, 4.4.3 show that \( \dot{\varphi}(\tau^-), \dot{\varphi}(\tau^+) > 0 \) wherever \((\nu, u)\) is continuous. Firstly, this shows that \( \varphi \) cannot be equal to zero over an interval of nonzero length. To see this, note that otherwise, due to piecewise continuity of \( \nu \) and \( u \), there exists a subinterval inside the interval of \( \varphi = 0 \) over which, \((\nu, u)\) is continuous. Thus \( \varphi \) is differentiable over this subinterval, and necessarily \( \dot{\varphi} = 0 \) for any time inside that subinterval, which is not possible. Thus, referring to (4.2.13), \( \nu \) is bang-bang, i.e., \( \nu \in \{0, \nu_{\text{max}}\} \).

Secondly, referring to property 2, we conclude that \( \varphi = 0 \) at at most one point inside \((0 \ldots T)\) interval. Since (from (4.2.8)) \( \varphi(T) > 0 \) and because \( \varphi \) is a continuous function of time, \( \varphi(t) > 0 \) for an interval of nonzero length towards the end of \((0 \ldots T)\). If \( \varphi(t) > 0 \) for all \( 0 \leq t \leq T \), then \( \nu = 0 \) throughout the interval. Otherwise, there exists a \( t_0 \in [0 \ldots T] \) such that \( \varphi(t) < 0 \) for \( t_1 < t \leq T \) and \( \varphi(t) > 0 \) for \( 0 \leq t < t_1 \). Theorem 4.3.1 now follows from the relation between optimal \( \nu \) and \( \varphi \) in (4.2.13).

\[\square\]

**Remark on the case of** \( \lambda_4 = 0 \) **The** Hamiltonian in (4.2.11) **for this case turns into:**

\[
H = \lambda_0 f(I) + \psi u - \lambda_1 q - \lambda_2 b + \varphi \nu.
\]
Note that maximization of $H$ with respect to $\nu$ (as stated in (4.2.12)) does not change at all and hence the same arguments in the proof applies.

4.4.2 Proof of Theorem 4.3.2: optimal scanning rate/Tx range

The optimal $u$ is given by (4.2.15) and (4.2.16) in terms of $\psi(t)$. We first show that function $\psi$ is a strictly decreasing function of time (lemma 4.4.4). Subsequently, we establish the statement of the theorem by investigating the implication of lemma 4.4.4 on the structure of $u$ for cases of strictly convex $h(u)$ and concave $h(u)$ separately.

Lemma 4.4.4. $\psi(t)$ is a strictly decreasing function of time for $0 \leq t \leq T$.

Proof. Let us calculate the time derivative of the $\psi$ function wherever it exists (which is wherever $(\nu,u)$ is continuous):

$$
\dot{\psi} = (\lambda_2 - \lambda_1) \beta IS + \frac{I \psi}{T} + S \frac{\psi}{S} \quad \text{[: (4.2.9)]}
$$

$$
= [-\lambda_0 f' - (\lambda_2 - \lambda_1) \beta uS + \lambda_2 b' - \frac{\varphi}{T} \nu + (\lambda_2 - \lambda_1) \beta uI - \lambda_1 q'] \beta IS
$$

$$
+ (\beta uIS - b - \nu I) \frac{\psi}{T} + (-\beta uIS - q) \frac{\psi}{S} \quad \text{[: (4.1.1),(4.2.4)]}
$$

$$
= -\lambda_0 f' \beta IS + \lambda_2 b' \beta IS - \varphi \nu \beta S - \lambda_1 q' \beta IS + (-b - \nu I) \frac{\psi}{T} + (-q) \frac{\psi}{S}
$$

$$
+ \{ -H \beta S + [\lambda_0 f - h + \psi u - \lambda_1 q - \lambda_2 b + \varphi \nu S] \beta S \} \quad \text{[: (4.2.11)]}
$$

$$
= -H \beta S + (f - f') \lambda_0 \beta S + \lambda_2 (b' I - b) \beta S - \lambda_1 q' \beta IS - \lambda_1 q \beta S
$$

$$
+ \left( \frac{b}{T} - \frac{q}{S} + u \beta S \right) \psi - \nu \psi - \beta Sh. \quad (4.4.6)
$$

In lemmas 4.4.1 and 4.4.3, we showed that $H$ is a positive constant and $\lambda_1 \geq 0$ for all $t \in [0 \ldots T]$.

From lemma 4.4.3, $\lambda_2$ is also non-negative. Also recall that by definition, $\psi = (\lambda_2 - \lambda_1) \beta IS$. By lemmas 4.1.1 and 4.4.3, $\psi(t) \geq 0$ for all $t$, $0 \leq t \leq T$. These facts along with the assumptions in (4.3.1) and (4.3.2) and lemmas 4.1.1 and 4.4.2, show that $\dot{\psi} < 0$ wherever $(\nu,u)$ is continuous (fact-I). Recall that $(\nu,u)$ is continuous except potentially at finite number of time epochs. From
Pontryagin Maximum Principle, states and co-states and hence $\psi$ are continuous functions of time (fact-II). The lemma now follows from fact-I and fact-II.

We are now ready to prove theorem 4.3.2. We consider the cases of strictly convex $h(.)$ and concave $h(.)$ separately.

**Strictly Convex** $h(u)$

*Proof.* Since by lemma 4.4.4, $\psi$ is a strictly decreasing (and continuous) function of time and since for a strictly convex $h$, $h'(u_{\min}) < h'(u_{\max})$, there exist $t_0$ and $t_1$, $0 \leq t_0 < t_1 \leq T$, such that $\psi \geq h'(u_{\max})$ for $t \in [0 \ldots t_0]$, $h'(u_{\min}) < \psi < h'(u_{\max})$ for $t \in [t_0 \ldots t_1]$ and $\psi \leq h'(u_{\max})$ for $t \in [t_1 \ldots T]$. From (4.2.15), $u = u_{\max}$ over the first interval and $u = u_{\min}$ over the last interval. According to (4.2.5), $\psi(T) = 0$, and due to continuity of $\psi$, the last interval is of nonzero length. Thus we only need to show that $u$ is a strictly decreasing function of time during $[t_0 \ldots t_1]$.

From (4.2.15), for this interval we have $u = h'^{-1}(\psi)$. For a strictly convex $h$, $h'^{-1}(\psi)$ is strictly increasing in its argument, i.e., $\psi$. Hence, from lemma 4.4.4, $h'^{-1}(\varphi)$ is a strictly decreasing function of time. This concludes the proof.

**Concave** $h(u)$

*Proof.* Since according to lemma 4.4.4, $\psi$ is a strictly decreasing (continuous) function of time, $\psi = \rho$ at at most one time epoch, $t_0$. Specifically, $\psi > \rho$ for $t \in [0 \ldots t_0)$ and $\psi < \rho$ for $t \in (t_0 \ldots T]$. The theorem now readily follows from (4.2.16).

**Remark on the case of concave** $h(.)$ **and** $u_{\min} = 0$  
When $u_{\min} = 0$ (which is not unnatural to assume), then theorem 4.3.2 for concave $h(.)$ holds without the fast-healing assumption, which we explain briefly here. The idea is to show $\psi$ has negative (right and left) time derivatives at $\rho$-crossing points, and hence arguing similar to the proof of theorem 4.3.1. This can be shown by referring to (4.4.6), and rearranging to obtain the term $\beta S(\psi u - h(u))$ where all of the other terms
are negative. Let a $\rho$-crossing time epoch of $\psi$ be denoted by $\tau$. Since $u$ is piecewise continuous except for finite number of time epochs, $u(\tau^+)$ and $u(\tau^-)$ is either $u_{\text{min}} = 0$ or $u_{\text{max}}$, for both of which we have $(\rho u - h(u)) = 0$ and hence the term $\beta S(\psi u - h(u))$ vanishes from the equation, proving that $\psi$ has negative side time derivatives at its $\rho$-crossing points. We can now apply property 2, as we did in proof of theorem 4.3.1, to derive the statement of theorem 4.3.2 for concave $h(.)$.

**Remark on the case of $\lambda_4 = 0$**  The Hamiltonian in (4.2.11) for this case turns into

$$H = \lambda_0 f(I) + \psi u - \lambda_1 q - \lambda_2 b + \varphi \nu.$$  

Thus, according to (4.2.12), an optimal $u$ needs to maximize $\psi u$. By definition in (4.2.9), $\psi = (\lambda_2 - \lambda_1)\beta IS$, which according to lemmas 4.1.1 and 4.4.3 is always strictly positive, and thus the optimal $u$ is trivially $u = u_{\text{max}}$ for the entire interval of $[0 \ldots T]$. Intuitively, when the battery reserve is sufficient to use $u_{\text{max}}$ throughout the interval, it is trivially optimal to do so.

### 4.5 Numerical computations

Our numerical computations are designed to complement our analysis in the previous two sections. We compare the efficacy of our dynamic policy against two heuristic policies for a variety of parameters. We investigate the effect of some of the issues related to implementation of optimal dynamic attacks such as approximate parameter estimation and imperfect timings. We use the insights revealed by these computations in designing efficient counter-measures.

We chose $T = 10$, $I_0 = 0.1$, $\beta = 0.4$, $u_{\text{max}} = 1$, $\nu_{\text{max}} = 0.5$, $u_{\text{min}} = 0$, $f(I) = 0.1I$, $\kappa = 1$, $h(u) = u^2$ (which is strictly convex) and $C = 5$. We have selected $C$ such that the choice of

---

*For our numerical calculations, we used the PROPT® software designed by Tomlab Optimization Inc. Specifically, each instance of our optimal control problems took one second, using an Intel® Xeon® CPU X5355, 2.66 GHz 8 Gb RAM, 2Gb swap memory machine.*
\( u(t) = u_{\text{max}} \) for all \( t \in [0, T] \) violates the battery constraint of (4.1.4b). Also, we take \( Q(x) = \gamma \) and \( B(x) = \pi \gamma \) for all \( x \in [0,1] \), i.e., \( q(S) = \gamma S \) and \( b(I) = \pi \gamma I \). Here \( \pi \in \{0, 1\} \) determines whether the countermeasure involves only immunizing the susceptibles (\( \pi = 0 \)) or, the same security patch can successfully remove the infection, if any, and immunize a node against future infection (\( \pi = 1 \)). We refer to \( \gamma \) as the recovery rate and take \( \gamma = 0.2 \).

Our first observation is that for all ranges of parameters that will follow in this section, the structural results of theorems 4.3.1 and 4.3.2 for the optimal solution hold, even when the regime is not fast-recovery which we assumed while proving theorem 4.3.2. One example is fig. 4.2 that depicts the optimal controllers as well as the states as functions of time.

![Figure 4.2: Evaluation of the optimal controllers and the according states as functions of time.](image)

\( h(u) = u^2, \beta = 0.9, u_{\text{max}} = 1, \gamma = 0.2, \) and \( \pi = 0 \) in left and \( \pi = 1 \) in right. Thus \( \beta u_{\text{max}} = 0.9 > 0.4 \geq (\gamma + \pi \gamma) \).

Therefore, the fast-healing regime does not hold. However, as we can see, the pattern for optimal \( u \) is consistent with statement of by theorem 4.3.2 and strictly convex \( h(u) \).

Next, we investigate the effects that changing different parameters of the system have on the optimal controllers. According to fig. 4.3 and 4.4, we observe that increasing the recovery rate (\( \gamma \)) generally:

- decreases the jump time in the \( \nu \) (fig. 4.3).

- extends the initial period during which \( u = u_{\text{max}} \) and makes the subsequent descent in \( u \)
Intuitively, this phenomenon can be explained in the following manner: in a system with a large recovery rate, both the susceptible and infective nodes recover rapidly. Hence, the worm should use more of its power resources early on and also starts killing them earlier in order to not lose many nodes to the pool of recovered. Note also that the starting time of the killing is more sensitive to the value of recovery rate when $\pi = 1$. This is because for $\pi = 0$, the security patches can only immunize the susceptibles and once a node is infective, it will not be recovered by the system.

**Figure 4.3:** Jump points of optimal $\nu$ (starting time of the slaughter period) versus $\gamma$ for both $\pi = 0$ and $\pi = 1$. Note that for $\pi = 1$ and for $\gamma \geq 0.30$, malware starts killing the infectives from time zero.

**Figure 4.4:** The optimal $u$ (media scanning rate times the transmission rates of infectives) for different values of $\gamma$ for both $\pi = 0$ (left) and $\pi = 1$ (right).

Next, we compare the efficacy of our dynamic policies against two heuristic policies for
various ranges of parameters. In the first heuristic policy, \( u \) starts initially at \( u_{\text{max}} \) until time 
\[ \min(C/u_{\text{max}}^2, T)^7 \] 
after which, it switches off to zero. The value of the \( \nu \) is fixed throughout. The fixed value of \( \nu \) is varied a priori and the one which yields the maximum damage is selected. We call this policy Static 1. In the second heuristic policy, both \( u \) and \( \nu \) are set to fixed a priori values throughout the operation interval. \( u \) is set to the fixed value of 
\[ \min(u_{\text{max}}, \sqrt{C/T})^8, \] 
so that throughout the interval, the battery condition is not violated but is maximally used. The fixed value of the \( \nu \) is then selected similar to Static 2. We refer to this new policy as Static 2. As we observe in figures 4.5 through 4.9, for all ranges of changing \( \beta, I_0, \gamma, C \) and \( \nu_{\text{max}} \), the order of maximum inflicted damage is as follows: Dynamic > Static 1 > Static 2. The advantage of dynamic attacks over heuristic attack is more pronounced for \( \pi = 0 \) and can exceed 50% increase. The trend of damage with change of each parameter is intuitive. Interestingly, when \( \pi = 1 \), that is when the security patches can heal and immunize the infectives as well as the susceptibles, not only the overall damage is lower, but also the dynamic efficacy of the attacker (i.e., the advantage of using optimal dynamic policies) is reduced.

Robustness of our dynamic policy is the subject of the next investigation. In practice, the malware-writer might not accurately know the parameters of the system, and only have access to rough estimates. Therefore, it is important to measure the drop in the efficacy of such dynamic policies as a result of inaccurate parameter estimations. We apply our dynamic policies as well as heuristic policies that are calculated based on estimations of one parameter with potential inaccuracy of 50%. We then depict (fig. 4.10) the total cost incurred by applying these sub-optimal policies. The horizontal axis is the estimated value of the parameters where the center point is the value of the parameter in reality. Specifically, in subfig. 4.10(a), the real value of \( \beta \) is 0.4 and

\[ h(u) = u^2. \] 
Thus the battery constraint (in (4.1.4b)) for this heuristic policy is translated to 
\[ \int_0^T u_{\text{max}}^2 \chi_{t < t^*} \, dt \leq C, \] 
where \( t^* \) is the threshold time. This yields 
\[ t^* = \min\left(\frac{C}{u_{\text{max}}^2}, T\right), \] 
as provided in the text.

\[ \int_0^T u_0^2 \, dt \leq C, \] 
which gives 
\[ u_0 = \min(u_{\text{max}}, \sqrt{C/T}), \] 
as stated in the text.
Comparison of the aggregate damage inflicted by our dynamic policy versus two heuristic policies: Static 1 and Static 2.

In subfig. 4.10(b), the real value of $\gamma$ is 0.2. As we can observe, the decrease in the aggregate damage as a result of 50% inaccuracy in the estimation of the value of $\beta$ (subfig. 4.10(a)) and $\gamma$ (subfig. 4.10(b)) is less than 15%. Moreover, the dynamic policy consistently outperforms both of static policies despite the presence of erroneous estimation of network and defense parameters.

As we mentioned earlier, drifts in local clocks of the nodes make exact timing of the execution of the dynamic policies difficult, and may affect the overall damages that a malware can inflict on the network. Here, we evaluate the overall damage when infective nodes’ clocks drift from the global clock by different amounts, and hence they choose dynamic policies which are
Figure 4.10: Robustness of optimal dynamic policy against parameter estimation. The dotted line designates the real value of the parameters (the center of the x-axis).

shifted aside in time from the global control by their individual (additive) drifts. We chose clock drifts which are statistically independent and uniformly distributed between $-\Delta \times T$ and $\Delta \times T$. Fig. 4.11 depicts the overall damage versus $\Delta$ averaged over 100 simulation runs where the number of nodes is 50. Note that even for $\Delta$ as large as 0.5, the decrease in the overall damage as compared to the zero-drift case is less than 11%.

Finally, we consider the problem of choosing the best parameters from the viewpoint of the system. Specifically, the system chooses the recovery rate a priori for a worst case scenario, which is when the attacker knows the parameters of the system (including the recovery rate) and chooses the optimal dynamic attack policy. As anticipated, our numerical computations reveal that higher recovery rates (larger $\gamma$) and lower reception gains of the nodes (smaller $\beta$), reduces the damage due to the attack (fig. 4.7 and 4.5, respectively). However, increasing the
recovery rate is achieved through greater usage of costly resources such as bandwidth and power, and thereby inflicts a recovery cost on the system. Likewise, decreasing the reception gain of the nodes thus indiscriminate quarantining of nodes disrupts the functionality of networks by introducing delay and hence deteriorating the quality of service (note that a susceptible node does not know whether the node it is communicating with is infective or otherwise a priori; hence it can not selectively reduce its reception gain). We consider the overall system cost as the sum of the damage caused by the worm and the expense of providing the immunization and healing rates of $\gamma$ and the cost due to deterioration of the QoS which is inversely proportional to the inter-contact rates $\beta$. The system faces a trade-off in choosing the least-costly recovery and quarantining (reduced inter-contact) rates, which we resolve numerically. In fig. 4.12 we have plotted the overall system cost assuming a simple linear recovery cost induced by $\gamma$ (specifically $1 \times \gamma$). In fig. 4.13, we adopt $0.1/\beta$ as the QoS cost, inspired by the work in [30] in which the authors show the average delay in a DTN is proportional to $\beta^{-1}$. In each case, the overall cost is minimized at unique values of $\gamma$ and $\beta$. 

Figure 4.11: Robustness of the dynamic attack strategy with respect to clock drifts.
Figure 4.12: System cost (malware’s damage + the cost of patching) versus $\gamma$ (rate of patching).

Figure 4.13: System cost (malware’s damage + the cost of quarantining) versus $\beta$. 
Part II

Defense
Chapter 5

Rate Reduction

Introduction

In this section, we focus on the containment of infection in a mobile wireless network. Several wireless properties enhance the severity of the infection. However, these unique features can also be utilized to contrive new counter-measures against the spread of infection. An infected node can transmit its infection to another node only if they are in communication range of each other. We propose to quarantine the infection by regulating the communication range of the nodes. Specifically, the reception gain of the healthy nodes can be reduced to abate the frequency of contacts between the mobile nodes and thus suppress the spread of the infection. In the case of MMS networks, this can be emulated by simply dropping (refusing) a fraction of the communication requests. In fact, there is an interesting analogy between the spread of a worm in mobile wireless networks and a biological epidemic in a human community. During a biological virus outbreak, individuals might choose to restrain their contacts with the rest of the society. This abstinence decreases the chance of getting infected at the expense of deterioration in the quality of life: a decrease in the rate of communication between the members of the society hampers their ability to fully perform their daily tasks [61]. Such a trade-off also exists in the case of a mobile wire-
less network: reducing the communication range of nodes can deteriorate the QoS offered by the network, as the end-to-end communication delay increases.

We present a containment strategy based on power control. We propose an optimal control framework to characterize the trade-off between the containment efficacy and communication capabilities of the nodes (section 5.1). Using Pontryagin’s Maximum Principle, we devise a framework for computing the dynamically evolving optimal communication range. We identify several structural characteristics of the optimal control by examining the analytical properties of the solution (section 5.3). Specifically, for a general concave cost function (subsection 5.3.1), we show that the optimal solution has the classical bang-bang structure, i.e., it is only at its minimum or maximum values. We prove that the optimal solution in this case has at most two (abrupt) transitions between these extreme values. Subsequently, we establish that the optimal solution follows a similar structure for a strictly convex cost function, with the exception that transitions are continuous and smooth instead of being abrupt (subsection 5.3.2). Finally, we demonstrate that dynamic optimal control of the communication range significantly outperforms static choices, and is also robust to errors in estimation of the network and attack parameters (Section 5.6).

5.1 System model

Transmission of a packet between a pair of nodes is successful if the received SNR is above the minimum level necessary to decode the signal. The signal power at the receiver node is:

\[
\text{transmission gain} \times \text{reception gain} \times \text{base signal power} \times \frac{\text{distance}^{\text{Propagation loss factor}}}{\text{distance}^{\text{Distance factor}}} = \text{base signal power}
\]  

(5.1.1)

in which the base signal power is the power of the signal at the output of the transmitter antenna when the transmission gain is unity, and the propagation loss factor is a constant no less than 2, determined by the type of media and geographical features of the network [5, 77]. Thus two nodes can communicate only if they are within a certain distance from each other, which we refer to as their communication range. Recall that when two nodes are in communication range of each
other, we say they are in contact. Following our modeling assumptions discussed in Chapter 2, the pairwise inter-contact rate of a given pair of nodes is estimated as \( \hat{\beta}u \) where \( \hat{\beta} = \frac{2wE[V^*]}{A} \), \( w \) is a constant factor pertaining to the specific mobility model, and \( E[V^*] \) is the average relative speed between two nodes. When a susceptible and an infective node are in contact, the infection is transmitted to the former with a certain probability. We assume that \( \hat{\beta} \) does not change with time.

Upon detection of an infective node, either the user of an infected device or the network operator removes the infection of the node by installing a security patch, which also grants the node permanent immunity against that threat. However, this does not take place immediately upon infection, but rather after an exponentially distributed random delay with mean \( 1/\gamma \). This delay is associated with detection of the malware before obtaining the appropriate patch. First, we assume that each node obtains the security patch directly from a trusted source, such as a server, or authorized access points, or trained human agents. In section 5.4 we consider an alternative setting for obtaining these security patches. As before, the infective nodes which receive the patch are referred to as recovered.

Now, as we will discuss in more detail in Appendix A, as \( N \) grows, \( S(t), I(t), R(t) \) converge to the solution of the differential equations

\[
\begin{align*}
\dot{S} &= -\beta u IS, \\
\dot{I} &= \beta u IS - \gamma I, \\
\dot{R} &= \gamma I
\end{align*}
\]

with initial states \( (S_0, I_0, R_0) \), where \( S_0 = \lim_{N \to \infty} n_S(0)/N \), \( I_0 = \lim_{N \to \infty} n_I(0)/N \), \( R_0 = \lim_{N \to \infty} n_R(0)/N \) and \( \beta = \lim_{N \to \infty} N\hat{\beta} \).

We assume that at time zero, a nonzero portion \( (I_0) \) of the nodes, but not all of them, are infective: \( 0 < I(0) = I_0 < 1 \). Similarly, \( 0 < S_0 < 1 \). Moreover, in general, some fraction of the nodes may be previously immunized to the infection, i.e., \( 0 \leq R(0) = R_0 < 1 \). Using the fact that \( S + I + R = N/N = 1 \), the system of differential equations presented above may be reduced to
the following 2-dimensional system

\[
\begin{align*}
\dot{S} & = -\beta u IS \\
\dot{I} & = \beta u IS - \gamma I
\end{align*}
\]

\begin{align*}
S(0) & = 1 - I_0 - R_0 \\
I(0) & = I_0
\end{align*}

(5.1.2a, 5.1.2b)

with the state constraints

\[0 \leq S, I, \quad S + I \leq 1.\]  

(5.1.3)

As we can see from the system dynamics in (5.1.2), reduction of the communication range between susceptible and infective nodes, \(u\), can repress the propagation of the malware. Recall from (5.1.1) that the communication range between an infective transmitter and a susceptible receiver is governed both by the transmission gain of the infective and the reception gain of the susceptible node. This motivates a defense policy for wireless networks: upon detection of malicious behavior, susceptible nodes can reduce their reception gains. Effectively, this results in a reduction of their communication range, which lessens the frequency of contacts between the infective and susceptible nodes. This in turn reduces the rate of propagation of the infection. Thus, the reception gain of the susceptible nodes and hence the communication range \(u(t)\) can be a control variable, which is bounded between a maximum and minimum value:

\[u_{\text{min}} \leq u \leq 1.\]  

(5.1.4)

These bounds are imposed by the physical constraints of the device as well as the MAC protocol and the minimum acceptable QoS. Note that the actual bounds of the communication range can always be re-scaled and normalized, and their impact can be captured by an appropriate \(\beta\), so that \(u_{\text{max}} = 1\). Any \(u(t)\) that satisfies the above constraint is called admissible, and the range \([u_{\text{min}} \ldots 1]\) is referred to as the admissible range. We make the technical assumption that \(u_{\text{min}} > 0\).

Our model applies to cases in which the malware does not have controllable access to the parameters of the MAC, and thus the transmission gain of the infective nodes is unchanged. Even if the malware could indeed modify the transmission gain of the infective nodes, in case there
is no restriction about the underlying energy resources of the network, then irrespective of the choice of the reception gain of the susceptibles, it is apt to use the maximum transmission range and scanning rate that is physically realizable by the devices, so as to accelerate its spread. The resulting increase in the transmission range of the infectives can be effectively captured through appropriate scaling of $\beta$, and the model for the dynamics of the system does not change.$^1$

We now construct a meaningful cost function which captures the advantages and disadvantages of changing the communication range. Our cost functions are naturally integration of an instantaneous cost over an operation period. As we discussed before, infective nodes can be used by the malware to perform various forms of malicious activities. Hence, the instantaneous cost grows larger with an increase in the fraction of the infective nodes. Here, we assume a linear dependence on $I(t)$. Let us now explore the relation between the instantaneous cost and the communication range. Note that $u_{\text{max}}$ (which is considered to be 1 after appropriate scaling) is the normal communication range of the nodes and constitutes the optimum operating point in absence of malware. Reducing the communication range below $u_{\text{max}}$ undermines the ability of the nodes to deliver their own traffic and increases delays in the end-to-end delivery of messages related to the normal function of the network. This is more so because nodes can not selectively reduce their communication ranges based on whether they are receiving from an infective or a susceptible node. This is because an infected node does not detect that it is infected for some time, and upon detection it is swiftly recovered by the system. Thus, information about whether or not a node is infective or susceptible, is not available to that node and to any other nodes. Therefore, the reduction of communication range affects communication of packets between all pairs, and thus deteriorates the overall QoS.$^2$

We model the effect of changing $u$ on the QoS:

$^1$When battery lifetimes are limited, which we do not consider here, malware may have an advantage in dynamically varying the propagation range of the infective nodes. This scenario may be analyzed by considering a dynamic game. We analyze a version of such games in part III.

$^2$Assuming bi-directional communication, $u$ is in fact the communication range between a susceptible and an infective or between two susceptible nodes. Specifically, the control of $u$ may not alter the communication range between the
through a double differentiable cost function \( h(u) \) that increases with decrease in \( u \), i.e., \( h'(u) \leq 0 \) for \( u_{\text{min}} \leq u \leq 1 \) and, without loss of generality, \( h(1) = 0 \). To simplify the technical arguments, we further assume \( h'(1) \) is strictly negative. Since the characterization of \( h(\cdot) \) depends on the implemented MAC and routing policies, we consider two classes of \( h(\cdot) \) function: (i) concave \( h \), i.e., \( h''(u) \leq 0 \) for \( u_{\text{min}} \leq u \leq 1 \), and strictly convex \( h \), i.e., \( h''(u) > 0 \) for \( u_{\text{min}} \leq u \leq 1 \).

The overall cost incurred by the network therefore can be represented as follows:

\[
J = \int_0^T (CI + h(u)) \, dt + KI(T). \tag{5.1.5}
\]

Coefficient \( C \geq 0 \) determines the relative importance (hazard) of the infection. The term \( KI(T) \), where \( K \geq 0 \), represents the cost associated with the final tally of the infectives at the end of the operation period. The decision process of the susceptibles may now be represented as a dynamic control problem, that of determination of the \( u(\cdot) \) that minimizes the network cost over all admissible \( u(\cdot)s \) subject to satisfaction of the system dynamics in (5.1.2) - such a \( u(\cdot) \) is denoted as the optimal control.

Note that we allow \( u \) to vary as a function of time, i.e., it is selected dynamically. Particularly, susceptibles may initially choose a lower value of the reception gain to suppress the spread of contagion and to buy time for the recovery process of the nodes to eliminate a safe number of infectives, and subsequently choose higher values of \( u \) so as to minimally disrupt the network communication.

![Figure 5.1: u(t) is the reception gain of the susceptible nodes at time t.](image)

However, as far as QoS is concerned, only the communication range between the susceptible nodes counts.
5.2 Optimal reception gain control

We develop a framework for numerical computation of the optimal control $u$. We start by proving lemma 5.2.1.

**Lemma 5.2.1.** For any admissible $u(\cdot)$, states $(S, I)$ strictly satisfy the state constraints (5.1.3) for the entire interval of $(0, 1]$. 

This lemma allows us to deal with an optimal control problem without any state constraints, since the state constraints are never active - thus, constraints (5.1.3) are ignored henceforth.

**Proof.** Note that at $t = 0$, by assumption we have $0 < I = I_0 < 1$, and also $0 < S = S_0 = 1 - I_0 - R_0 < 1$. Hence, from continuity of the states, the first two constraints in (5.1.3), i.e., $0 \leq S, I$ are strictly satisfied on an interval starting from $t = 0$. The last constraint, i.e., $S + I \leq 1$ is active at $t = 0$, however, by summing equations (5.1.2a) and (5.1.2b) we have $\frac{d}{dt}(S + I)$ at time zero is equal to $-\gamma I_0$, which, following the assumptions, is negative. Therefore, there exists an interval after time zero on which the constraint $S + I \leq 1$ is strictly met. Now suppose that the statement of the lemma is not true. Then, let $t_0$ where $0 < t_0 \leq T$, be the first time that (at least) one of the three state constraints in (5.1.3) becomes active. Thus, the constraints are strictly met in $(0, \ldots t_0)$. For $0 < t < t_0$, from (5.1.2a) we have $\dot{S} \geq -\beta S$, thus $S \geq S_0 e^{-\beta t}$, for all $0 \leq t < t_0$ and therefore, due to continuity of $S(\cdot)$, $S(t_0) > 0$. Similarly, for $0 < t < t_0$ from (5.1.2b) we have $\dot{I} \geq -\gamma I$, thus $I(t_0) > 0$ as well. Now by summing (5.1.2a) and (5.1.2b), we obtain $\frac{d}{dt}(S + I) = -\gamma I$. Hence at $t_0$, $S + I < S_0 + I_0 = 1$. Thus, none of the constraints could have become active, a contradiction. 

We can now apply the *Pontryagin’s Maximum Principle* [47, P.232] on the unconstrained optimal control problem. Consider a piecewise continuous control $u(\cdot)$ and the corresponding state functions $(S, I)$. The Hamiltonian $H$ is the following scalar function of the co-state or adjoint vari-
ables $\lambda_1$ and $\lambda_2$:

$$H = CI + h(u) + (\lambda_2 - \lambda_1)\beta u IS - \lambda_2 \gamma I. \quad (5.2.1)$$

Here, except at the discontinuity epochs of $u(\cdot)$,

$$\dot{\lambda}_1 = -\frac{\partial H}{\partial S} = -(\lambda_2 - \lambda_1)\beta u I \quad (5.2.2)$$
$$\dot{\lambda}_2 = -\frac{\partial H}{\partial I} = -C - (\lambda_2 - \lambda_1)\beta u S + \lambda_2 \gamma.$$  

Also, $\lambda_1, \lambda_2$ have the following final value constraints

$$\lambda_1(T) = 0, \lambda_2(T) = K. \quad (5.2.3)$$

Then, according to Pontryagin’s Maximum Principle, any optimal controller $u$, minimizes the Hamiltonian (5.2.1) over all admissible controls at each time epoch:

$$u \in \arg \min_{u_{\min} \leq u \leq 1} \left\{ H(\lambda_1, \lambda_2, S, I, u) \right\}, \quad (5.2.4)$$

where the state and co-state variables $(S, I, \lambda_1, \lambda_2)$ are absolutely continuous functions of time that satisfy (5.1.2), (5.2.2) and (5.2.3) with the optimum $u$. Let

$$\varphi \triangleq \beta IS(\lambda_2 - \lambda_1), \quad (5.2.5)$$

which is a continuous function of states and co-states and thus, a continuous function of time. This allows us to rewrite the Hamiltonian (in (5.2.1)) as follows:

$$H = CI + h(u) + \varphi u - \lambda_2 \gamma I. \quad (5.2.6)$$

Thus according to (5.2.4), the optimal solution $u$ satisfies

$$h(u) + \varphi u \leq h(y) + \varphi y, \quad (5.2.7)$$

where $y$ is any admissible controller, i.e., $y \in [u_{\min} \ldots 1]$. Thus, to find the optimal controller, one needs to minimize the function $h(y) + \varphi y$ over the admissible set $y \in [u_{\min} \ldots 1]$.  

\footnote{In the terminology of Pontryagin’s Maximum Principle, $S, I, \lambda_1, \lambda_2$ are often referred to as variables, though they are functions of time in reality.}
For strictly concave \( h, h(u) + \varphi u \) is a strictly concave function of \( u \), and is therefore minimized at either \( u = u_{\min} \) or \( u = 1 \). Let \( \kappa \equiv \frac{h(u_{\min})}{1 - u_{\min}} > 0 \). Comparing the values of the function at \( u \in \{u_{\min}, 1\} \), we obtain the optimal \( u \) as

\[
\begin{align*}
  u(t) &= \begin{cases} 
  u_{\min}, & \varphi(t) > \kappa \\
  1, & \varphi(t) < \kappa \\
  u_{\min} \text{ or } 1, & \varphi(t) = \kappa.
  \end{cases}
\end{align*}
\]  

(5.2.8)

For linear \( h(u) \), i.e., for \( h(u) = 1 - u \), \( \kappa = 1 \), and the optimal \( u \) can assume any value in \([u_{\min}, 1]\) if \( \varphi(t) = 1 \). Thus, we just have:

\[
\begin{align*}
  u(t) &= \begin{cases} 
  u_{\min}, & \varphi(t) > 1 \\
  1, & \varphi(t) < 1.
  \end{cases}
\end{align*}
\]  

(5.2.9)

On the other hand, for strictly convex \( h, h(u) + \varphi u \) can be minimized at \( u = u_{\min} \), or at \( u = 1 \) or at \( u = x \in (u_{\min}, 1) \) at which \( \frac{\partial}{\partial x} (h(x) + \varphi x) = 0 \). This yields the following relation for an optimal \( u \) :

\[
\begin{align*}
  u(t) &= \begin{cases} 
  u_{\min}, & -h'(u_{\min}) \leq \varphi(t) \\
  h^{-1}(-\varphi), & -h'(1) < \varphi(t) < -h'(u_{\min}) \\
  1, & \varphi(t) \leq -h'(1).
  \end{cases}
\end{align*}
\]  

(5.2.10)

We have therefore expressed the optimum \( u \) as a function of the state \((S, I)\) and co-state \((\lambda_1, \lambda_2)\) functions. Now, (5.1.2) and (5.2.2), provide a system of differential equations involving only the state and co-state functions, and not the control function. Using the initial and final values on the state and co-state functions, this system can be solved numerically to obtain the optimum state and co-state functions, which can then be used to compute \( u \) via (5.2.8), (5.2.9), (5.2.10), and the overall cost via (5.1.5).
5.3 Structural results

In this section, we show that for a concave $h$, any optimal communication range is a bang-bang function of time, that is, it possesses only two possible values $u_{\text{min}}$ and 1 (theorem 5.3.1). Moreover, it switches abruptly between the extreme values and has at most two such jumps. An optimal solution for a strictly convex $h$ again has at most two switches between $u_{\text{min}}$ and 1, but the transitions are smooth and traverses through all intermediate values (theorem 5.3.2). We first observe the following monotonicity result:

**Corollary 1.** For any admissible control function, $S$ is a strictly decreasing function of time, i.e., $S \searrow S(T)$.

5.3.1 Concave $h(u)$:

**Theorem 5.3.1.** For concave $h$, the optimal $u(\cdot)$ has the following structure:

- $u(t) = 1$ for $0 \leq t < t_1$ for $0 \leq t_1 \leq T$;
- $u(t) = u_{\text{min}}$ for $t_1 < t \leq t_2$ for $t_1 \leq t_2 \leq T$;
- $u(t) = 1$ for $t_2 < t \leq T$.

Thus, optimal $u(t)$ has one of these five forms: it either has no jump and is fixed at $u_{\text{min}}$ or 1 throughout $[0\ldots T]$ ($t_1 = 0, t_2 = T$ or $t_1 = T$, respectively); or has only one jump of the form $u = u_{\text{min}} \uparrow 1$ or $u = 1 \downarrow u_{\text{min}}$ ($0 = t_1 < t_2 < T$ or $0 < t_1 < t_2 = T$, respectively); or has only two jumps which is necessarily of the form $u = 1 \downarrow u_{\text{min}} \uparrow 1$ ($0 < t_1 < t_2 < T$).

We first develop some intuition behind the occurrence of each case. If the malware is highly contagious (large $\beta$), or highly dangerous (large $C,K$), or the recovery process is slow (small $\gamma$), or the cost inflicted by reducing $u$ is low (small $h(u)$), then susceptibles should maintain $u = u_{\text{min}}$ throughout. The other extreme arises for small $\beta$, high $\gamma$, small $C,K$ or large $h(u)$: deviation from the normal $u = 1$ is then sub-optimal. The structure of $u$ in cases that lie between these
two extremes is not apriori clear. The cost \( \int_0^T h(u) \, dt \) due to the deterioration of QoS depends on the duration and the extent of the reduction of \( u \), but not on the timing of such reductions. If \( u \) is reduced early on and subsequently restored to its normal value of 1, infectives start growing only later and thus the time-accumulative cost \( C \int_0^T I \, dt \) due to the growth of the infectives is low. But then since the infection starts spreading later, not enough infectives would be detected and recovered by the end of the operation interval \([0, T]\). Hence, the final tally of the infectives \( I(T) \) may be high as compared to when the reduction of \( u \) starts (and also ends) later. The timing of the reduction must therefore be chosen depending on the relative values of \( C \) and \( K \) and also the spread rate \( \beta \) and the recovery rate \( \gamma \). The one jump case arises if the reduction is either applied at the beginning or at the end, and the two jump case corresponds to when the reduction is applied in an intermediate interval. Note that the theorem establishes that the reductions must be applied in one contiguous interval and also \( u \) is never reduced to an intermediate value between \( u_{\text{min}} \) and \( 1 \) - facts that may not be anticipated based on intuition.

**Proof.** We first consider \( h \) to be strictly concave, and use the optimal control characterization in (5.2.8). The proof is organized as follows:

**Step 1** First we prove that the optimal controller is bang-bang (i.e., it assumes only its maximum and minimum values), by arguing that \( \varphi \) cannot be equal to \( \kappa \) on an interval of nonzero length.

**Step 2** Next we show that \( \varphi \) can have at most two \( \kappa \)-crossing points (the time epochs at which \( \varphi - \kappa \) changes its sign). From (5.2.8) these are the time epochs at which \( u \) switches between its extreme values, and therefore, the optimal controller has at most two jumps.

**Step 3** Finally, we use the terminal value condition of \( \varphi \) to evince the nature of the jumps of the optimal controller.

**Proof of Step 1.** From the definition of \( \varphi \) in (5.2.5), and state and co-state equations respect-
tively in (5.1.2) and (5.2.2), at any \( t \) at which \( u(t) \) is continuous we have

\[
\frac{\dot{\phi}}{\beta} = IS(\lambda_2 - \lambda_1) + I\dot{S}(\lambda_2 - \lambda_1) + IS(\dot{\lambda}_2 - \dot{\lambda}_1)
\]

\[
= (\beta u IS - \gamma I)S(\lambda_2 - \lambda_1) + I(-\beta u IS)(\lambda_2 - \lambda_1)
\]

\[
+ IS(-C - (\lambda_2 - \lambda_1)\beta u S + \lambda_2 \gamma + (\lambda_2 - \lambda_1)\beta u I)
\]

Thus,

\[
\dot{\phi} = -\beta IS(C - \lambda_1 \gamma). \quad (5.3.1)
\]

Now, suppose that \( \phi = \kappa \) on an interval of nonzero length. Since \( u(t) \) is a piecewise continuous function of time, \( u(t) \) is continuous on a subinterval of this interval. On such a subinterval, \( \dot{\phi} \) is equal to zero. Consider now two distinct points of this subinterval, call them \( t_1 \) and \( t_2 \). We have:

\[
\dot{\phi}(t_1) = -\beta I(t_1)S(t_1)(C - \lambda_1(t_1)\gamma) = 0
\]

\[
\dot{\phi}(t_2) = -\beta I(t_2)S(t_2)(C - \lambda_1(t_2)\gamma) = 0.
\]

Following lemma 5.2.1, we must have: \( \lambda_1(t_1) = \lambda_1(t_2) \). However,

\[
\dot{\lambda}_1 = -\frac{\dot{\phi}}{S}u.
\]

Since \( \phi = \kappa > 0 \), and \( u \geq u_{\text{min}} > 0 \), this is a contradiction.

**Proof of Step 2.** We denote \( \kappa \)-points \( t_\kappa \) as epochs at which \( \phi = \kappa \). A \( \kappa \)-crossing point must also be a \( \kappa \)-point, but the reverse is not true. Let the variables with tilde denote their values at \( t_\kappa \).

Next, note that the Hamiltonian is autonomous, i.e., does not explicitly depend on the independent variable \( t \) (\( \frac{\partial H}{\partial t} \equiv 0 \)). When the final time \( T \) is fixed and the Hamiltonian is autonomous then ( [47, P.236]):

\[
H(S(t), I(t), u(t), \lambda_1(t), \lambda_2(t)) \equiv \text{constant} \equiv H. \quad (5.3.2)
\]

From (5.2.5) and by equating \( \phi(t_\kappa) = \kappa \), we obtain

\[
\beta \dot{I} S(\tilde{\lambda}_2 - \tilde{\lambda}_1) = \kappa. \quad (5.3.3)
\]
Since \( u \) is piecewise continuous, state and co-state functions, and hence \( \varphi \), are piecewise differentiable. Thus, we can write\(^4\)

\[
\dot{\varphi}(t^-_\kappa) = \dot{\varphi}(t^+_\kappa) = -\beta \tilde{I} \tilde{S} (C - \tilde{\lambda}_1 \gamma) \quad \text{[from (5.3.1)]}
\]

\[
= -\beta \tilde{I} \tilde{S} (C + \gamma (\frac{\kappa}{\beta IS} - \tilde{\lambda}_2)) \quad \text{[from (5.3.3)]}
\]

\[
= -\beta \tilde{S} (C \tilde{I} - \tilde{\lambda}_2 \gamma \tilde{I}) - \gamma \kappa
\]

\[
= -\beta \tilde{S} (H - h(u) - \dot{\varphi} u) - \gamma \kappa \quad \text{[from (5.2.6)]}
\]

\[
= -\beta \tilde{S} (H - \kappa) - \gamma \kappa.
\]  \hspace{1cm} (5.3.4)

Equation (5.3.4) follows since according to (5.2.8), approaching \( t_\kappa \), a \( \kappa \)-point, \( u \) is either 1 or \( u_{\text{min}} \) and for both of these two values, we have \( h(u) + \dot{\varphi} u = \kappa \).

Here, we re-state a general property of continuous and piecewise differentiable functions which we introduced and proved in §4.4.1 (Property 2).

**Property 3.** Let \( f(\cdot) \) be a continuous and piecewise-differentiable function. Let \( t_1, t_2 \) be its consecutive \( L \)-Level points, that is, \( f(t_1) = f(t_2) = L \) and \( f(t) \neq L \) for all \( t_1 < t < t_2 \). Also, \( \dot{f}(t_1^+) \neq 0 \) and \( \dot{f}(t_2^-) \neq 0 \). Then \( \dot{f}(t_1^+) \) and \( \dot{f}(t_2^-) \) must have opposite signs.

We investigate the case of \( H - \kappa \geq 0 \) first. Then according to (5.3.4) and lemma 5.2.1, \( \dot{\varphi}(t^-_\kappa) = \dot{\varphi}(t^+_\kappa) = -\gamma \kappa < 0 \), as \( \kappa > 0 \). Thus, first of all, \( \varphi \) cannot equal \( \kappa \) over an interval of nonzero length, since that would require \( \varphi \) to be equal to zero over that interval. Now let there be more than one \( \kappa \)-point and call the first two as \( t_{\kappa 1} \) and \( t_{\kappa 2} \). We have \( \tilde{\varphi}(t_{\kappa 1}^+), \tilde{\varphi}(t_{\kappa 2}^-) \leq -\gamma \kappa < 0 \). This contradicts property 3. Thus there is at most one \( \kappa \)-point, and hence at most one \( \kappa \)-crossing point.

Now, let \( H - \kappa < 0 \). Since \( \beta, H, \gamma \) are constants, (5.3.4) is linear in \( \tilde{S} \). Also, recall from Corollary 1 that \( S \) is a strictly monotonic function of time. Thus \( \tilde{S} \), as samples of \( S \), is strictly monotonic in \( t_\kappa \). Therefore, \( \tilde{\varphi} \) is strictly monotonic in \( t_\kappa \). This, together with property (3) show that there are at most three distinct \( \kappa \)-points, say \( t_{\kappa 1} \) to \( t_{\kappa 3} \). Thus, if there are more than two \( \kappa \)-crossing points,\(^4\) \( f(t_{\kappa}^+) \triangleq \lim_{t \downarrow t_{\kappa}} f(t) \quad \text{and} \quad f(t_{\kappa}^-) \triangleq \lim_{t \uparrow t_{\kappa}} f(t) \).
then they have to be \( t_{\kappa 1} \) to \( t_{\kappa 3} \). According to (5.3.4) \( \ddot{\varphi} \) is indeed either negative for all \( t_{\kappa} \) epochs (case of \( H - \kappa \geq 0 \), or is strictly decreasing between consecutive samples at \( t_{\kappa} \) epochs (case of \( H - \kappa < 0 \), a critical fact that we will use later. Thus, by property 3 and the strict monotonicity of \( \ddot{\varphi} \) in \( t_{\kappa} \), \( \ddot{\varphi}(t_{\kappa 2}^-) = \ddot{\varphi}(t_{\kappa 2}^+) = 0 \), and \( \ddot{\varphi}(t_{\kappa 1}^+) \) and \( \ddot{\varphi}(t_{\kappa 3}^-) \) have opposite signs. But this contradicts the following property of continuous and piecewise differentiable functions (which we proved in §4.4.1 as Property 1):

**Property 4.** Let \( f(\cdot) \) be a continuous and piecewise-differentiable function. Let \( t_1, t_2, t_3 \) be three consecutive \( L \)-level points that are also \( L \)-crossing points, that is, \( f(t_1) = f(t_2) = f(t_3) = L \), \( f(t) \neq L \) for all \( t_1 < t < t_2 \) and \( t_2 < t < t_3 \), and \( (f(t) - L) \) changes its sign at these points. Now, if we have \( \dot{f}(t_1^+) \neq 0 \) and \( \dot{f}(t_2^-) = \dot{f}(t_2^+) = 0 \) and \( \dot{f}(t_3^-) \neq 0 \), then \( \dot{f}(t_1^+) \) and \( \dot{f}(t_3^-) \) must have the same sign.

Therefore, there cannot be more than two \( \kappa \)-crossing points.

**Proof of Step 3.** Note that \( \varphi(t) \) is a continuous function that following (5.2.3), ends at

\[
\varphi(T) = \beta u(T) I(T) (\lambda_2(T) - \lambda_1(T)) = \beta u(T) I(T) K. \tag{5.3.5}
\]

First suppose \( \varphi(T) < \kappa \). Hence, from (5.2.8), the optimal controller \( u(t) = 1 \) in a subinterval towards the end of \( (0 \ldots T) \). Now if \( \varphi \) has no \( \kappa \)-crossing point then \( u(t) = 1 \) throughout \( (0 \ldots T) \). If \( \varphi \) has one \( \kappa \)-crossing point, say \( t_1 \in (0 \ldots T) \), then \( u = u_{\text{min}} \) in \( (0 \ldots t_1) \) and \( u = 1 \) in \( (t_1 \ldots T) \). Finally, if \( \varphi \) has two \( \kappa \)-crossing points, since \( \varphi(T) < \kappa, \varphi(t) - \kappa \) must change its sign from negative to positive at some time \( 0 < t_1 < T \) and then back to negative at some later time \( t_1 \) where \( 0 < t_1 < t_2 < T \). Thus, \( u(t) = 1 \) in \( (0 \ldots t_1) \), then \( u(t) = u_{\text{min}} \) in \( (t_1 \ldots t_2) \) and \( u(t) = 1 \) again after \( t_2 \).

Now let \( \varphi(T) > \kappa \). As we argued in step-2, \( \dot{\varphi} \) at \( \kappa \)-crossing points is either always negative, or is decreasing between consecutive \( \kappa \)-crossing points. This shows that the case of \( \varphi \) crossing down \( \kappa \) and then crossing back up \( \kappa \) is not possible since that would require \( \dot{\varphi} \) at its \( \kappa \)-crossing points to be strictly increasing. Thus either \( \varphi \) always stays above \( \kappa \) in which case \( u = u_{\text{min}} \) throughout, or
\( \varphi \) crosses \( \kappa \) up once, which is the case in which \( u \) switches from \( u = 1 \) to \( u_{\text{min}} \). Similar arguments apply for the case of \( \varphi(T) = \kappa \), depending whether \( \varphi(t) > \kappa \) or \( \varphi(t) < \kappa \) as \( t \) approaches \( T \). This completes step-3 and thus proves the theorem for strictly concave \( h \).

We now consider linear \( h \), i.e., \( h(u) = 1 - u \), and use the optimal control characterization in (5.2.9). Following similar footsteps that lead to eq. (5.3.4), and using the fact that here \( H = \dot{I}(C - \gamma \dot{\lambda}_2) + 1 \), we obtain:

\[
\dot{\varphi} = -\beta \dot{S}(H - 1) - \gamma.
\]

The proof is otherwise similar to that for strictly concave \( h \), with \( \kappa \) replaced with 1.

**Remark 5.3.1.**

**I:** \( H \geq -\frac{\gamma \kappa}{\beta (1 - I_0)} + \kappa \). Then \( \dot{\varphi} < 0 \). This follows from (5.3.4), and since \( 0 < S < S_0 = 1 - I_0 \) (Corollary 1). The negativity of \( \dot{\varphi} \) along with the fact that \( \varphi \) is a continuous function of time, according to property 3, show that there can be at most one switch in the sign of \( \varphi - \kappa \), and hence the optimal \( u(\cdot) \) has at most one jump. Recall from (5.3.5) that \( \varphi(T) = 0 < \kappa \). Thus, if \( \varphi(0) = \beta I_0 S_0 (\lambda_2(0) - \lambda_1(0)) < \kappa \) then \( u(t) = 1 \) for \( t \in [0, T] \). If, on the other hand, \( \varphi(0) > \kappa \), then it follows from the Intermediate Value Theorem (IVT) that \( u(\cdot) \) jumps from \( u_{\text{min}} \) to 1 in \( (0, T) \).

**II:** \( H < -\frac{\gamma \kappa}{\beta (1 - I_0)} + \kappa \). This therefore constitutes a necessary condition for the optimal control to have two jumps. According to (5.2.3) and (5.3.2), \( H = H(T) = CI(T) + h(u(T)) + \varphi(T)u(T) - \gamma \lambda_2(T)I(T) \). Also, from (5.1.2b) and following the argument in the proof of lemma 5.2.1, we have \( I(T) \geq I_0 e^{-\gamma T} \). The necessary condition therefore is:

\[
I_0 e^{-\gamma T} C < -\frac{\gamma \kappa}{\beta (1 - I_0 - R_0)} + \kappa,
\]

which, for instance, requires \( \beta (1 - I_0 - R_0) > \gamma \).

**5.3.2 Strictly convex \( h(u) \):**

**Theorem 5.3.2.** Let Phases 1 and 2 be defined as follows.
**Phase 1:**

a. \( u(t) = 1 \), on \( 0 \leq t < t_1 \leq T \) for some \( t_1 \geq 0 \);

b. \( u(t) \) strictly and continually decreases on \( t_1 \leq t < t_2 \leq T \) for some \( t_2 \geq t_1 \);

c. \( u(t) = u_{\text{min}} \) on \( t_2 \leq t \leq t_3 \) for some \( t_2 \leq t_3 \leq T \).

**Phase 2:**

a. \( u(t) \) strictly and continually increases on \( t_3 \leq t \leq t_4 \leq T \) for some \( t_3 \leq t_4 \leq T \);

b. \( u(t) = 1 \) on the interval \( t_4 \leq t \leq T \).

For strictly convex \( h \), an optimal \( u(t) \) is a **continuous** function consisting of

- Only Phase 1, or

- Only Phase 2, or

- Phase 1 followed by Phase 2.

Qualitatively, the optimal controller for strictly convex \( h(\cdot) \) shows similar pattern of up to two transitions between a maximum and minimum value as that for concave \( h(\cdot) \). The transitions are however smooth for strictly convex \( h(\cdot) \) as a slight increase in \( u \) from \( u_{\text{min}} \) decreases the cost due to QoS and hence the overall cost significantly. In contrast, for a concave \( h(u) \), the decrease in the overall cost as a result of a slight increase in the value of \( u \) is insignificant and if it is at all beneficial to increase \( u \) so as to enhance QoS, it is better to increase it to the maximum possible value of 1.

**Proof of Theorem 5.3.2.** We use the optimal control characterization in (5.2.10). It follows from the continuity of \( \varphi \) that the optimal \( u \) is a continuous function of time. Thus the state and co-state functions and thus any differentiable function of them, e.g. \( \varphi \), is differentiable throughout \((0\ldots T)\).
Note that due to strict convexity and decreasing properties and assumptions on \( h \), we have 
\[ 0 < -h'(1) < -h'(u_{\text{min}}) \]. The following key lemma can be validated similar to the steps 1 and 2 of the proof of theorem 5.3.1:

**Lemma 5.3.3.** Consider any \( L > 0 \). (i) \( \varphi \) cannot be equal to level \( L \) over an interval of nonzero length. (ii) \( \varphi = L \) for at most three time epochs. (iii) \( \varphi \) crosses any level \( L \) at most at two time epochs in \((0 \ldots T)\). Moreover, (iv) \( \dot{\varphi} \) either is negative at these \( L \)-crossing points or is decreasing between consecutive \( L \)-crossing points.

Thus, there exists at most one interval of nonzero length on which \( \varphi > L \) for any level \( L > 0 \) (e.g., \( L = -h'(1) \)). Otherwise \( \varphi \), as a differentiable function of time, either has to cross \( L \) more than twice, or has to be at \( L \) for an interval of positive length, or has to cross \( L \) down and then above which requires \( \dot{\varphi} \) to be non-decreasing between its consecutive \( L \)-crossing points. However, all of these cases would contradict the above lemma.

**Lemma 5.3.4.** \( \dot{\varphi} = 0 \) at at most one time epoch during the (only possible) interval on which \( \varphi > -h'(1) \).

**Proof.** Suppose \( \dot{\varphi} \) is zero at \( t_1, t_2 \) in the interval on which \( \varphi > -h'(1) > 0 \), and \( t_1 < t_2 \). Since from lemma 5.2.1, \( IS \) is never zero, from the expression for \( \dot{\varphi} \) in (5.3.1) we must have:

\[ C - \lambda_1(t_1) \gamma = 0 = C - \lambda_1(t_2) \gamma. \quad (5.3.6) \]

Hence

\[ \lambda_1(t_1) = \lambda_1(t_2). \quad (5.3.7) \]

The relation for \( \dot{\lambda}_1 \) in (5.2.2) can be rewritten as follows:

\[ \dot{\lambda}_1 = -\frac{\varphi u}{S} \]

Note that \( \varphi u > 0 \) over \((t_1 \ldots t_2)\). Thus \( \lambda_1 \) is strictly decreasing during this interval. This contradicts (5.3.7). \( \square \)
Next, from (5.2.10),
\[
\frac{du}{dt} = \begin{cases} 
  h^\prime(h^{-1}(-\varphi)), & -h^\prime(1) < \varphi(t) < -h^\prime(u_{\text{min}}) \\
  0, & \text{otherwise}.
\end{cases}
\] (5.3.8)

The above relation shows that on the interval over which 
\(-h^\prime(1) < \varphi(t) < -h^\prime(u_{\text{min}})\), \(\dot{u}\) has the opposite sign of \(\dot{\varphi}\) and over such intervals \(\dot{u} = 0\) only if \(\dot{\varphi} = 0\).

If \(\varphi \leq -h^\prime(1)\) throughout \([0 \ldots T]\), then (5.2.10) implies that \(u = 1\) throughout and we only have phase 2-b. Otherwise, there exists exactly one interval, denoted as \((\nu_1 \ldots \nu_2)\), \(0 \leq \nu_1 < \nu_2 \leq T\), such that \(\varphi > -h^\prime(1)\) in \((\nu_1 \ldots \nu_2)\), and \(\varphi \leq -h^\prime(1)\) at \(t \leq \nu_1\) and \(t \geq \nu_2\). Thus, referring to (5.2.10), \(u = 1\) over the intervals \([0 \ldots \nu_1]\) and \([\nu_2 \ldots T]\), which respectively correspond to phases 1-a and 2-b. Second, Lemmas 5.3.3 and 5.3.4 imply that on the interval over which \(\varphi > -h^\prime(1) > 0\), i.e., \((\nu_1 \ldots \nu_2)\), \(\varphi\) is either (A) always strictly decreasing; (B) always strictly increasing; or (C) strictly increasing on a sub-interval \((\nu_1 \ldots \nu_3)\) and strictly decreasing during \((\nu_3 \ldots \nu_2)\).

Here, we investigate case (A). Similar arguments can be made about cases (B) and (C). In case (A), \(\nu_1 = 0\). Now either (i) \(\varphi \leq -h^\prime(u_{\text{min}})\) throughout \((0 \ldots \nu_2)\); or (ii) \(\varphi > -h^\prime(u_{\text{min}})\) on \((0 \ldots \nu_4)\), then \(\varphi \leq -h^\prime(u_{\text{min}})\) on \((\nu_4 \ldots \nu_2)\). For case (i), \(u\) is strictly increasing over \([0 \ldots \nu_2]\), and assuming \(\nu_2 < T\), then \(u = 1\) over \([\nu_2 \ldots T]\) (phase 2-a followed by phase 2-b). If \(\nu_2 = T\), phase 2-b has length zero.

On the other hand, for case (ii), assuming \(\nu_2 < T\), we have \(u = u_{\text{min}}\), over \([0 \ldots \nu_4]\) (phase 1-c), then \(u\) strictly increases over \([\nu_4 \ldots \nu_2]\) (phase 2-a), then \(u = 1\) over \([\nu_2 \ldots T]\) (phase 1-c). Again, if \(\nu_2 = T\), phase 2-b has length zero.

\[\square\]

5.4 Distribution of patches through the underlying network

Security patches may themselves be compromised unless they are obtained directly from trusted resources such as authorized access points, or trained human agents. Nevertheless, we still investigate the alternative (less secure) distribution of the patches through the underlying wireless
network. In this case, decreasing the reception gain of the susceptible nodes can increase the delay in delivery of the patches. We therefore replace the recovery rate $\gamma$ with $\gamma_0 + \gamma_1 u$ where $\gamma_1 \geq 0$, and show that theorem 5.3.1 extends. The differential equation for $I$ in (5.1.2b) changes to:

$$\dot{I} = \beta u IS - \gamma_0 I - \gamma_1 u I.$$ 

The Hamiltonian in (5.2.1) is updated as follows:

$$H = CI + h(u) + (\lambda_2 - \lambda_1) \beta u IS - \lambda_2 \gamma_0 I - \lambda_2 \gamma_1 u I.$$ 

If we update the definition of $\varphi$ in (5.2.5) as

$$\varphi \triangleq \beta IS(\lambda_2 - \lambda_1) - \lambda_2 \gamma_1 I,$$

the optimal $u$ may be characterized as in (5.2.8) and (5.2.9). Rewriting the Hamiltonian using the definition of $\varphi$ yields:

$$H = CI + h(u) + \varphi u - \lambda_2 \gamma_0 I.$$ 

Since the system is autonomous, $H$ is a constant. Hence,

$$H = H(t^+) = H(t^-) = C \bar{I} + \kappa - \dot{\lambda}_2 \gamma_0 \bar{I}. \quad (5.4.1)$$ 

At $t_\kappa$ we have:

$$\varphi(t_\kappa) = (\dot{\lambda}_2 - \dot{\lambda}_1) \beta \bar{I} \bar{S} - \dot{\lambda}_2 \gamma_1 \bar{I} = \kappa. \quad (5.4.2)$$

The co-state equation for $\dot{\lambda}_2$ changes to the following:

$$\dot{\lambda}_2 = -C - (\lambda_2 - \lambda_1) \beta S + \lambda_2 (\gamma_0 + \gamma_1 u).$$

The time derivative of $\varphi$ turns out to be:

$$\dot{\varphi} = -\beta I S C + \beta I S \lambda_1 \gamma_0 + \gamma_1 I C. \quad (5.4.3)$$

89
Hence,

\[ \dot{\phi}(t^-) = \dot{\phi}(t^+) \]

\[ = -\beta \ddot{S} + \gamma_1 \dot{I}C \]

\[ + (\lambda_2 - \frac{\kappa + \lambda_2 \gamma_1 \ddot{I}}{\beta \ddot{S}}) \beta \ddot{S} \gamma_0 \quad \text{[from (5.4.2)]} \]

\[ = -\beta \ddot{S} + \lambda_2 \beta \ddot{S} \gamma_0 + \gamma_1 \dot{I}C - \gamma_1 \lambda_2 \gamma_0 \ddot{I} - \kappa \gamma_0 \]

\[ = -\beta (\ddot{I}C - \lambda_2 \gamma_0 \ddot{I}) \ddot{S} + \gamma_1 (\ddot{I}C - \lambda_2 \gamma_0 \ddot{I}) - \kappa \gamma_0 \]

\[ = -\beta (H - \kappa) \ddot{S} + \gamma_1 (H - \kappa) - \kappa \gamma_0. \quad \text{[from (5.4.1)]} \]

Therefore, \( \dot{\phi}(t^-) \) and \( \dot{\phi}(t^+) \) are linear in \( \ddot{S} \) and theorem 5.3.1 can be established using similar arguments as in subsection 5.3.1.

### 5.5 Implementation and practical issues

Dynamic control of the reception gain of the nodes is possible through control of antenna gains, which may be realized through the use of smart antennas and adaptive antenna arrays (see e.g. [55, 60]). A simple example for circuitry and algorithms for achieving controllable gain at the receiver end of adaptive antennas is presented in [21]. Such smart antennas have been implemented e.g. by Ericsson and Mannesmann Mobilfunk [4], and are expected to be more pervasive in wireless devices in near future. Note that it may not be possible to adjust antenna gains up to arbitrary precision, and in practice, only a few quantized gain levels may be available. This does not lead to any sub-optimality when the \( h(\cdot) \) function is concave, since as we proved, the optimal \( u \) in this case is either at \( u_{min} \) or 1 during different intervals. For a strictly convex \( h(\cdot) \), quantization may however lead to sub-optimality as the optimal \( u \) may assume any intermediate value between \( u_{min} \) and 1. Nevertheless, our numerical computations presented in the next section reveal that the above sub-optimality is insignificant.

In absence of adaptive antennas, reduction of reception gain may be achieved by simply re-
jecting some of the communication requests. In this case $u$ is the fraction of communication requests accepted by each node. In more details, here the rate of contacts of each pair of node is \( \frac{2w\alpha E[V^*]}{A} \) where \( \alpha \) is the communication range of the nodes which is now fixed. However, only a fraction $u$ of such contacts result in successful communication. Hence the rate of permitted communication between susceptible and infective nodes is \( \frac{2w\alpha E[V^*]}{A} u \), and hence the governing system of differential equations is the same as before with \( \beta = \frac{2w\alpha E[V^*]}{A}. \)

Recall that the optimal control for the case of concave $h$ is completely specified by (at most two) jump points, and for a strictly convex $h$ consists of at most two phases, characterized by at most four time epochs. Thus, the reception gain may be optimally controlled by the nodes without any local or global coordination or information exchange once they know these transition epochs. Upon detection of a new malware in the network, a central surveillance can assess the cost coefficients $C, K$, the rate of recovery $\gamma$, and estimate (or may already have an estimate of) the spread rate $\beta$ of messages from the mobility pattern and the density of the nodes etc. Switching epochs can then be calculated and distributed with small communication overhead at time zero. Alternatively, nodes can receive the estimated parameters from the central surveillance and calculate the epochs themselves.

### 5.6 Numerical computations

We first develop some intuition about the trends of changes in the structure of the optimum control as a result of changes in values of parameters $\beta, I_0, R_0, K, C$. We subsequently demonstrate that overall costs can be substantially lowered by using dynamic optimal reception gain control as compared to static gain control. Moreover, through simulations, we demonstrate how a heuristic policy which utilizes approximate and temporally evolving state information in a node’s neighborhood (hence a node-specific policy) compares to our dynamic optimal policy which requires only one time estimates of the system parameters. Finally, we demonstrate that
Figure 5.2: Optimal $u$, varying $K$. The $h(u)$ functions used for concave and convex cases are $0.5(1-u)$ and $(1-u)^{1.2}$, respectively. Other parameters are $u_{\text{min}} = 0.1, \gamma = 0.2, \beta = 0.4, R_0 = 0$ and $C = 1$.

- The dynamic optimal policy is robust to errors in the above estimates, and also to quantization errors in gain control.

As fig. 5.2 reveals, the optimal control becomes more conservative (selects lower values) for higher values of $K$. However, an interesting phenomenon is that increasing $I_0$ does not necessarily lead to more conservative defense policy. In fact, the defense policy chooses progressively lower values of $u$, when $I_0$ is increased up to a certain value, but once $I_0$ exceeds this threshold the defense barely deviates $u$ from the normal value of 1. This is because for large $I_0$ the defense’s efficacy is so low that reducing the reception gain does not help the containment but only deteriorates the QoS. The optimal controller becomes more conservative for higher and lower values of $\beta, \gamma$ respectively (fig. 5.3 and fig. 5.4). Finally, for large $C$, $u$ is reduced earlier so as to reduce the time-accumulative cost associated with the infectives (and increased earlier too to provide the desired QoS) (fig. 5.5). Also, as all the above figures reveal, for concave $h$, usually the optimal $u$ is either at 1 throughout or jumps once from $u_{\text{min}}$ to 1. But, scenarios where it has two jumps
does indeed arise (Fig. 5.6).

Fig. 5.7 compares the overall costs inflicted by the optimal dynamic policy versus the best static policy, as a function of $\beta$. A static policy is one in which the same value of reception gain is used throughout and we have optimized this fixed value to obtain the best static policy. Our dynamic policy achieves substantially lower costs except when $\beta$ is small; in the latter case its choice is largely static ($u \approx 1$ most of the time).

As we discussed before, a node usually does not have information about the states of those that it contacts. However, by monitoring the anomalous increase in the media access activity as a result of attempts of infective nodes to spread the malware, a node may be able to estimate the number of infectives in its neighborhood. This estimate, however, depends on measurements over fading channels in a network whose topology is constantly changing due to mobility. Hence, these estimates have limited accuracy and are fraught with random errors. An important question that remains to be answered then is whether and how nodes can utilize this noisy information about the number of infective nodes in their neighborhood, even at the cost of higher
signal processing and computations. In order to assess the usefulness of these noisy estimates, we develop a heuristic node-specific policy that utilizes the available information, and compare its efficacy against our dynamic optimal control through simulation. In the heuristic policy, each node estimates the number of infective nodes in its neighborhood; however, the state of each neighbor is not flawlessly known. In the simulation, we modeled this imprecision in detection by adding a Gaussian noise with mean zero and power $\sigma^2$ to the indicator that a node is infective or not. Upon contact by one of its neighbors, the receptive node blocks the communication, by reducing its reception gain to $u_{\text{min}}$, if the estimated fraction of infected nodes in its vicinity is greater than a certain threshold. (We consider $u_{\text{min}}$ very close to 0 and hence when $u = u_{\text{min}}$, the communication is effectively blocked). This policy can be optimized over the selected threshold and the size of the sensing area which determines the set of neighbors. Specifically, at any given time $t$, the neighbors of a node are those who are in contact with it in a time window $(t - \Delta \ldots t + \Delta)$, and $\Delta$ depends on the size of the sensing area and node velocity. We choose $\Delta$ (as also the decision threshold) so as to minimize the overall cost incurred by the heuristic policy.
Our dynamic optimal control blocks communications at all times at which the optimal $u$ equals $u_{\text{min}}$ (as again $u_{\text{min}} \approx 0$) and accepts communications otherwise (since the optimal $u$ equals 1 otherwise). We ran the simulations for $N = 50$ nodes over a period of $T = 20$, with $\beta = 0.5$, $\gamma = 0.2$, $I_0 = 0.2$ (i.e., $n_I(0) = 0.2 \times 50 = 10$), $C = 10$, $K = 0$, $h(u) = 1 - u$, and considering exponentially distributed inter-contact times, with parameter $\hat{\beta} = \beta/N$ (refer to Section 5.1, 3rd para), as is the case for random waypoint and random direction mobility models ([8, 58]). The overall cost is calculated for both the heuristic policy and our dynamic policy through simulation as follows: the cost of infectives ($\int_0^T CI \, dt$ in (5.1.5)) is obtained by integrating ($C$ times) the fraction of infectives over time and the cost due to reduction of $u$ is considered as the fraction of blocked communications. The latter corresponds to $h(u) = 1 - u$, as when $u = u_{\text{min}} \approx 0$ ($u = 1$, respectively) every contact results in a blocked (successful, respectively) communication and incurs unit (0, respectively) cost as per the $h(.)$ function. As fig. 5.8 reveals, the heuristic policy attains slightly lower costs than our optimal control policy, which does not use any local or global state information, for small estimation errors. This better performance is due to avoiding unnecessary
blocking of communication and hence not losing too much of QoS. However, as the estimation
noise increases this advantage quickly diminishes and in fact our dynamic policy significantly
outperforms the heuristic. Hence, considering the computation overhead that state estimations
introduces and since accuracy in such estimates is hard to achieve, our dynamic policy which
requires no state information is preferable.

In order to calculate our dynamic policy, one requires a one time (as opposed to a continuous
estimation of the state) estimate of the parameters of the system, e.g., $\beta, I_0$ etc. Here, we demon-
strate that the cost achieved by our dynamic policy is robust to errors in estimation of these
parameters. Suppose that $\beta$ equals 0.5 but the optimal control is calculated based on an estimate
that is somewhere between 0.35 and 0.65. Fig. 5.9(a) reveals that the increase in the overall cost as
a result of inaccurate estimation of $\beta$ up to 30% is less than 6%. Similar observation holds about
$I_0$: as fig. 5.9(b) depicts, up to 75% error in the estimation of $I_0$ results in less than 2.5% increase
in the cost incurred by our dynamic policy. Finally, as we pointed out in the previous section,
the reduction of communication rates may only be possible at quantized levels, which leads to
sub-optimality only when the $h(.)$ function is strictly convex. The quantization of $u$ however only
minimally increases the overall cost: as Fig. 5.9(c) and 5.9(d) show that even when the number of
levels is only 2 (and thus the controller is bang-bang), the increase in cost is less than 3%.
Figure 5.7: Cost comparison: optimum dynamic versus the static policies. The parameters are $T = 25$, $u_{\text{max}} = 1$, $u_{\text{min}} = 0.1$, $\gamma = 0.2$, $I_0 = 0.2$, $C = 5$, $K = 50$ and $h(u) = 1 - u$.

Figure 5.8: Comparison of the costs achieved by our dynamic optimal control and a heuristic control that uses (noisy) local state information.
Figure 5.9: The first two figures respectively demonstrate the robustness with respect to $\beta$ and $I_0$ respectively for $h(u) = 1 - u$. The last two figures demonstrate robustness with respect to quantization in the control for $h(u) = (1 - u)^{1.5}$. In the last figure, the $x$-axis represents the number of levels available for $u$, and the control is rounded to the level closest to the optimal value, e.g., $x = 2$ means the output is rounded to $u_{\text{min}}$ and 1. The other parameters for all the figures are $\beta = 0.5, I_0 = 0.2, R_0 = 0, \gamma = 0.2, u_{\text{min}} \approx 0, u_{\text{max}} = 1, C = 10, T = 20$. 
Chapter 6

Patching

Introduction

The spread of contagion in mobile wireless networks can be countered by immunization and healing. Specifically, the underlying vulnerability utilized by the worm, can be amended by installing security patches [78] that immunize the susceptible, and heal and immunize the infective nodes. However, the distribution of the patches burdens the limited available bandwidth, and hence if not carefully controlled, can become a menace itself. The adverse effect of application of countermeasures is aggravated in wireless networks as the media being shared and consequently bandwidth limitations are more stringent. In the first chapter of this part, we introduced the reduction of reception gain of the nodes as a defense mechanism and studied its optimal control, while keeping the patching rates constant. Here, we investigate the dynamic control of patching as the second defense mechanism to attain desired trade-offs.

We consider non-replicative and replicative settings for dissemination of the security patches in a mobile wireless network. In the non-replicative model, a number of mobile (or stationary) nodes, referred to as dispatchers, are pre-loaded with the security patch, and deliver the patch to other nodes upon contact. Recall that an instance of contact can refer to a physical proximity of a
pair of nodes such that they enter the communication range of each other, or can simply refer to an instance of communication in an MMS network. The susceptible and infective receptors subsequently become immune to the contagion, and are referred to as recovered. In the replicative model, the receptors, in addition, become dispatchers themselves - thus the dispatchers replicate. In each model, the trade-off between bandwidth consumption and security can be controlled by activating only a desired fraction of dispatchers and also regulating the rate at which they transmit packets. Activation of more of such nodes and increasing their rates of transmission accelerate both the spread of the security patch and the bandwidth consumption in transmission of patches. The activation fraction and the transmission rates can either be selected statically (that is once at the start of network operation), or varied dynamically. The dynamic control of the above decision variables is likely to be more effective in obtaining the desired trade-offs, while the static may be easier to implement. Quantification of security risks and the bandwidth consumption costs and identification of optimal decisions in each model are therefore imperative for evaluating their relative efficacy.

First, we model the dynamics of the spread of the worm in mobile wireless networks in presence of arbitrary dynamic dispatcher activation and transmission rate control policies, and quantify the costs associated with the corresponding security risks and additional bandwidth consumptions (§6.1). The dynamics depend on whether the dissemination of security patches is replicative or non-replicative. We formulate the dynamic activation of the dispatchers and setting their communication rates as an optimal control problem that seeks to minimize the above overall cost and develop a framework for numerically computing the optimal policies.

Second, using Pontryagin’s Maximum Principle and some simple real analysis observations, in both non-replicative and replicative models, we prove that optimal policies have simple structures: for a concave bandwidth consumption cost, activate all dispatchers and choose the maximum possible transmission rate for them until a certain time; subsequently all dispatchers must be de-activated until the end of the network operation period (§§6.2,6.3). We have therefore
shown that the optimal control is bang-bang with at most one jump that terminates at the minimum possible value. Optimality of a bang-bang control and the quantification of the number of jumps to be at most one, are established despite the facts that the network state evolutions do not constitute monotonic functions of time, and involve non-linear dynamics, and the cost functions are not assumed to be linear. The optimal control has a similar structure for a convex bandwidth consumption cost, except that its transition from the maximum to minimum values is (strict but) continuous rather than abrupt.

Finally, using numerical evaluation, we assess the relative efficacy and robustness of the replicative and non-replicative dispatch and static and dynamic optimal controls (§6.5). We demonstrate that the optimum dynamic control incurs significantly lower aggregate costs and is more robust against parameter estimation errors and implementation inaccuracies than the best-static control in both replicative and non-replicative settings. Moreover, replicative dynamic dispatch incurs a substantially lower aggregate cost than dynamic non-replicative dispatch.

6.1 System model

6.1.1 Non-replicative dispatch

System Dynamics

A fraction $R_0$ of nodes, referred to as dispatchers, are pre-loaded with security patches. A dispatcher can be stationary such as a base-station or an access point in a 3G/4G cellular network, or a roaming agent as in a delay-tolerant network (DTN). The dispatchers are immune to infection themselves and are therefore always in the recovered state. The dispatchers can transmit the patches to the susceptible and infective nodes and immunize the susceptibles and possibly heal the infectives to the recovered state.

Recall that $S(t) + I(t) + R(t) + D(t) = 1$. One can therefore represent the system using any
three of the above states: we choose \((S, I, D)\). At the start of the recovery process, that is at time zero, some but not all nodes are infected: \(0 < I(0) = I_0 < 1\), and WLoG only the dispatchers are in the recovered state: \(R(0) = R_0, 0 < R_0 < 1, I_0 + R_0 < 1\), and WLoG no node is dead: \(D(0) = 0\). Thus, \(S(0) = 1 - I_0 - R_0\).

As before, two nodes are said to be in contact whenever they communicate. Following the description of assumptions in Chapter 2, specifically the homogeneous mixing property, each pair of infective-susceptible nodes contact at rate \(\hat{\beta}\). A dispatcher initiates a communication with another node at a possibly different rate \(\tilde{\beta}\). Let the fraction of activated dispatchers at time \(t\) be \(\varepsilon(t)\). Upon a contact between an activated dispatcher and another node at time \(t\), the security patch is transmitted from the dispatcher to the receiver node with probability \(u(t)\) which we refer to as the patch transmission rate. Note that, as we alluded to in Chapter 2, distinction between an infective node and a susceptible node is difficult a priori. Indeed, we assume that from the system’s point of view, information about whether or not a node is infective, is not available to that node or to any other node. Therefore, information about the state of the nodes which a dispatcher communicates with is either nonexistent or at best represents a statistics about the average state of the whole network, which is identical for all dispatchers. Hence, at any given time \(t\), the selection of which dispatchers to be activated is nonspecific (as long as the fraction of activated ones is \(\varepsilon(t)\)), and the activated dispatcher nodes use the same \(u(t)\), as opposed to an individual based strategy. Nevertheless, the fraction of activated dispatchers \(\varepsilon\) and the rate of dispatching \(u\) can be allowed to vary with time, \textit{i.e.}, selected dynamically, though identically among individual nodes. In fact as we demonstrate in \(\S6.5\), such dynamic selections substantially enhance the efficacy of the countermeasure. Implementation of such dynamic policies, however, may require global coordination among the dispatchers. But as we will prove later (\(\S\S6.2,6.3\)), optimal strategies follow very simple structures which make them amenable to implementation. Moreover, as our numerical computations in Appendix A suggest, the overall cost is robust against drifts in the local clocks of the dispatchers.
If the receptor of a security patch is a susceptible node, it installs the security patch, is subsequently immunized, and its state changes to recovered. If however the receptor is an infective, the patch may fail to heal it, or, the worm may obstruct or delay its installation. As we mentioned in chapter 2, we capture the above possibility, by introducing a coefficient \( 0 \leq \pi \leq 1 \). \( \pi = 0 \) corresponds to the case where the patch is completely unable to remove the worm from infectives, and only immunizes the susceptibles, whereas \( \pi = 1 \) represents the other extreme scenario where a patch can equally well immunize and heal susceptibles and infectives, and intermediate values of \( \pi \) represent probabilistic or delayed recovery for infectives. Let \( \vartheta(t) := u(t)\varepsilon(t) \),

and let

\[
\beta_0 := \lim_{N \to \infty} N \times \beta, \quad \beta_1 := \lim_{N \to \infty} N \times \hat{\beta}.
\]

Now the evolution of the state of the system can be modeled as the following system of differential equations:

\[
\dot{S}(t) = -\beta_0 I(t)S(t) - \beta_1 \vartheta(t)R_0 S(t)
\]

\[
\dot{I}(t) = \beta_0 I(t)S(t) - \pi \beta_1 \vartheta(t)R_0 I(t) - \delta I(t)
\]

\[
\dot{D}(t) = \delta I(t)
\]

with initial constraints:

\[
I(0) = I_0, \quad S(0) = 1 - I_0 - R_0, \quad D(0) = 0
\]

and also satisfy the following constraints at all \( t \):

\[
0 \leq S(t), I(t), D(t), \quad S(t) + I(t) + D(t) \leq 1.
\]

**Aggregate Cost**

The network may suffer over time from the infected hosts, used by the worm to (i) eavesdrop and analyze and/or (ii) alter or destroy the traffic that is generated or relayed by the infected
hosts. An attacker also inflicts cost by killing nodes. At each time \( t \), the network incurs a cost at the rate of \( f(I(t)) \) due to the presence of the infectives, and \( g(D(t)) \) owing to the loss of nodes through mortality, where \( f(.) \) is a non-decreasing, twice-differentiable, convex function of \( I \) such that \( f(0) = 0 \) and \( f(I) > 0 \) for \( I > 0 \), \( g(.) \) is a non-decreasing differentiable function of \( D \) such that \( g(0) = 0 \).

Here, we motivate a cost function based on the overall bandwidth consumed through dissemination of the security patches. Recall that there are a total of \( NR_0 \) dispatchers, \( \varepsilon(t) \) fraction of them are activated at time \( t \), which transmit the patches at rate \( u(t) \). Thus the total rate of bandwidth consumed for distribution of the patches at time \( t \) is directly proportional to \( \varepsilon(t)u(t)R_0 = \vartheta(t)R_0 \). The network incurs a cost at rate \( h(R_0\vartheta(t)) \) due to the above bandwidth consumption, where \( h(x) \) is a twice-differentiable and increasing function in \( x \) such that \( h(0) = 0 \) and \( h(x) > 0 \) when \( x > 0 \). Note that the assumptions on \( f(.) \), \( g(.) \), \( h(.) \) are mild and natural and a large class of functions satisfy them.

The aggregate network cost therefore is:

\[
J = \int_0^T [f(I(t)) + g(D(t)) + h(R_0\vartheta(t))] \, dt. \tag{6.1.5}
\]

Since \( J \) depends on the integration of \( f(I(t)) \) and \( g(D(t)) \) over time, \( J \) is minimized not only when the levels of infection and dead are suppressed, but also when this is accomplished early. Since \( J \) depends on the bandwidth consumption through the integration of the \( h(\cdot) \) function, the minimization of \( J \) attains desired trade-offs between the speed of infection control and the bandwidth consumed in patching.

Once the function \( \vartheta(\cdot) \), hereafter denoted as the immunization rate function, is selected, the system state vector \((S, I, D)\) is specified at all \( t \) as a solution to (6.1.2) and (6.1.3), and hence the aggregate cost \( J \) is determined as well. Thus, the control \( \vartheta(\cdot) \) is considered only as a function of time rather than that of the system states, and \( J \) is denoted as \( J(\vartheta) \) instead. The system seeks

---

\(^1\)The cost function can also have terms depending on the final concentration of the infective and the dead nodes.
to minimize the aggregate cost $J(\vartheta)$ by appropriately regulating the immunization rate function $\vartheta(t)$ subject to $0 \leq \vartheta(t) \leq \vartheta_{\text{max}}$ for all $t \in [0, T]$. The bounds on $\vartheta(t)$ arise since $0 \leq \varepsilon(t) \leq 1$ and $0 \leq u(t) \leq u_{\text{max}}$ due to physical constraints of the dispatcher devices. With appropriate scaling by choice of $\beta_1$, we can assume $\vartheta_{\text{max}} = 1$. Thus,

$$0 \leq \vartheta(t) \leq 1 \text{ for all } t \in [0, T].$$

(6.1.6)

**Definition 1.** An immunization rate function $\vartheta(\cdot)$ is called an admissible control if (i) $\vartheta(\cdot)$ satisfies (6.1.6), and (ii) $\vartheta(\cdot)$ is piecewise continuous such that the left and right hand limits exist at the points of discontinuity. A pair of state and control functions $((S(\cdot), I(\cdot), D(\cdot)), \vartheta(\cdot))$ is called an admissible pair if (i) $\vartheta(\cdot)$ is an admissible control and (ii) the pair satisfies (6.1.2), (6.1.3).

We soon show in lemma 6.1.1 that for any admissible pair of state and control functions, the state constraints in (6.1.4) are automatically satisfied throughout $(0 \ldots T]$. Hence, we ignore (6.1.4) and pose the optimal control problem as follows:

**Problem Statement 1 (Minimum cost immunization).** Let $((S(\cdot), I(\cdot), D(\cdot)), \vartheta(\cdot))$ be an admissible pair. If $J(\vartheta) \leq J(\bar{\vartheta})$ for any admissible control $\bar{\vartheta}(\cdot)$ then $((S(\cdot), I(\cdot), D(\cdot)), \vartheta(\cdot))$ is called an optimal solution and $\vartheta(\cdot)$ is called an optimal control or the optimal immunization rate function and $J(\vartheta)$ the minimum cost under non-replicative dispatch.

**Lemma 6.1.1.** Any admissible pair of state and control functions $((S(t), I(t), D(t), \bar{\vartheta}(t)))$, satisfies the state constraints in (6.1.4) in $[0, T]$ interval. Moreover, all constraints except $D(t) \geq 0$ are satisfied in the strict form in $[0, T]$.

**Proof.** First, let $\delta > 0$. Since $0 < I_0 + R_0 < 1$, $I_0, R_0 > 0$ the initial conditions in (6.1.3) ensure that all constraints (6.1.4) are strictly met at $t = 0$, except that $D(0) = 0$. The lemma follows if we show that all constraints in (6.1.4) are strictly satisfied in $(0, T]$.

All $S(\cdot), I(\cdot)$ and $D(\cdot)$, resulting from (6.1.2) are continuous functions of time. Thus, since $S(0), I(0) > 0$ and $S(0) + I(0) + D(0) = 1 - R_0 < 1$, there exists an interval $(0, t_0)$ of nonzero length
on which both $S(t)$ and $I(t)$ are strictly positive and $S(t) + I(t) + D(t) < 1$. Thus, from (6.1.2) and (6.1.3), $\dot{D}(t) > 0$ in $[0, t_0)$. Thus, from (6.1.3), $D(t) > 0$ in $(0, t_0)$. Thus, (6.1.4) is strictly satisfied in $[0, t_0)$.

Now, suppose that the constraints in (6.1.4) are not strictly satisfied in $(0, T]$. Then, there exists a time $t_1$ which is the first time after $t = 0$ at which, at least one of the constraints in (6.1.4) becomes active. That is, we have (i) $S(t_1) = 0$ OR (ii) $I(t_1) = 0$ OR (iii) $D(t_1) = 0$ OR (iv) $S(t_1) + I(t_1) + D(t_1) = 1$ AND throughout $(0, t_1)$, we have $0 < S(t), I(t), D(t)$ and $S(t) + I(t) + D(t) < 1$.

Thus, for $0 \leq t < t_1$ from (6.1.2), (6.1.3), (6.1.6) and since $R_0 < 1$, we have $\dot{S}(t) \geq -(\beta_0 + \beta_1)S(t)$. Hence, $S(t) \geq S(0)e^{-(\beta_0 + \beta_1)t}$ for all $0 \leq t < t_1$. Since $S(\cdot)$ is continuous, $S(t_1) \geq S(0)e^{-(\beta_0 + \beta_1)t_0}$. Similarly, we can show that $I(t_1) \geq I(0)e^{-(\beta_1 + \delta)t_0}$. Thus, since $S(0) > 0$, $I(0) > 0$, (i) and (ii) are ruled out. Next, from (6.1.2), $\dot{D}(t) > 0$ in $(0, t_1)$. Thus, from the continuity of $D(\cdot)$ and since $D(t) > 0$ in $(0, t_1)$, (iii) is ruled out. Again, $\frac{d}{dt}(S(t) + I(t) + D(t)) \leq 0$ in $(0, t_1)$. Thus, from the continuity of $S(\cdot), I(\cdot), D(\cdot)$ and since $S(t) + I(t) + D(t) < 1$ in $(0, t_1)$, (iv) is ruled out as well. This negates the existence of $t_1$. Thus, by contradiction, the constraints in (6.1.4) are strictly satisfied in $(0, T]$.

If $\delta = 0$, from (6.1.2) and (6.1.3), $D(t) = 0$ for all $t \in [0, T]$. Using similar arguments we can show that $S(t), I(t) > 0$ and $S(t) + I(t) < 1$ for all $t \in [0, T]$. The lemma follows.

### 6.1.2 Replicative dispatch

The dynamics of state evolution in replicative dispatch differs from the non-replicative case in only that once a node receives a security patch, it can retransmit it upon contact with other nodes. Thus, all recovered nodes become dispatchers in the replicative model, and hence the fraction of dispatchers grows to $R(t)$ at time $t$ starting from the initial value of $R_0$, whereas the fraction of dispatchers continue to be $R_0$ at all times in the non-replicative model.

Here, we represent the system using $(S(t), I(t), R(t))$ (in contrast to $(S(t), I(t), D(t))$ in the
Figure 6.1: The top figures represent the optimal controls and the bottom figures the corresponding system states as functions of time for non-replicative dispatch with concave $h(.)$. Here, $f(I) = 10I^2$, $g(D) = 20D^2$, $T = 100$, $\beta_0 = \beta_1 = 0.2$, $\delta = 0.005$, $I_0 = R_0 = 0.1$, $h(\vartheta) = 10R_0\vartheta$. Also, Left: $\pi = 0$, Right: $\pi = 1$.

The specific choices make the analysis more convenient for each case.

\begin{align*}
\dot{S}(t) &= -\beta_0 I(t) S(t) - \beta_1 \vartheta(t) R(t) S(t) \\
\dot{I}(t) &= \beta_0 I(t) S(t) - \pi \beta_1 \vartheta(t) R(t) I(t) - \delta I(t) \\
\dot{R}(t) &= \beta_1 \vartheta(t) R(t) S(t) + \pi \beta_1 \vartheta(t) R(t) I(t)
\end{align*}

with initial constraints:

\begin{align*}
I(0) &= I_0, & R(0) &= R_0, & S(0) &= 1 - I_0 - R_0,
\end{align*}

and as before $0 < I_0, R_0, I_0 + R_0 < 1$. Also,

\begin{align*}
0 &\leq S(t), I(t), R(t), & S(t) + I(t) + R(t) &\leq 1.
\end{align*}

Note that (6.1.7) differs from (6.1.2) in only that the equations for $\dot{S}(t)$ and $\dot{I}(t)$ have $R(t)$ instead of $R_0$.

The cost incurred at time $t$ due to the bandwidth consumed by the dispatchers is $h(R(t)\vartheta(t))$ (instead of $h(R_0\vartheta(t))$) in the non-replicative case. Thus, the aggregate network cost is:

\begin{equation}
J(\vartheta) = \int_0^T [f(I(t)) + g(D(t)) + h(R(t)\vartheta(t))] dt,
\end{equation}
where \( D(t) = 1 - (S(t) + I(t) + R(t)) \). Here, \( f(\cdot), g(\cdot), h(\cdot) \) satisfy the same assumptions as before.

Lem. 6.1.1 can be readily extended to the replicative case. Thus, the state constraints (6.1.9) are ignored henceforth and the optimal control problem can be posed similar to problem statement 1.

### 6.1.3 Remarks

Note that since \( R(t) \geq R_0 \) at all \( t \), we can always (dynamically) choose the value of \( \vartheta_{\text{rep}} \) in replicative setting so that \( R\vartheta_{\text{rep}} \) is equal to \( R_0 \vartheta_{\text{non-rep}} \) and hence the aggregate cost under replicative dispatch is no higher than that under non-replicative dispatch. However, comparably, replicative dispatch is more vulnerable to contamination of the patches themselves as the number of dispatchers may grow exponentially. Note that since only the initial dispatchers transmit the patches in non-replicative setting, the system can counter this threat relatively easily by securing only these dispatchers. Despite this risk, replicative dispatch constitutes a powerful defense mechanism owing to the potential offered by the growth of the dispatchers, and has therefore been investigated in communication settings such as peer-to-peer, internet [68,78] etc., but with constant dissemination rates. We will quantify the aggregate cost and compare the relative efficacy of dynamic and static policies in §6.5.

### 6.2 Optimal non-replicative dispatch

We consider the optimal control problem posed in problem statement 1 of §6.1.1. We first present a framework for numerical computation of \( \vartheta(t) \) and \( J(\vartheta) \) (§6.2.1). We subsequently prove that \( \vartheta(t) \) follows simple structures (§6.2.2).
Figure 6.2: The optimal control and the corresponding system states as functions of time for non-replicative dispatch. The parameters are the same as in fig. 6.1, except that \( h(\vartheta) = 10(R_0\vartheta)^2 \), hence a strictly convex function. Also, Left: \( \pi = 0 \), Right: \( \pi = 1 \).

6.2.1 Numerical framework

Let \( ((S, I, D), \vartheta) \) be an optimal solution. Consider the Hamiltonian \( H \), and co-state or adjoint functions \( \lambda_1(t) \) to \( \lambda_3(t) \) defined as follows:

\[
H = f(I) + g(D) + h(R_0\vartheta) + (\lambda_2 - \lambda_1)\beta_0 IS - \beta_1 R_0\vartheta\lambda_1 S - \pi\beta_1 R_0\vartheta\lambda_2 I + (\lambda_3 - \lambda_2)\delta I.
\]

(6.2.1)

\[
\dot{\lambda}_1 = -\frac{\partial H}{\partial S} = -(\lambda_2 - \lambda_1)\beta_0 I + \beta_1 R_0\vartheta\lambda_1
\]

\[
\dot{\lambda}_2 = -\frac{\partial H}{\partial I} = -f'(I) - (\lambda_2 - \lambda_1)\beta_0 S + \pi\beta_1 R_0\vartheta\lambda_2 - (\lambda_3 - \lambda_2)\delta
\]

(6.2.2)

\[
\dot{\lambda}_3 = -\frac{\partial H}{\partial D} = -g'(D).
\]

along with the transversality conditions:

\[
\lambda_1(T) = 0, \quad \lambda_2(T) = 0, \quad \lambda_3(T) = 0.
\]

(6.2.3)

Then according to Pontryagin’s Maximum Principle ([24, P.109, Theorem 3.14]), there exist continuous and piecewise continuously differentiable state and co-state functions \( S, I, D, \lambda_1, \lambda_2, \lambda_3 \), that (i) satisfy (6.1.3), (6.2.3), and (ii) at every \( t \in [0 \ldots T] \) where \( \vartheta \) is continuous, satisfy (6.1.2),
(6.2.2). Also,

$$\vartheta \in \arg \min_{0 \leq \vartheta \leq 1} H(\tilde{\lambda}, (S, I, D), \vartheta). \quad (6.2.4)$$

Relation (6.2.4) between the optimum control $\vartheta$ and the Hamiltonian (6.2.1) allows us to express $\vartheta$ as a function of the state $(S, I, D)$ and co-state $(\lambda_1, \lambda_2, \lambda_3)$ functions in (6.1.2) and (6.2.2), resulting in a system of differential equations involving only the state and co-state functions, and not the control function. Using the initial and final values on the state and co-state functions, (6.1.3) and (6.2.3) respectively, this system can be solved numerically to obtain the optimum state and co-state functions, which can now be used to compute (i) $\vartheta$ via (6.2.4), (6.2.1) and (ii) $J(\vartheta)$ via (6.1.5).

### 6.2.2 Structure of an optimal non-replicative dispatch

We now show that the optimal immunization rate function $\vartheta(.)$ follows simple structures:

**Theorem 6.2.1.** An optimal immunization rate function $\vartheta(.)$ has the following structure:

1. When $h(.)$ is concave, $\vartheta(t) = 1$ for $0 < t < t_1$ and $\vartheta(t) = 0$ for $t_1 < t < T$.

2. When $h(.)$ is strictly convex, $\exists t_0, t_1, 0 \leq t_0 \leq t_1 \leq T$:
   
   (a) $\vartheta(t) = 1$ on $0 < t \leq t_0$;
   
   (b) $\vartheta(t)$ strictly and continually decreases on $(t_0, t_1)$;
   
   (c) $\vartheta(t) = 0$ on $t_1 \leq t < T$.

Thus, any optimal immunization rate function is a non-increasing function of time. In retrospect, this is intuitive. This is because the bandwidth consumption cost associated with such a function depends only on the area of the $h(\cdot)$ function, and thus an increasing segment may be replaced by a non-increasing one without increasing the area. Choosing higher values of the immunization rate later (as opposed to earlier) will only let the number of infective and dead nodes
increase. This increases the integrations of the $f(I(t))$, $g(D(t))$ functions, and also potentially reduces the efficacy of the recovery process - the latter happens because healing (of infectives) is slower (or rather not faster) than the immunization (of susceptibles) for the same immunization rate since $\pi \leq 1$ (in fact the proof of Theorem 6.2.1 heavily relies on the property that $\pi \leq 1$).

The nature of the decrease of the optimal immunization rate function, whether continuous or abrupt, strict or otherwise, may not however be intuited easily. Theorem 6.2.1 characterizes the decrease pattern as well. When $h(.)$ is concave (either strictly concave or linear), any optimal immunization rate function is single-jump bang-bang: applies the maximum immunization rate in the beginning until a threshold time and then stops the immunization. When the threat is marginal, this threshold time is zero; then it is best not to patch at all, rather than patching with intermediate intensities. When $h(.)$ is strictly convex, an optimal immunization rate function may however start with rate values between 0 and 1, and monotonically and continuously decrease down to the final value of 0. Figures 6.1, 6.2 illustrate the optimum controls for linear and strictly convex $h(.)$ respectively.

**Proof.** Let $\varphi := \beta_1 R_0 (\lambda_1 S + \pi \lambda_2 I)$ which is a continuous function of time, and by (6.2.3), $\varphi(T) = 0$. Also, as we prove in §6.2.2,

**Lemma 6.2.2.** $\varphi(t)$ is a strictly decreasing function of $t$ for $t \in [0, T)$.

Now we can rewrite the Hamiltonian in (6.2.1) as:

$$H = f(I) + g(D) + (\lambda_2 - \lambda_1)\beta_0 IS + (\lambda_3 - \lambda_2)\delta I + h(R_0 \vartheta) - \varphi \vartheta.$$  

From (6.2.4), for each admissible control $\vartheta$, and for all $t \in [0, T]$,

$$h(R_0 \vartheta(t)) - \varphi(t) \vartheta(t) \leq h(R_0 \vartheta(t)) - \varphi(t) \vartheta(t)$$

$$\implies \vartheta(t) \in \arg \min_{x \in [0,1]} h(R_0 x) - \varphi(t) x.$$  

Also, since $\vartheta = 0$ is an admissible control, using (6.2.6),

$$h(R_0 \vartheta) - \varphi \vartheta \leq h(0) = 0 \text{ at all } t.$$  

111
We now separately consider the cases that $h(.)$ is concave and strictly convex.

$h(.)$ concave

When $h'' \leq 0$, at each time $t$, $h(R_0 x) - \varphi(t)x$ is a concave function of $x$, and thus a minimum in (6.2.7) is either at $x = 0$ or $x = 1$. Then,

$$\vartheta(t) = \begin{cases} 
0, & \varphi(t) < h(R_0) \\
1, & \varphi(t) > h(R_0). 
\end{cases} \quad (6.2.9)$$

According to $\varphi(T) = 0$ and the continuity of $\varphi$ and since $h(R_0) > 0$, we have $\varphi(t) < h(R_0)$ over a subinterval that extends to $T$. If this sub-interval starts from $t = 0$, the theorem follows from (6.2.9) with $t_1 = 0$. Else, from the continuity of $\varphi$, and the Intermediate Value Theorem, $\varphi(t) = h(R_0)$ for some $t \in [0, T)$. But, there can be at most one such $t$, say $t_1$, by lemma 6.2.2. Lemma 6.2.2 also implies that $\varphi(t) > h(R_0)$ for $t \in [0, t_1)$, and $\varphi(t) < h(R_0)$ for $t \in (t_1, T]$. The theorem follows from (6.2.9).

$h(.)$ strictly convex:

When $h(.)$ is strictly convex (i.e., $h'' > 0$), (6.2.7) implies that, if $\frac{\partial}{\partial x} (h(R_0 x) - \varphi(t)x)|_{x=y} = 0$ at a $y \in [0, 1]$, then $\vartheta(t) = y$, else $\vartheta(t) \in \{0, 1\}$. Then,

$$\vartheta = \begin{cases} 
0, & \varphi \leq R_0 h'(0) \\
\frac{1}{R_0} h^{-1}(\varphi/R_0), & R_0 h'(0) < \varphi \leq R_0 h'(R_0) \\
1, & R_0 h'(R_0) < \varphi. 
\end{cases} \quad (6.2.10)$$

Note that $\varphi(T) = 0 \leq R_0 h'(0)$, since $R_0 > 0$ and $h'(x) \geq 0$ for all $x$. Also, since $h(.)$ is strictly convex, $h'(.)$ is a strictly increasing function - hence, since $R_0 > 0$, $h'(0) < h'(R_0)$. Thus, following lemma 6.2.2, there exist $t_0, t_1$, $0 \leq t_0 \leq t_1 \leq T$, such that $\varphi > R_0 h'(R_0)$ on $0 < t \leq t_0$, $R_0 h'(0) < \varphi \leq R_0 h'(R_0)$ on $t_0 < t < t_1$, and $\varphi \leq R_0 h'(0)$ on $t_1 \leq t \leq T$. The theorem now follows from (6.2.10). \qed
Proof of lemma 6.2.2

The state and co-state functions, and hence the \( \varphi \) function, are differentiable at each \( t \in [0, T) \) at which the \( \vartheta \) function is continuous. Since \( \vartheta \) is piecewise continuous and \( \varphi \) is continuous, the lemma follows if we can show that \( \dot{\varphi} < 0 \) at each such \( t \). Since \( \beta_1, R_0 > 0 \), at each such \( t \in [0, T) \),

\[
\frac{\dot{\varphi}}{\beta_1 R_0} = \frac{1}{\beta_1 R_0} \frac{d}{dt} \varphi = \dot{\lambda}_1 S + \lambda_1 \dot{S} + \pi \dot{\lambda}_2 I + \pi \lambda_2 \dot{I} = - (\lambda_2 - \lambda_1) \beta_0 IS - (1 - \pi) \lambda_1 \beta_0 IS - \pi f'(I) I - \pi \lambda_3 \delta I
\]

The right hand side is negative at each \( t \in [0, T) \) from lemma 6.1.1, since \( 0 \leq \pi \leq 1, \beta_0, \beta_1 > 0, \delta \geq 0, f'(x) \geq 0 \) at each \( x \), and because:

**Lemma 6.2.3.** For all \( 0 \leq t < T \), we have \( \lambda_3 \geq 0, \lambda_1 > 0, \) and \( (\lambda_2 - \lambda_1) > 0 \).

Note that a direct corollary of this lemma is that \( \lambda_2 > 0 \) for all \( 0 \leq t < T \) as well.

**Proof.** First, \( \lambda_3(T) = 0 \) and at any \( t \in [0, T] \) at which \( \vartheta \) is continuous, \( \dot{\lambda}_3(t) = -g'(D(t)) \leq 0 \). Thus, since \( \vartheta \) is piecewise continuous, \( \lambda_3(t) \geq 0 \) for all \( 0 \leq t \leq T \). We prove the other two inequalities using the following real analysis properties.

**Property 5.** Let \( \psi(t) \) be a continuous and piecewise differentiable function of \( t \). Let \( \psi(t_1) = L \) and \( \psi(t) > L \) for all \( t \in (t_1 \ldots t_0) \). Then\(^2 \dot{\psi}(t_1^+) \geq 0 \).

**Proof.** Proof by contradiction. Suppose that the property did not hold, thus

\[
\psi(t_1) = L, \quad \dot{\psi}(t_1^+) < 0
\]

\[
\Rightarrow \exists \delta_1 \in (0 \ldots t_0 - t_1) \text{ such that } \dot{\psi}(t) < 0 \quad \forall t \in (t_1, t_1 + \delta_1).
\]

However, by integrating \( \dot{\psi} \) from \( t_1 \) to \( t_1 + \delta \), we obtain \( \psi(t_1 + \delta) < L \). This contradicts the assumption that \( \psi(t) > L \) for all \( t_1 < t < t_0 \). \( \square \)

\(^2\)For a general function \( \psi(x) \), the notations \( \psi(x^+_0) \) and \( \psi(x^-_0) \) are defined as \( \lim_{x \downarrow x_0} \psi(x) \) and \( \lim_{x \uparrow x_0} \psi(x) \), respectively.
Property 6. For any convex and differentiable function, \( v(x) \), which is 0 at \( x = 0 \), \( v'(x)x - v(x) \geq 0 \) for all \( x \geq 0 \).

Proof. Define \( \xi(x) = v'(x)x - v(x) \). Clearly, \( \xi(0) = 0 \). Also,

\[
\xi'(x) = v''(x)x + v'(x) - v'(x) = v''(x)x.
\]

The convexity of \( v(.) \) implies that \( \xi'(x) \geq 0 \) for all \( x \geq 0 \). Thus, since \( \xi(0) = 0 \), \( \xi(x) \geq 0 \) at all \( x \geq 0 \). The property follows.  

The system is autonomous, i.e., the Hamiltonian and the constraints on the control (6.1.6) do not have an explicit dependence on the independent variable \( t \). Thus, [47, P236]

\[
H(S, I, D, \theta, \lambda_1, \lambda_2, \lambda_3) = \text{constant.} \tag{6.2.11}
\]

Thus, from (6.2.3), \( H = H(T) = f(I(T)) + g(D(T)) + h(R_0\vartheta(T)) \). Also, \( \dot{D} = \delta I \geq 0 \), and \( g(.) \) is a non-decreasing function, thus \( g(D(T)) \geq g(D(t)) \) for all \( t \in [0 \ldots T] \). Hence:

\[
H - g(D(t)) \geq f(I(T)) + h(R_0\vartheta(T)) > 0. \tag{6.2.12}
\]

The positivity follows since (i) according to lemma 6.1.1, \( I(T) > 0 \) and hence \( f(I(T)) > 0 \) and (ii) \( h(R_0\vartheta(T)) \geq 0 \).

We proceed in the following two steps:

Step-1. \( \lambda_2(T) - \lambda_1(T) = 0 \) and \( \dot{\lambda}_2(T) = \dot{\lambda}_1(T) = -f'(I(T)) < 0 \). Also, \( \lambda_1(T) = \dot{\lambda}_1(T) = 0 \) and \( \ddot{\lambda}_1(T) = -\lambda_2(T)\beta_0 I(T) > 0 \). Therefore, \( \lambda_1(t) \) and \( \lambda_2(t) - \lambda_1(t) \) are positive in an open interval of nonzero length ending at \( T \).

Step-2. Proof by contradiction. Let \( t^* \geq 0 \) be the last time before \( T \) at which (at least) one of the other two inequality constraints is active, i.e.,

\[
\text{for } t^* < t < T : \quad \lambda_1(t) > 0, \quad (\lambda_2(t) - \lambda_1(t)) > 0
\]

and, \( \lambda_1(t^*) = 0 \) OR \( \lambda_2(t^*) - \lambda_1(t^*) = 0 \)
First, let $\lambda_2(t^*) - \lambda_1(t^*) = 0$. Now, from (6.2.2) and (6.2.5),

$$(\dot{\lambda}_2(t^*) - \dot{\lambda}_1(t^*)) = -f'(I) + \pi \beta_1 R_0 \vartheta \lambda_2 - (\lambda_3 - \lambda_2) \delta - \beta_1 R_0 \vartheta \lambda_1 - \frac{H}{I} + \frac{f(I)}{I} + \frac{g(D)}{I} + \frac{1}{I} (h(R_0 \vartheta) - \varphi \vartheta) + (\lambda_3 - \lambda_2) \delta$$

$$= \frac{1}{I} [f(I) - f'(I) I] - \frac{H - g(D)}{I} - (1 - \pi) \beta_1 R_0 \vartheta \lambda_1 + \frac{1}{I} (h(R_0 \vartheta) - \varphi \vartheta)$$  (6.2.13)

From the supposition on $t^*$ and continuity of $\lambda_1(t^*) \geq 0$. Now, $f(I) - f'(I) I \leq 0$ because of Property 6, since $f(x)$ is convex, $f(0) = 0$ and $I > 0$ at all $t$ by lemma 6.1.1. Thus, from (6.1.6), (6.2.8), (6.2.12) and (6.2.13), we observe that $|\frac{d}{dt} (\lambda_2 - \lambda_1)|_{t^*} < 0$. This contradicts Property 5. Hence, $(\lambda_2(t^*) - \lambda_1(t^*)) > 0$. Now let $\lambda_1(t^*) = 0$. Then from (6.2.2), $\dot{\lambda}_1|_{t^*} = -(\lambda_2 - \lambda_1) \beta_0 I$. Since $(\lambda_2(t^*) - \lambda_1(t^*)) > 0$, and from lemma 6.1.1, $\dot{\lambda}_1(t^*) < 0$. This contradicts Property 5, and hence negates the existence of $t^*$. The lemma follows.

6.3 Optimal replicative dispatch

As in the non-replicative case, we first present a framework for numerical computation of $\vartheta(t)$ and $J(\vartheta)$ (§6.3.1). The main question however is whether similar simple structural properties apply in the replicative case as well. Unlike the non-replicative case, the set of dispatchers grow at potentially exponentially fast speeds. An intricate structure for the optimum dispatching policy may make the implementation difficult. Fortunately, as we prove in §6.3.2, $\vartheta(t)$ follows similar simple structures as for the non-replicative case.

6.3.1 Numerical framework

We seek to find an admissible $\vartheta(t)$ to minimize the cost function in (6.1.10) for the state dynamics (6.1.7) and initial state values (6.1.8). We again apply Pontryagin’s Maximum Principle. Define
the Hamiltonian as:

\[ H = f(I) + g(D) + h(R\vartheta) + (\lambda_2 - \lambda_1)\beta_0 IS - (\lambda_1 - \lambda_3)\beta_1 \vartheta RS - (\lambda_2 - \lambda_3)\pi \beta_1 \vartheta RI - \lambda_2 \delta I. \]

(6.3.1)

where \( D = 1 - (S + I + R) \), and the co-state functions as:

\[ \dot{\lambda}_1 = -\frac{\partial H}{\partial S} = - (\lambda_2 - \lambda_1)\beta_0 I + (\lambda_1 - \lambda_3)\beta_1 \vartheta R + g'(D) \]

\[ \dot{\lambda}_2 = -\frac{\partial H}{\partial I} = -f'(I) - (\lambda_2 - \lambda_1)\beta_0 S + (\lambda_2 - \lambda_3)\pi \beta_1 \vartheta R + \lambda_2 \delta + g'(D) \]

(6.3.2)

\[ \dot{\lambda}_3 = -\frac{\partial H}{\partial R} = (\lambda_1 - \lambda_3)\beta_1 \vartheta S + (\lambda_2 - \lambda_3)\pi \beta_1 \vartheta I - \vartheta h'(R\vartheta) + g'(D) \]

and transversality conditions as:

\[ \lambda_1(T) = \lambda_2(T) = \lambda_3(T) = 0. \]

(6.3.3)

Then according to Pontryagin’s Maximum Principle ([24, P. 109, Theorem 3.14]), there exist continuous and piecewise continuously differentiable state and co-state functions \( S, I, R, \lambda_1, \lambda_2, \lambda_3 \), that (i) satisfy (6.1.8), (6.3.3), and (ii) at every \( t \in [0 \ldots T] \) where \( \vartheta \) is continuous, satisfy (6.1.7), (6.3.2). Also,

\[ \vartheta \in \arg \min_{0 \leq \vartheta \leq 1} H(\tilde{\lambda}, (S, I, R), \vartheta). \]

(6.3.4)

### 6.3.2 Structure of optimal replicative dispatch

In this section, we show that the optimum control has the same structure as under non-replicative dispatch. Specifically, Theorem 6.2.1 holds. Despite the similarity of structure, the \( \vartheta \) functions are obviously not identical for the replicative and non-replicative dispatch. For example, figures 6.3(a) to 6.5(a) demonstrate that the transition from 1 to 0 in the bang-bang optimal control invariably occurs earlier for replicative dispatch when \( h(\cdot) \) is linear. This is because in replicative dispatch the number of dispatchers increases exponentially fast. Thus, more infectives and susceptibles are healed and immunized respectively in shorter duration allowing for smaller initial period of
maximum rate immunization. Also, the exponential growth in the number of dispatchers may result in a huge cost due to $\vartheta$, if it is not shut down to zero earlier.

Proof. Let us define $\varphi$ as follows:

$$\varphi := (\lambda_1 - \lambda_3)\beta_1 RS + (\lambda_2 - \lambda_3)\pi_1 RI$$  \hspace{1cm} (6.3.5)$$

which is a continuous function of time, with the following final value according to (6.3.3):

$$\varphi(T) = 0.$$  \hspace{1cm} (6.3.6)$$

We rewrite the Hamiltonian in (6.3.1) as follows:

$$H = f(I) + g(D) + (\lambda_2 - \lambda_1)\beta_0 IS - \lambda_2 \delta I + h(R\vartheta) - \varphi \vartheta.$$  \hspace{1cm} (6.3.7)$$

From (6.3.4), for each admissible control $\vartheta$, and for all $t \in [0, T]$,

$$h(R(t)\vartheta(t)) - \varphi(t)\vartheta(t) \leq h(R(t)\bar{\vartheta}(t)) - \varphi(t)\bar{\vartheta}(t)$$  \hspace{1cm} (6.3.8)$$

$$\Rightarrow \vartheta(t) \in \arg \min_{x \in [0,1]} h(R(t)x) - \varphi(t)x.$$  \hspace{1cm} (6.3.9)$$

Now, since $\vartheta = 0$ constitutes an admissible control, (6.3.8) implies that:

$$[h(R\vartheta) - \varphi \vartheta] \leq 0 \text{ at all } t.$$  \hspace{1cm} (6.3.10)$$

As in the non-replicative dispatch, we consider the cases that $h(.)$ is concave and strictly convex separately. In both, we will use the expression for $\dot{\varphi}$ at each $t$ at which $\vartheta$ is continuous, which we next obtain using (6.3.5):

$$\dot{\varphi} = (\dot{\lambda}_1 - \dot{\lambda}_3)\beta_1 RS + (\dot{\lambda}_2 - \dot{\lambda}_3)\pi_1 RI$$

$$+ (\lambda_1 - \lambda_3)\beta_1 \dot{R}S + (\lambda_2 - \lambda_3)\pi_1 \dot{R}I$$

$$+ (\lambda_1 - \lambda_3)\beta_1 \dot{R} \dot{S} + (\lambda_2 - \lambda_3)\pi_1 \dot{R} \dot{I}$$
(a) varying $\beta$. Here, $R_0 = 0.1$, $K_u = 10$, $I_0 = 0.1$ and $\delta = 0.005$.

(b) varying $R_0$. Here, $\beta = 0.20$, $K_u = 10$, $I_0 = 0.1$ and $\delta = 0.005$.

Figure 6.3: The jump point of the bang-bang optimum control for replicative and non-replicative dispatch. Here, $f(I) = 10I^2$, $g(D) = 20D^2$, $h(x) = K_u x$, and $T = 100$, $\delta = 0.005$, $\beta_0 = \beta_1 = \beta$.

replacing from (6.1.7) and (6.3.2) and simplifying yields:

$$\pi = \pi \beta_1 \beta_0 RIS + \beta_0 \beta_1 RIS \lambda_2$$

$$-\beta_1 \beta_0 RIS - \pi \beta_1 \beta_0 RIS \lambda_1 + \pi \beta_1 f'(I) R I - \pi \beta_1 R I \delta \lambda_3 + \dot{R} h'(R \delta)$$

$$\rightarrow \pm \beta_0 \beta_1 RIS \lambda_1 \text{ and re-arrangement } \rightarrow$$

$$= -\beta_0 \beta_1 (1 - \pi) RIS (\lambda_1 - \lambda_3) - \beta_0 \beta_1 RIS (\lambda_2 - \lambda_1)$$

$$- \pi \beta_1 f'(I) R I + \pi \beta_1 R I \delta \lambda_3 + \dot{R} h'(R \delta). \hspace{1cm} (6.3.11)$$

We will also use the following key properties of the co-state functions, which we prove in § 6.3.2.

**Lemma 6.3.1.** For all $0 \leq t < T$, we have $(\lambda_2 - \lambda_1) > 0$, $(\lambda_1 - \lambda_3) > 0$ and $\lambda_3 \leq 0$.
(a) varying $K_u$. Here, $\beta = 0.20$, $R_0 = 0.1$, $I_0 = 0.1$ and $\delta = 0.005$.

(b) varying $I_0$. Here, $\beta = 0.20$, $R_0 = 0.1$, $K_u = 10$ and $\delta = 0.005$.

Figure 6.4: (Continuation of) the jump point of the bang-bang optimum control for replicative and non-replicative dispatch. Refer to fig. 6.3 for the parameters of choice.

$h(.)$ concave

When $h(.)$ is concave (i.e., $h'' \leq 0$), at each time $t$, $h(R(t)x) - \varphi(t)x$ is a concave function of $x$, and thus a minimum in (6.3.9) is either at $x = 0$ or $x = 1$, and this minimum is unique unless $h(R) - \varphi = 0$. Then,

$$\vartheta = \begin{cases} 
0, & \varphi - h(R) > 0 \\
1, & \varphi - h(R) < 0 
\end{cases} \quad (6.3.12)$$

For the case of $h'' < 0$, whenever $h(R) - \varphi = 0$, $\vartheta \in \{0, 1\}$. Let

$$\psi(t) := \varphi(t) - h(R(t))$$

From (6.3.6) and (6.3.12), since $h(R(T)) > 0$, $\psi < 0$ over a subinterval that extends to and includes $T$. Thus, from (6.3.12), $\vartheta = 0$, and hence $\vartheta$ is continuous, in this subinterval.
Figure 6.5: (Continuation of) the jump point of the bang-bang optimum control for replicative and non-replicative dispatch. Refer to fig. 6.3 for the parameters of choice.

for all \( t \in [0, T) \), \( \psi(t) \) strictly decreases with increase in \( t \). The rest of the proof is identical to that for concave \( h(.) \) in the proof of Theorem 6.2.1 (with \( \psi \) instead of \( \varphi \) and 0 instead of \( h(R_0) \) in the arguments).

Since \( \vartheta \) is piece-wise continuous and \( \varphi, h, R \) are continuous, it suffices to show that \( \dot{\psi} \) is negative at any \( t \in [0, T) \) at which \( \vartheta \) is continuous. Referring to (6.3.11), at any such \( t \):

\[
\dot{\psi} = \dot{\varphi} - h'(R) \dot{R} = -\beta_0 \beta_1 (1 - \pi) RIS(\lambda_1 - \lambda_3) - \beta_0 \beta_1 RIS(\lambda_2 - \lambda_1) - \pi \beta_1 f'(I) RI + \pi \beta_1 RI \delta \lambda_3 - \dot{R}(h'(R) - h'(R \vartheta))
\]

We only need to show that the right hand side is negative at each \( t \in [0, T) \). Note that, by assumption, \( \beta_0, \beta_1 > 0, 0 \leq \pi \leq 1, \delta \geq 0, f(.) \) is non-decreasing. Also, \( \dot{R}(h'(R) - h'(R \vartheta)) \equiv 0 \).

This follows readily for \( h'' \equiv 0 \) as then \( h'(R) - h'(R \vartheta) \equiv 0 \) for any value of \( \vartheta \). When \( h'' < 0 \), as we argued in (6.3.12) and after, \( \vartheta \in \{0, 1\} \); now for \( \vartheta = 1 \), \( h'(R) - h'(R \vartheta) = 0 \) and for \( \vartheta = 0 \), \( \dot{R} = 0 \).

The negativity follows from lemma 6.1.1 for the replicative case and lemma 6.3.1.
When $h(.)$ is strictly convex (i.e., $h'' > 0$), (6.3.9) implies that, if $\frac{\partial}{\partial x} (h(R(t)x) - \varphi(t)x)|_{x=y} = 0$ at a $y \in [0, 1]$, then $\vartheta(t) = y$, else $\vartheta(t) \in \{0, 1\}$. Thus,

$$\vartheta = \begin{cases} 
0, & \frac{\varphi}{R} \leq h'(0) \\
\frac{1}{\alpha}h'^{-1}(\frac{\varphi}{R}), & h'(0) < \frac{\varphi}{R} \leq h'(R) \\
1, & h'(R) < \frac{\varphi}{R}.
\end{cases} \quad (6.3.14)$$

Thus, since (i) $\varphi, R, h'$ are continuous, (ii) $h'$ is strictly increasing, and (iii) $R > 0$ at all $t \in [0, T]$ by lemma 6.3.1, $\vartheta(t)$ is continuous at all $t \in [0, T]$. Note that $\varphi(T)/R(T) = 0 \leq h'(0)$, from (6.3.6), lemma 6.3.1 and since $h'(x) \geq 0$ for all $x$. The rest of the proof is identical to that for strictly convex $h(.)$ in the proof of Theorem 6.2.1 provided we can show that $\psi = (\varphi/R)$ is a strictly decreasing function of time.

$$\psi = \frac{\dot{\varphi} - \dot{R}\varphi/R}{R} = \frac{\{\text{negative term}\} + \dot{R}[h'(R\vartheta) - \varphi/R]}{R}$$

The last equality follows from (6.3.11), and the negative term is $-\beta_0\beta_1(1 - \pi)R\alphaS(\lambda_1 - \lambda_3) - \beta_0\beta_1R\alphaS(\lambda_2 - \lambda_1) - \pi\beta_1f'(I)RI + \pi\beta_1RI\delta\lambda_3$. The negativity of this term is established by lemma 6.1.1 for the replicative case, lemma 6.3.1 and the assumptions that $\beta_0, \beta_1 > 0, 0 \leq \pi \leq 1, \delta \geq 0, \ f(.)$ is non-decreasing. Also, $\dot{R} \geq 0$ because of the above. Thus, from (6.3.14), $\dot{\psi} < 0$ since (i) if $\varphi/R \leq h'(0)$, then $\vartheta = 0$, and hence $\dot{R} = 0$, (ii) if $h'(0) < \frac{\varphi}{R} \leq h'(R)$, then $h'(R\vartheta) - \frac{\varphi}{R} = 0$ and (iii) if $\frac{\varphi}{R} > h'(R)$, $\vartheta = 1$ and $h'(R) - \frac{\varphi}{R} < 0$. \hfill $\Box$

**Proof of lemma 6.3.1**

We first show that $\lambda_3(t) \leq 0$ for all $0 \leq t \leq T$. First, we note that $\lambda_3(T) = 0$. Thus, if we show that $\dot{\lambda}_3(t) \geq 0$ at any $t$ at which $\vartheta$ is continuous, the result follows since $\vartheta$ is piecewise continuous.
Using (6.3.5) in (6.3.2) at any such $t$:

$$\dot{\lambda_3} = \frac{\varphi \vartheta - R \vartheta h'(R \vartheta)}{R} + g'(D).$$

Since $g(.)$ is a non-decreasing function, $g'(D) \geq 0$. Thus, using lemma 6.1.1 for the replicative case, the result follows if we show that

$$\varphi \vartheta - R \vartheta h'(R \vartheta) \geq 0 \text{ at all } t. \tag{6.3.15}$$

When $h(.)$ is strictly convex, (6.3.15) is a consequence of (6.3.14).

When $h(.)$ is concave, we decompose $\varphi \vartheta - R \vartheta h'(R \vartheta)$ as

$$\varphi \vartheta - R \vartheta h'(R \vartheta) = \varphi \vartheta - h(R \vartheta) + h(R \vartheta) - R \vartheta h'(R \vartheta).$$

Now, referring to (6.3.10), $\varphi \vartheta - h(R \vartheta) \geq 0$. (6.3.15) follows if we show that $h(R \vartheta) - R \vartheta h'(R \vartheta) \geq 0 \ \forall \ \vartheta \in [0 \ldots 1]$. This follows from Property 6, letting $x := R \vartheta$, and noting that (i) $x \geq 0$ from lemma 6.1.1 for the replicative case and since $\vartheta \geq 0$, (ii) $h(0) = 0$, and (iii) $-h(x)$ is convex.

For proving the other two inequalities in lemma 6.3.1, we observe, as in the non-replicative model, that the Hamiltonian is a constant $H$ since the system is autonomous, and

$$H - g(D(t)) \geq f(I(T)) + h(R(T)\vartheta(T)) > 0. \tag{6.3.16}$$

The proof for (6.3.16) is identical to that for (6.2.12), and uses the fact that $g(D(T)) \geq g(D(t))$ for all $t \in [0 \ldots T]$.

We proceed in the following two steps:

**Step-1.** First, $(\lambda_2(T) - \lambda_1(T)) = (\lambda_1(T) - \lambda_3(T)) = 0$. Next, as in the proof of lemma 6.3.1, $\lambda_1, \lambda_2, \lambda_3$ are continuously differentiable in an interval extending to and including $T$. Moreover, $\frac{d}{d\vartheta} (\lambda_2 - \lambda_1)(T) = -f'(I(T)) < 0$. Also, $(\lambda_1 - \lambda_3)(T) = \frac{d}{d\vartheta} (\lambda_1 - \lambda_3)(T) = 0$, and $\frac{d}{d\vartheta} (\lambda_1 - \lambda_3)(T) = -\dot{\lambda}_2(T) \beta_0 I(T) > 0$. Therefore, both inequalities are satisfied in an open interval of nonzero length.

\[\text{Note that for strictly convex } h(\cdot), \text{ we obtained (6.3.14) without using lemma 6.3.1. Thus, we can use (6.3.14) in proving lemma 6.3.1.}\]
ending at $T$.

**Step-2.** Proof by contradiction. Let $t^* \geq 0$ be the last time before $T$ at which (at least) one of the other two inequalities is violated, i.e., for $t^* < t < T$:

$$(\lambda_2 - \lambda_1)(t) > 0, \quad (\lambda_1 - \lambda_3)(t) > 0.$$

$$(\lambda_2 - \lambda_1)(t^*) = 0 \quad \text{OR} \quad (\lambda_1 - \lambda_3)(t^*) = 0$$

First, suppose that $\lambda_2(t^*) = \lambda_1(t^*)$. Now:

$$\dot{\lambda}_2(t^*) - \dot{\lambda}_1(t^*) = - f'(I) + (\lambda_2 - \lambda_3)\pi\beta_1\vartheta R + \delta\lambda_2 - (\lambda_1 - \lambda_3)\beta_1\vartheta R$$

$$= - f'(I) + (\lambda_2 - \lambda_3)\pi\beta_1\vartheta R + \delta\lambda_2 - (\lambda_1 - \lambda_3)\beta_1\vartheta R$$

$$- \frac{H}{I} + \frac{g(D)}{I} + \frac{1}{I}(h(R\vartheta) - \varphi\vartheta) - \delta\lambda_2$$

$$\leq \frac{H - g(D)}{I} - (\lambda_1 - \lambda_3)(\beta_1 - \pi\beta_1)\vartheta R$$

(6.3.17)

From the definition of $t^*$, $(\lambda_1 - \lambda_3)(t^+) \geq 0$. Now, since $\beta_1 > 0, \pi \leq 1, \vartheta \geq 0$, from (6.3.10), (6.3.16), (6.3.17), lemma 6.1.1 for the replicative case, Property 6, convexity of $f(.)$ and since $f(0) = 0, \dot{\lambda}_2(t^*) - \dot{\lambda}_1(t^*) < 0$. This contradicts Property 5. Hence, $(\lambda_2(t^*) - \lambda_1(t^*)) > 0$.

Now, suppose that $\lambda_1(t^*) = \lambda_3(t^*)$. Now, from (6.3.2) and (6.3.5):

$$\dot{\lambda}_1(t^*) - \dot{\lambda}_3(t^*) = -(\lambda_2 - \lambda_1)\beta_0 I - \frac{\varphi\vartheta - R\vartheta h'(R\vartheta)}{R}.$$
by the (only possible) jump point. Also, the optimal defense strategy for a strictly convex $h$ can be simply divided into at most three phases, characterized by at most two time epochs. The threshold times can be computed by a central unit that estimates the system parameters $\beta_0, \beta_1, \pi, I_0, \delta$ etc. a priori (e.g., $\beta_0, \beta_1$ may be obtained from the long term average node contact rates) and knows the cost functions $f(I), g(D), h(\vartheta)$. This computation needs to be performed once, (at $t = 0$, i.e., when the central unit learns the presence of the worm in the system), and the value of the transition points can be transmitted to all devices via a secure broadcast. Since this is a one-time transmission, such secure broadcasts can be afforded. The devices can subsequently execute the optimal defense strategies without coordinating any further among themselves or with the central unit, or without requiring any local or global information as time progresses. Thus, the initial information is sufficient to determine the decision of the nodes for the entire interval.

Note that the transition times of the optimal controls can be determined by solving a system of differential equations, as described in the previous sections. Such systems can be solved very fast due to the existence of efficient numerical algorithms for solving differential equations, and the computation time is constant in that it does not depend on the number of nodes $N$. Given that many mobile devices have computing capabilities, and that this is a one-time computation, these differential equations can even be solved at each mobile device once they have estimated and/or learned the parameters of the system. The estimations may however be inaccurate in practice. We demonstrate using numerical computations in the next section that the defense is robust to estimation inaccuracies.

In practice, due to drifts in local clocks, different dispatchers may stop transmitting the security patches at slightly different times. Our simulations presented in Appendix A reveal that the overall costs are robust to clock drifts for our dynamic optimal policies.
6.5 Numerical computations

We evaluate some features of our dynamic policies. Specifically, we compare the performance of optimum dynamic replicative and non-replicative dispatch policies, and also those of optimum dynamic and static controls in the two dispatch models for different values of network and attack parameters.\textsuperscript{4} Recall that in a static policy [68, 78], in contrast to a dynamic policy, the rate of dispatch is fixed throughout the period of network operation. We vary the (fixed) value of the dispatch rate and choose the one that achieves the least aggregate cost. We refer to this policy as best-static policy. As we will see, dynamic policies significantly outperform the corresponding best-static policies, both in terms of the overall inflicted costs and robustness against parameter estimations. We also show that the performance of our dynamic policies is not sensitive to the accuracy of global coordination. We choose $T = 100$, $\pi \in \{0, 1\}$ and $\beta_1 = \beta_0 = \beta$, $f(I) = 10I^2$ and $g(D) = 20D^2$. Here, $T$ is chosen large enough so that most susceptibles are either infected or immunized by the end of the time window $[0, T]$, and the system reaches a steady state. Also, $f(I)$ is convex, consistent with our model. We have chosen the same function for $g$, albeit with a larger multiplier as the dead nodes ought to be more costly than the infectives. We consider a linear $h$ function: $h(x) = K_u x$, with $K_u$ as a parameter.

Under each dispatch model, the optimal dynamic control will incur lower aggregate cost than the best-static control since the set of feasible solutions for a dynamic control is a strict superset of that for a static control. Also, as discussed in the Remarks subsection of §6.1.1, the optimal dynamic replicative dispatch incurs lower aggregate costs than its non-replicative counterpart - the goal in both of the above cases is to investigate the extent of the difference between the overall costs. Under static control, however, the aggregate cost of replicative dispatch may exceed that for non-replicative dispatch since the population of dispatchers grows throughout $[0, T]$ in the

\textsuperscript{4}For our numerical calculations, we used the PROPT\textsuperscript{®} software. PROPT is a commercial software launched by Tomlab Optimization Inc, http://tomopt.com/tomlab/ for MATLAB\textsuperscript{®}. Specifically, we could compute $\vartheta, J(\vartheta)$ in 1 second in each instance using PROPT in an Intel\textsuperscript{®}Xeon\textsuperscript{®}CPU X5355, 2.66 GHz 8 Gb RAM, 2Gb swap memory machine.
former whereas this population is constant in the latter - thus, for large $T$, the higher bandwidth consumption cost in the former offsets the advantages due to lower fraction of infectives and dead nodes. In contrast, the optimal dynamic control in replicative dispatch de-activates all dispatchers after a certain time; yet regulates the levels of infection and mortality by immunizing at the maximum possible rate initially (Theorem 6.2.1). Figures 6.6 to 6.10, where we compared the minimum aggregate cost of the four different versions, (i) dynamic replicative dispatch, (ii) dynamic non-replicative dispatch, (iii) best-static replicative dispatch, and (iv) best-static non-replicative dispatch, by respectively varying the values of individual parameters $\beta$, $R_0$, $K_u$, $I_0$, $\delta$ invariably reveal the following order: $J_{\text{dyn. rep.}} \leq J_{\text{dyn. non-rep.}} \leq J_{\text{stat. non-rep.}} \leq J_{\text{stat. rep.}}$. The only exception to this ordering is one data point in fig. 6.8 where $J_{\text{stat. rep.}}$ is lower than $J_{\text{dyn. non-rep.}}$, $J_{\text{stat. non-rep.}}$ but still exceeds $J_{\text{dyn. rep.}}$. The differences between (i) $J_{\text{dyn. non-rep.}}$ and $J_{\text{dyn. rep.}}$ and (ii) $J_{\text{stat. rep.}}$ and $J_{\text{dyn. rep.}}$ are in general significant. The replicative dispatch incurs only half the cost of the non-replicative dispatch under optimal dynamic control, and the optimal dynamic control incurs only $1/3$ the cost of the optimal static control under replicative dispatch for certain choices of parameters. $J_{\text{dyn. non-rep.}}$, $J_{\text{stat. non-rep.}}$ are somewhat closer, though the ratio can be as high as 2 for some instances of parameters.

Finally, all four policies incur higher costs with increase in (i) $\beta$ (faster spreading virus) (fig. 6.6), (ii) decrease in $R_0$ (fig. 6.7) (fewer initial dispatchers), (iii) increase in $K_u$ (larger security patches) (fig. 6.8) and (iv) increase in $I_0$ (larger initial infection) (fig. 6.9). Somewhat contrary to intuition, the overall cost might decrease by increasing $\delta$ (fig. 6.10). This is because increasing $\delta$ has two opposing effects: on one hand, it leads to a more rapid paralysis of the infective nodes and thereby increases the aggregate cost, however, on the other hand, a dead node is no longer able to propagate the infection. Thus, the process of killing the nodes may indeed dampen the spread of the virus and in turn reduces the overall cost by reducing the level of infection (and may even lead to fewer dead nodes) over time.

Recall that as per Theorem 6.2.1, the optimal dynamic control is bang-bang for linear $h(.)$
under both non-replicative and replicative dispatch models, and the jump points are the epochs of abrupt transitions of the immunization rates from 1 to 0. In figures 6.3(a) through 6.4(b), we explore the effect of changing $\pi, \beta, K_u, I_0, R_0, \delta$ on the jump points. Increasing $K_u$ naturally decreases the value of the jump point (fig. 6.4(a)), as a higher $K_u$ increases the bandwidth consumption cost related to $\vartheta$. However, there is no general trend for the variation of the jump point with increase in $\pi, \beta, R_0, I_0, \delta$ and the trends are problem specific. This is because a higher $\beta$ and/or $I_0$ indicates a more serious infection and a lower $R_0$ and/or $\pi$ indicates weaker defense, and in some scenarios these may prolong the initial maximum immunization effort to counter the more serious threat or compensate for the lower recovery rate, while with a different set of parameters, these may render the immunization comparably less effective, as the susceptible nodes will be rapidly claimed by the worm and may also be rapidly killed, thus making a shorter immunization period more favorable by cutting down on the bandwidth consumption cost and thus the aggregate cost. The lack of a general trend for the variation of the jump point with increase in $\delta$ is expected owing to the opposing effects of increasing $\delta$ on the aggregate cost. The figures, however, suggest that the initial period of maximum effort is shorter in case of replicative patching compared to that on non-replicative, as in the replicative patching the number of communication of patches increases exponentially fast and may result in a huge cost due to $\vartheta$, if it is not shut down to zero. Also, the value of the jump point is less sensitive to the value of $\beta$ and $I_0$, in the case of replicative patching compared with the non-replicative patching.

A practical issue in implementing the dynamic polices is that the system parameters ($\beta_0, \beta_1, I_0, \delta$) are not always accurately known, and only rough estimates are available. We therefore investigate the sensitivity of the efficacy of the defense to estimation inaccuracies. We evaluate the dynamic and static policies under potential inaccuracy of 50% in estimation of one parameter. Fig. 6.11 depicts the total cost incurred by the policies computed based on the estimated value of the parameters plotted in the horizontal axis when the center point is the value of the parameter in reality. As fig. 6.11(a) and 6.11(b) show, the increase in the total cost due to inaccurate estima-
tion of $I_0$ is low, indicating that the non-replicative and replicative dynamic policies are robust to the erroneous estimation of $I_0$. Also, the dynamic policies calculated using an inaccurate estimation of $I_0$ consistently outperform the best-static policies by a significant margin despite the presence of large estimation inaccuracies. Fig. 6.11(c) and 6.11(d) reveal similar robustness when the estimation of $\beta_0, \beta_1$ are erroneous (we assume equal $\beta_0, \beta_1$ in these computations).

Finally, we evaluate the performance, i.e., the overall cost, when dispatchers’ clocks drift from the global clock by different amounts, and hence they choose different controls which are shifted aside in time from the global control by their individual (additive) drift. We chose clock drifts which are statistically independent and uniformly distributed between $-\theta t^*$ and $+\theta t^*$, where $t^*$ is the calculated value of the threshold time. Fig. 6.12 depicts the overall cost as a function of $\theta$ averaged over 100 simulation runs. Note that even for $\theta$ as large as $t^*/2$ (i.e., 50% inaccuracy in the value of the threshold times) the increase in the overall damage as compared to the zero-drift case is less than 15%. 


Figure 6.6: varying $\beta$. Here, $R_0 = 0.1$, $K_u = 10$, $\delta = 0.005$ and $I_0 = 0.1$.

Figure 6.7: varying $R_0$. Here, $\beta = 0.20$, $K_u = 10$, $\delta = 0.005$ and $I_0 = 0.1$

Figure 6.8: varying $K_u$. Here, $\beta = 0.20$, $R_0 = 0.1$, $\delta = 0.005$ and $I_0 = 0.1$

Comparison of costs for four policies.
Figure 6.9: varying $I_0$. Here, $\beta = 0.20$, $R_0 = 0.1$, $\delta = 0.005$ and $K_u = 10$.

Figure 6.10: varying $\delta$. Here, $\beta = 0.20$, $R_0 = 0.1$, $K_u = 10$, $I_0 = 0.1$.

(Continuation of) comparison of costs for four policies.
Figure 6.11: Robustness of the dynamic policy. The increase in the overall cost, as a result of 50% inaccuracy in the estimation of the value of $I_0$ and $\beta_0$ is less than 5%.
Figure 6.12: Robustness of the patching with respect to clock drift. The increase in the overall cost is less than 15%.
Part III

Game
Introduction

In part I, we consider two different attack settings, and we derived optimal dynamic attack policies assuming that the defense counter-measures are static and set a priori. In part II, we investigated the complementary problem of optimal dynamic defense policies when the modus operandi of the malware is unaltered over time. Given the flexibility that software-based operation provides, it can be expected that future malware will demonstrate a dynamic behavior over time in response to the dynamics of the network, in order to maximize the overall damage it inflicts. In return, the network should also dynamically change its counter-measure policies to more effectively oppose the spread of the infection. The infinite dimension of freedom introduced by variation over time and antagonistic optimization of malware and network against each other demand new attempts for modeling and analysis of their confrontation. This chapter investigates such confrontations and identifies maximum damage dynamic strategies of attack and devises robust dynamic defense before such threats emerge.

The worm may disrupt the normal functionalities of the hosts, steal their private information, and use them to eavesdrop on other nodes. A worm can also render the host dysfunctional by deliberately draining its battery, or by executing a pernicious code that incurs irretrievable critical hardware or software damage. We specifically consider the latter to be the decision action of the malware over time.

Upon the outbreak of a new worm, anomaly detection techniques can be used to identify the presence of malicious activities and generate security patches [87] that can then be distributed among the nodes. Such patches either immunize susceptible nodes against future attacks, by rectifying their underlying vulnerability, or heal the infectives of the infection and render them robust against future attacks. In the meanwhile, reducing the communication rates in the network can quarantine the worm by slowing down its spread. Specifically, hosts can simply drop packets sent to them before processing them, or even refuse some connection requests, or reduce
the reception gain of their antennas.

Since the media in the wireless network is common and the channels are unreliable, the bandwidth consumed for distribution of the security patches can itself disrupt the normal functionality of the network. Hence, as in Chapter 6, excessive quarantining through reception rate reduction also deteriorates the quality of service (QoS) by introducing delays for the data traffic. Such quarantining can not usually discriminate based on the identity of the transmitters, since the hosts applying the reception rate control in general do not know which other nodes are infected; the reception rate itself may however be judiciously selected. The network’s challenge now is to achieve a guaranteed performance by selecting the instantaneous (a) rate of patching, and (b) reception rate, that jointly minimize the overall damage due to (i) the subversive activities of the malware that is capable of annihilating infectives, and (ii) the additional resource consumption and deterioration of QoS owing to the application of the countermeasures. The design must adapt over time, remaining cognizant of the malware’s ability to dynamically optimize its spread in response to the network’s dynamic strategy.

As in Chapter 4, the malware also faces a trade-off: should it kill its host as soon as feasible after infecting it? While a quick annihilation of a host inflicts a high instantaneous cost on the network, it also rules out the use of that node in infecting the remaining susceptibles. Thus, early mutilation of infective nodes may thwart the spread of malware. Moreover, killing a node deprives the malware of the other malicious activities the node can be used for, such as eavesdropping, stealing private information, etc. Deferral of killing, on the other hand, is at the risk of losing that node through installation of security patches and recovery of that node by the network.

A robust counter-measure is one that seeks to minimize the damage inflicted by the malware assuming that the malware chooses its strategy so as to maximize the damage with full knowledge of the counter-measure. Due to the above trade-offs and since an optimal strategy of the malware depends on the strategy of the network and vice versa, determination of the robust strate-
gies of either is non-trivial. In this section we propose a method to answer these questions.

First, we construct a mathematical framework which models the strategic confrontations between the malware and the network as a zero-sum dynamic game (§7.2.1), drawing from (i) a deterministic epidemic model for worm propagation in a wireless networks (§7.1), and (ii) damage functions that we introduce to investigate the trade-offs resulting from different decisions of the entities concerned (§7.1). We then prove the existence of the robust (i.e., saddle-point) strategies of the network and the malware (§7.1), and compute them (§7.2.2). Existence of such strategies and also their computations are not clear a priori, since the strategy set of each player is uncountably infinite and consists of functions of time and the model is non-linear.

We prove that the robust defense strategy has a simple two-phased structure (§7.2.3): (i) patch at the maximum possible rate until a threshold time, and then stop patching (ii) choose the minimum possible reception rate (i.e., the maximum packet drop rate at the receivers) until a threshold time and subsequently revert to the normal reception rate. The initial aggressive defense limits the spread of infection and thereby the pool of nodes that can potentially be compromised or killed; this guarantees an upper bound on the damage inflicted irrespective of the malware’s choice of annihilation strategy. Given its simple structure, the defense control can readily be implemented in resource constrained wireless devices. From a game-theoretical point of view, the structural results are somewhat surprising given the non-linear dynamics of state evolutions and the non-monotonicity of the state functions, and their proofs rely on our developed techniques.

Our numerical computations reveal that our robust dynamic defense strategy attains substantially lower value of the maximum damage inflicted by the malware as compared to that for heuristic static choice of defense parameters. Our dynamic strategies are shown robust to parameter estimation and clock drifts.
7.1 System model

Dynamics of state evolution

A susceptible accepts a communication request with a probability \( u^{N_r}(t) \). At any given \( t \), there are \( n_S(t) n_I(t) \) infective-susceptible pairs. Susceptibles are thus transformed to infectives at rate \( \hat{\beta} u^{N_r}(t) n_S(t) n_I(t) \). Infection propagation, therefore, can be contained through appropriate regulation of \( u^{N_r}(t) \) subject to: \( 0 < u^{N_r}_{\text{min}} \leq u^{N_r}(t) \leq u^{N_r}_{\text{norm}} \) at each \( t \). The lower bound \( u^{N_r}_{\text{min}} \) arises due to the minimum quality of service (QoS) requirements for data traffic (since the acceptance probability is the same irrespective of whether the request arrives from another infective, susceptible, or recovered node). The upper bound \( u^{N_r}_{\text{norm}} \) (which can be normalized to 1) provides the reception rate that nodes use for providing the desired QoS in absence of security considerations.

We now consider the dissemination of security patches in the network. As in Chapter 6, a pre-determined set of nodes, referred to as dispatchers (e.g., BS for cellular and exit-points for delay-tolerant networks) are pre-loaded with the patches. We assume that the dispatchers can not be infected, and that there are \( NR_0 \) dispatchers where the network parameter \( R_0 \), is between 0 and 1. Each node communicates with the dispatchers, and thereby fetches security patches, at an overall rate \( \hat{\beta} NR_0 u^{N_i}(t) \) at any time \( t \). The parameter \( \hat{\beta} \) depends on node density, mobility parameters, allowable transmission rates etc. (Chapter 2), whereas \( u^{N_i}(t) \) as the instantaneous transmission rate of the agents is a control function which can be used to regulate the bandwidth consumed in propagation of patches - the higher the value of \( u^{N_i}(t) \), the higher is the recovery rate but so is the resource consumption in patch transmission. Clearly, \( 0 \leq u^{N_i}(t) \leq 1 \) at each \( t \).

If the node that receives the patch is a susceptible node, it installs the patch and its state changes to recovered. If an infective receives the patch, the patch may fail to heal it, or, the worm may prevent its installation. We capture the above possibility, by introducing a coefficient \( 0 \leq \pi \leq 1 \):

\( ^5 \)The subscript \( r \) represents reception.
\( ^6 \)Superscript \( N \) designates control functions of the network, and \( M \) designates control functions of the malware.
\( ^7 \)The subscript \( i \) denotes immunization.
\( \pi = 0 \) occurs when the patch is completely unable to remove the worm from infectives and only immunizes the susceptibles, whereas \( \pi = 1 \) represents the other extreme scenario where a patch can equally well immunize and heal susceptibles and infective nodes.\(^8\) Now, if the patch heals an infective, its state changes to recovered, else it continues to remain an infective.

The worm at an infective host kills the host with rate proportional to \( u^M(t) \) at a given time \( t \); this is accomplished by executing specific codes with a probability of choice. The worm regulates the death process by appropriately choosing \( u^M(t) \) at each \( t \), subject to: \( 0 \leq u^M(t) \leq u^M_{\text{max}} \) at each \( t \). The upper bound arises due to processor constraints and the resulting limitations on the maximum rate of execution of such codes. Let \( \beta_0 := N\hat{\beta}, \beta_1 := N\tilde{\beta}R_0 \) and \( \beta_2 := \pi\beta_1 \). Our discussions lead to the following system of differential equations representing the dynamics of the system:

\[
\begin{align*}
\dot{S}(t) &= -\beta_0 u^N_r(t)S(t) - \beta_1 u^N_i(t)R_0 S(t) \quad S(0) = 1 - I_0 \\
\dot{I}(t) &= \beta_0 u^N_r(t)S(t) - \beta_2 u^N_i(t)R_0 I(t) - u^M(t)I(t) \quad I(0) = \lim_{N \to \infty} n_I(0)/N = I_0 > 0, \\
\dot{D}(t) &= u^M(t)I(t) \quad D(0) = 0
\end{align*}
\]

and also satisfy the following constraints at all \( t \):

\[
0 \leq S(t), I(t), D(t) \quad \text{and} \quad S(t) + I(t) + D(t) \leq 1.
\]

Thus, \((S(\cdot), I(\cdot), D(\cdot))\) constitute the system state functions, \( u^N(\cdot) = (u^N_r(\cdot), u^N_i(\cdot))\) constitutes the network control functions and \( u^M(\cdot)\) constitutes the malware’s control function. Note that nodes use identical reception, patching and killing rate functions irrespective of the states in their neighborhoods since they do not know these states. Nevertheless, since these rates are allowed to vary with time, they can be chosen in accordance with how the overall network states are expected to evolve.

\(^8\)In order to avoid immediate detection and blacklisting, the infectives may choose not to refuse all connection requests from the dispatchers.
Henceforth, wherever not ambiguous, we drop the dependence on $t$ and make it implicit.

Fig. 7.13 illustrates the transitions between different states of nodes and the notations used.

![State transitions](image)

Figure 7.13: State transitions. $u^{N_i}(t)$ and $u^{N_r}(t)$ are the control parameters of the network while $u^M(t)$ is the control parameter of the malware.

**Defense and attack objectives**

The total damage inflicted by the malware during the network operation interval $[0, T]$ is due to the presence of infectives, the death of nodes, the resources consumed for spreading the security patches, and the QoS deterioration due to the reduction of reception rate. Infectives can perform harmful activities over time. Dead nodes are inoperative and thus inflict a time-accumulative cost on the network as a result of the absence of its functionality. Moreover, they incur a final cost due to the fact that a (one time) price had been paid to purchase the node which is now destroyed (and probably needs to be replaced for future). The bandwidth overhead at time $t$ due to the media scanning and transmission of the security packets by the dispatchers is $R_0 u^{N_i}(t)$. Due to the reception rate control, the susceptibles lose a $u_{norm}^{N_r} - u^{N_r}(t)$ fraction of packets transmitted by all nodes which degrades the overall QoS. We therefore consider the aggregate network damage at time $t$ as a combination of $I(t), D(t), u^{N_i}(t), u^{N_r}(t)$. We adopt a linear cost function in this chapter for analytical tractability. Note that the damage function can be scaled so that one of the coefficients may be chosen as unity: we choose the one associated with the instantaneous
bandwidth overhead. Thus, the damage over the time horizon \([0, T]\) is\(^9\):

\[
J(u^N(t), u^M(t)) = \int_0^T [\kappa_I I(t) + \kappa_D D(t) + R_0 u^{NI}_r(t) - \kappa_r u^{NR}_r(t)] \, dt + K_D D(T),
\]

(7.1.3)

\(K_D D(T)\) relates to the final tally of the dead nodes. The coefficients are all non-negative and represent the relative importance of each corresponding term in the overall damage, e.g., if the worm gains the most by killing, and thereby completely disabling nodes, \(\kappa_D >> \kappa_I\). Let \(\kappa_I > 0, \kappa_r > 0\).

The network seeks to choose its control vector \(u^N(.)\) so as to minimize the above while the malware seeks to choose its control \(u^M(.)\) so as to maximize the above, subject to satisfying the state constraints (7.1.2) and ensuring that

\[
u_{\text{min}}^{NR} \leq u^{NR}_r(t) \leq u_{\text{norm}}^{NR}, \quad 0 \leq u^{NI}_r(t) \leq 1,
\]

(7.1.4a)

\[
0 \leq u^M(t) \leq u_{\text{max}}^M.
\]

(7.1.4b)

In §7.2, we model their interactions resulting from opposing objectives as a dynamic game. The formulation relies on the following result that allows us to ignore the state constraints without any loss of generality. The proof is similar to the counterpart lemmas in previous chapters and is relegated to the appendix, at the end of the chapter.

Lemma 7.1.1. Any pair of strategies \((u^N(.), u^M(.))\) that satisfy the control constraints (7.1.4a), (7.1.4b), satisfy the state constraints (7.1.2) and further ensure that \(I(t) > 0, S(t) > 0\) for all \(t \in [0, T]\).

7.2 Network-malware dynamic game

7.2.1 Formulation

Consider a system with two players \(N\) (network) and \(M\) (malware), specified by a system of \(n\) differential equations [48, P.83]:

\[
\dot{x}(t) = f \left( t, x(t), u^N(t), u^M(t) \right) \quad t \in [t_0, T], \text{ where } u^N(t) \in U^N \subset
\]

\[
\text{Note that } (u_{\text{norm}}^{NR} - u^{NR}) \text{ inside the integral is replaced by } -u^{NR} \text{ as } \kappa_r u_{\text{norm}}^{NR} T \text{ does not depend on the states or the controls.}
\]

140
and \( u^M(t) \in U^M \subset \mathbb{R}^s \), and the initial condition \( x(t_0) = x_0 \), and a damage function (the functional) \( J(u^N, u^M) = g(x(T)) + \int_{t_0}^{T} h(x, u^N, u^M, t) \, dt \), where \( x(t) \) is the \( n \)-dimensional state vector. Player \( N \) seeks to minimize \( J \) by choosing the \( m \)-dimensional control function \( u^N(.) \), and player \( M \) seeks to maximize \( J \) by choosing the \( s \)-dimensional control function \( u^M(.) \). The game is therefore referred to as a dynamic two-player zero-sum game. The players’ payoffs, and the set of strategies available to them are called rules of the game. Both players know the rules of the game and each player knows that its opponent knows the rule and ad infinitum.\(^{10}\) In this thesis we consider open-loop strategies, which is, the controls only depend on time (and say, not on the state, or the previous history). This is appropriate in the context of the security in networks, as the instantaneous state of the network (exact fraction of the nodes of each type) is impossible (or very costly) to follow, for both of the players.

In our context, (7.1.1) provides the \( f(.) \) functions, the initial conditions are provided by (7.1.1), (7.1.3) provides the \( g(.) \), \( h(.) \) functions, (7.1.4a), (7.1.4b) provide \( U^N, U^M \). Also, we have, \( n = 3, m = 2, s = 1 \). Note that the \( f(.) \), \( h(.) \) functions in our context depends on time \( t \) only implicitly, that is through the state and control functions. Also, the formulation does not capture any other constraints on the state functions, and in our context it does not need to either, owing to Lemma 7.1.1.

We now consider the values of the game. The lower value denoted by \( V_* \), is the overall damage when the minimizing player (N) is given the upper-hand, i.e., selects its strategy after learning its opponent’s strategy. Mathematically, \( V_* = \max_{u^M} \min_{u^N} J(u^N, u^M) \). Conversely, the upper value of the game \( V^* \) is defined as \( V^* = \min_{u^N} \max_{u^M} J(u^N, u^M) \) Thus, \( V_* (V^*, \text{resp.}) \) is the maximum (minimum, resp.) damage that the malware (network, resp.) can inflict (incur, resp.) if the other player has the upper-hand. Hence, \( V_* \leq V^* \). A pair of strategies \((u^N^*, u^M^*)\) is called a saddle-point if \( J(u^N^*, u^M^*) \leq J(u^N^*, u^M^*) = V \leq J(u^N, u^M^*) \) for any strategy \( u^N \) of the network and \( u^M \) of the malware, and then \( V \) is the value of the game, and \( V = V_* = V^* \).

\(^{10}\)each player knows that each player knows that the opponent knows etc.
Thus, if the network selects its saddle-point strategy $u^N*$, irrespective of the strategy of the malware, the damage it incurs is at most $V$, which is also the minimum damage that the malware can inflict if it has the upper-hand. Thus, the network’s saddle-point strategy is also its robust strategy, in the sense, that it minimizes the maximum possible damage it can incur. Conversely, the malware’s saddle point strategy is also its robust strategy, since it maximizes the minimum possible damage it can inflict. Also, the network’s and the malware’s saddle point strategies are their respective best responses to the other’s robust strategy.\footnote{Note also that if a pair of strategies that is a saddle point strategy among open loop policies, then it is also a saddle-point among closed-loop policies (i.e., policies which utilize the exact instantaneous state information as well). That is, no player can improve their reward by deviating from an open-loop saddle-point strategy to a closed-loop one. Note that the converse may not be true, i.e., there are cases in which there is no saddle-point among open-loop policies, but there is among closed loop ones.}

We prove the existence of saddle-point pair in the next theorem.

**Theorem 7.2.1.** *The dynamic game defined above has a saddle-point pair of strategies.*

*Proof.* This theorem directly follows from theorem 2 in page 91 of [48]. The necessary conditions of the theorem are readily satisfied in our game. Namely:

(i): the system function $f(t, x, u^N, u^M)$ in this game is continuous in states and controls and is moreover bounded. Note that this is sufficient for the condition in page 83 of [48] to hold.

(ii): the instantaneous pay-off function $h(t, x, u^N, u^M)$ and the terminal pay-off function $g(x(T))$ are continuous in the states and controls (page 84 of [48]).

(iii): the system function $f(t, x, u^N, u^M)$ is linear in controls. the set defining controls are convex sets; and the instantaneous pay-off function $h(t, x, u^N, u^M)$ is linear in controls (page 91 of [48]).

\[\square\]
7.2.2 A framework for computation of the saddle-point strategies

Since the set of deterministic strategies of each player is uncountably-infinite, the saddle-point strategies and the value of the game can not be computed using convex or linear programming.

We now present a framework for numerical computation of the saddle-point strategies.

Define the Hamiltonian for a given policy pair \((u^N, u^M)\) in an arbitrary two-person dynamic game as

\[
H(u^N, u^M) = \langle \lambda, f(x, u^N, u^M, t) \rangle + h(x, u^N, u^M, t),
\]

where the state functions \(x(.)\) are those that correspond to the strategy pair \((u^N, u^M)\), and \(\lambda\), the co-state (or adjoint) functions, are continuous and piecewise differentiable functions of time that satisfy the following system of differential equations wherever the controls \((u^N, u^M)\) are continuous:

\[
\dot{\lambda} = -\partial H/\partial x(x,\lambda,t) = -\kappa_N u^N_r I + (\lambda_I - \lambda_S)\beta_0 u^N_r IS - \lambda_S \beta_1 R_0 u^N_i S - \lambda_I \beta_2 R_0 u^N_i I + (\lambda_D - \lambda_I) u^M I
\]

where again the state functions \((S(.), I(.), D(.))\) are obtained from (7.1.1) with \((u^N(.), u^M(.))\) as the control functions, and the co-state functions \((\lambda_S(.), \lambda_I(.), \lambda_D(.))\) are obtained from the following system of differential equations (with \((u^N(.), u^M(.))\) as the control functions) with the final conditions:

\[
\dot{\lambda}_S = -\partial H/\partial S = - (\lambda_I - \lambda_S)\beta_0 u^N_r I + \lambda_S \beta_1 R_0 u^N_i, \quad \lambda_S(T) = 0
\]

\[
\dot{\lambda}_I = -\partial H/\partial I = -\kappa_I - (\lambda_I - \lambda_S)\beta_0 u^N_r S + \lambda_I \beta_2 u^N_i R_0 - (\lambda_D - \lambda_I) u^M, \quad \lambda_I(T) = 0
\]

\[
\dot{\lambda}_D = -\partial H/\partial D = -\kappa_D, \quad \lambda_D(T) = K_D.
\]

Then, following [48, P.31], a necessary condition for the pair \((u^N, u^M)\) to be a saddle-point strategy pair is that for all \(t \in [0, T] :\)

\[
(u^N, u^M) \in \arg\min_{\tilde{u}^N} \max_{\tilde{u}^M} H(\tilde{u}^N, \tilde{u}^M) \quad \text{and} \quad (u^N, u^M) \in \arg\max_{\tilde{u}^M} \min_{\tilde{u}^N} H(\tilde{u}^N, \tilde{u}^M).
\]

(7.2.2a, 7.2.2b)
Henceforth, we denote the saddle point strategy pair as $(u^N(\cdot), u^M(\cdot))$, and $(S(\cdot), I(\cdot), D(\cdot))$, $(\lambda_S(\cdot), \lambda_I(\cdot), \lambda_D(\cdot))$ as the corresponding state and co-state functions and $\mathcal{H}$ as the corresponding Hamiltonian. We now express $(u^N(\cdot), u^M(\cdot))$ in terms of $(S(\cdot), I(\cdot), D(\cdot)), (\lambda_S(\cdot), \lambda_I(\cdot), \lambda_D(\cdot))$ using the necessary conditions (7.2.2). Define $\psi^{Nr} := (\lambda_I - \lambda_S)\beta_0 IS - \kappa_r$, and $\psi^{Ni} := R_0 - \lambda_S\beta_1 R_0 S - \lambda_I\beta_2 R_0 I$, and $\psi^M := (\lambda_D - \lambda_I)I$. Now, the Hamiltonian can be rewritten as:

$$\mathcal{H} = \kappa_I I + \kappa_D D + \psi^{Nr} u^{Nr} + \psi^{Ni} u^{Ni} + \psi^M u^M.$$ (7.2.3)

Thus, the Hamiltonian is a separable function of different components of the defense controls $(u^{Nr}(\cdot), u^{Ni}(\cdot))$ and the attack control $u^M(\cdot)$, that is, each of these appear in different terms in the R.H.S of the above characterization. Now, from the necessary conditions in (7.2.2) subject to the control constraints in (7.1.4), the saddle-point strategies are derived as:

$$u^{Nr} = u^{Nr}_{\min} \text{ if } \psi^{Nr} > 0 \text{ and } u^{Nr} = u^{Nr}_{\text{norm}} \text{ if } \psi^{Nr} < 0,$$ (7.2.4)

$$u^{Ni} = 0 \text{ if } \psi^{Ni} > 0 \text{ and } u^{Ni} = 1 \text{ if } \psi^{Ni} < 0,$$ (7.2.5)

$$u^M = u^M_{\max} \text{ if } \psi^M > 0 \text{ and } u^M = 0 \text{ if } \psi^M < 0.$$ (7.2.6)

Since $\psi^{Nr}, \psi^{Ni}, \psi^M$ are uniquely specified once the state and the co-state functions are known, the above relations express the saddle-point strategies in terms of the state and co-state functions. The strategies $u^{Nr}(\cdot), u^{Ni}(\cdot), u^M(\cdot)$ can be substituted by the above characterizations in (7.1.1) and (7.2.1), resulting in a system of 6 differential equations involving only the state and the co-state functions. Using standard numerical methods for solving differential equations, this system can be solved (very fast) using the initial and final conditions (7.1.1), (7.2.1). The state and co-state functions obtained as solutions will now provide the $\psi^{Nr}, \psi^{Ni}, \psi^M$ functions, and thereby the saddle-point strategies via (7.2.4), (7.2.5), (7.2.6). The resulting set of differential equations is non-linear and a closed-form solution is unknown. However, as we will show in the next section, using novel techniques, even without access to the closed-form solution, we can establish the type of behavior that the saddle-point strategies exhibit.
7.2.3 Structural properties of saddle-point defense strategy

We establish that the saddle-point defense strategy has a simple threshold-based structure that ought to facilitate its implementation in a localized manner in resource constrained wireless devices. Specifically, we prove that:

**Theorem 7.2.2.** For the saddle-point defense strategy $u^N(\cdot) = (u^{Nr}(\cdot), u^{Ni}(\cdot))$, there exists times $t_1, t_2, 0 \leq t_1 < T, 0 \leq t_2 < T$ such that:

- $u^{Nr}(t) = u^{Nr}_{\min}$ for $0 < t < t_1$, and $u^{Nr}(t) = u^{Nr}_{\norm}$ for $t_1 < t < T$.

- $u^{Ni}(t) = 1$ for $0 < t < t_2$, and $u^{Ni}(t) = 0$ for $t_2 < t < T$.

Theorem 7.2.2 states that the control functions should be applied with most intensity at the beginning of the epidemic period. In retrospect, this makes intuitive sense. Note that the costs associated with patching and rate reductions depend only on the area beneath the functions $u^{Ni}(t)$ and $u^{Nr}(t)$. Thus, by keeping the areas the same and shifting a candidate function to earlier times, this portion of the cost does not change. Choosing higher values of the patching rate (larger $u^{Ni}$) and lower values of reception rates (smaller $u^{Nr}$) later (as opposed to earlier) will only let the number of infective and dead nodes increase. This is because each susceptible that is infected can serve the propagation of the infection. This increases the integrations of the $\kappa_I I(t)$
and $\kappa_D D(t)$ as well as $K_D D(T)$. Moreover, this leads to a reduced efficacy of the recovery process - the latter happens because healing (of an infective node) is not as fast as the immunization (of a susceptible node) since $\pi \leq 1$ (equivalently $\beta_2 \leq \beta_1$). Note that the proof of the Theorem exploits the latter property. Thus, irrespective of the killing strategy of the malware, the containment of the epidemic ought start as soon as possible, if it is worth taking any action at all. The fact that the defense actions should come to a complete halt (rather than a gradual decline) is however less direct to predict.

Note that the defense strategy always chooses either the maximum or the minimum values of the parameters except possibly in a set of measure zero (i.e., except possibly at $t_1, t_2$). Such strategies are referred to as bang-bang in the control literature. The durations of the phases (i.e., the values of the threshold times $t_1, t_2$) and which defense subsides in the interim watchful period, depend on the damage coefficients $\kappa_I, \kappa_D, K_D, \kappa_r, \kappa_i$. We will shed more light on the latter in Theorem 7.2.4 later. But first, we conclude this sub-section by proving Theorem 7.2.2.

**Proof.** The continuity and piecewise differentiability of $\psi^{Nr}(\cdot)$, $\psi^{Ni}(\cdot)$ follows from those of the co-state functions. From the final conditions on the co-state functions, i.e., (7.2.1), $\psi^{Nr}(T) = -\kappa_r < 0$, $\psi^{Ni}(T) = R_0 > 0$. We show that $\psi^{Nr}(\cdot)$ ($\psi^{Ni}(\cdot)$, resp.) is a strictly decreasing (increasing, resp.) function of time. Thus, each has at most one zero-crossing point in $(0, T)$; denote these as $t_1, t_2$. If $\psi^{Nr}$ ($\psi^{Ni}$, resp.) has no zero crossing point in $(0, T)$, $t_1 = 0$ ($t_2 = 0$, resp.). Thus, from the continuity of the $\psi(\cdot)$ functions, and from their terminal values, (i) $\psi^{Nr}(\cdot)$ is negative in $(t_1, T)$ and positive in $(0, t_1)$, and (ii) $\psi^{Ni}(\cdot)$ is positive in $(t_2, T)$ and negative in $(0, t_2)$. The theorem follows from (7.2.4) and (7.2.5). We prove the strict monotonicity of $\psi^{Nr}(\cdot), \psi^{Ni}(\cdot)$, using:

**Lemma 7.2.3.** $\lambda_S > 0$ and $\lambda_I > \lambda_S, \lambda_D \geq 0 \forall t, 0 < t < T$.

The lemma is intuitive since the shadow prices (i.e., co-state variables) associated with the susceptibles and dead nodes ought to be positive, and also the shadow price associated with the infectives ought to be at least as high as that associated with susceptibles. However, as we
will see next, the proof requires detailed analysis of the state and co-state differential equations (7.1.1), (7.2.1) respectively, and is less direct.

**Proof.** Since \( \lambda_D(T) = K_D \geq 0 \) (from (7.2.1)), and \( \frac{d}{dt} \lambda_D \leq 0, \lambda_D \geq 0 \). Now, for the rest, we argue in two steps.

**Step 1:** \( \lambda_S(T) = 0 \) and \( \lambda_I(T) = K_I = 0 \), also: \( \dot{\lambda}_I(T) - \dot{\lambda}_S(T) = \dot{\lambda}_I(T) = -\kappa_I - K_D u^M(T) < 0 \). Therefore, \( \exists \epsilon > 0 \) s.t. on \((T - \epsilon \ldots T)\) we have \( \lambda_S > 0 \) and \( (\lambda_I - \lambda_S) > 0 \).

**Step 2:** Proof by contradiction. Let \( \tau \) be such that: \( \lambda_S > 0, (\lambda_I - \lambda_S) > 0 \) on \((\tau \ldots T)\) & \( \lambda_S(\tau) = 0 \) OR \( \lambda_I(\tau) = \lambda_S(\tau) \). From the continuity of the co-state functions, \( (\lambda_I(\tau) - \lambda_S(\tau)) \geq 0 \), and \( \lambda_S(\tau) \geq 0 \).

We first prove that \( (\lambda_I(\tau) - \lambda_S(\tau)) > 0 \). Suppose not. Then, \( \lambda_I(\tau) = \lambda_S(\tau) \). Thus: \( \dot{\lambda}_I(\tau) - \dot{\lambda}_S(\tau) = -\kappa_I + \lambda_I \beta_2 u^N - (\lambda_D - \lambda_I) u^M - \lambda_S \beta_1 u^N = -\kappa_I - \lambda_S u^N (\beta_1 - \beta_2) - (\lambda_D - \lambda_I) u^M \). Here, (i) the first term is strictly negative\(^{12}\), (ii) the second term is negative because \( \lambda_S(\tau) \geq 0 \) and \( \beta_2 \leq \beta_1 \) and (iii) the third term is negative because of (7.2.6). Thus, \( \dot{\lambda}_I(\tau) - \dot{\lambda}_S(\tau) > 0 \). But, then both \( \lambda_I(\tau) = \lambda_S(\tau) \), and \( (\lambda_I - \lambda_S) > 0 \) on \((\tau \ldots T)\) can not happen. Thus, \( (\lambda_I(\tau) - \lambda_S(\tau)) > 0 \).

Now, suppose \( \lambda_S(\tau) = 0 \). \( \dot{\lambda}_S(\tau) = - (\lambda_I - \lambda_S) \beta_0 u^N \big|_\tau < 0 \). The last inequality follows since \( (\lambda_I(\tau) - \lambda_S(\tau)) > 0 \), \( \beta_0 > 0 \), \( u^N \geq u^N_{\min} > 0 \) and \( I(\tau) > 0 \) (lemma 7.1.1). This again contradicts the assumptions that \( \lambda_S(\tau) = 0 \) and \( \lambda_S > 0 \) on \((\tau \ldots T)\). Thus, \( \lambda_S(\tau) \neq 0 \), and hence \( \lambda_S(\tau) > 0 \).

**Strict monotonicity of \( \psi^{N_r}(\cdot) \)**

We show that \( \dot{\psi}^{N_r}(t) \) is strictly negative at all \( t \in (0, T) \)\(^{13}\)

\[
\dot{\psi}^{N_r} = \frac{\partial}{\partial \theta} \psi^{N_r} = (\lambda_I - \lambda_S) \beta_0 IS + (\lambda_I - \lambda_S) \beta_0 I \dot{S} + (\lambda_I - \lambda_S) \beta_0 I \dot{S} \]

\(^{12}\)Negative in this proof is distinguished from strictly negative.
which after replacement and simplification yields

\[
\frac{\dot{\psi}_{NI}}{\beta_0 IS} = -\kappa_I - (\lambda_D - \lambda_S)u^M - \beta_1 I u^N_i + \beta_2 S u^N_i \\
= -\kappa_I - (\lambda_D - \lambda_I)u^M - (\lambda_I - \lambda_S)u^M - (\beta_1 - \beta_2) I u^N_i - (\lambda_I - \lambda_S) \beta_2 u^N_i.
\]

From (7.2.6), lemma 7.2.3 and since \(\kappa_I > 0, \beta_1 \geq \beta_2, u^M(t) \geq 0, u^N_i(t) \geq 0\) at all \(t\), the right hand side is negative. The result follows since \(\beta_0 > 0\) and \(S(t) > 0, I(t) > 0\) at all \(t\) (lemma 7.1.1).

**Strict monotonicity of \(\psi_{NI}(\cdot)\)**

\[
\dot{\psi}_{NI} = \frac{\partial}{\partial t} \psi_{NI} = (\dot{\lambda}_I - \dot{\lambda}_S) \beta_0 IS + (\lambda_I - \lambda_S) \beta_0 IS + (\lambda_I - \lambda_S) \beta_0 IS
\]

\[
= \kappa_I \beta_2 + \beta_2 u^M \lambda_D + \beta_0 \beta_1 S u^N_i (\lambda_I - \lambda_S)
\]

The R.H.S is positive from lemma 7.2.3 and since \(\kappa_I > 0, \beta_0 > 0\). Thus, \(\dot{\psi}_{NI} > 0\) since \(\beta_0 > 0\) and \(I(t) > 0\) at all \(t\) (lemma 7.1.1).

\[\square\]

In the next theorem, we show that under a sufficient condition, the quarantining period (by reduction of communication rates) ends before the immunization/healing effort is stopped. This is in accordance with our intuition that the primary use of quarantining is *buying time* for the recovery process in the network.

**Theorem 7.2.4.** Let \(t_1\) and \(t_2\) be as defined in Theorem 7.2.2. If \(\kappa_r \geq \frac{\beta_0 S_0}{\beta_2}\), then either \(t_2 = 0\) or \(t_1 < t_2\).

Note that the condition of the theorem is quite intuitive. For instance, if \(\beta_0 = \beta_2\), this condition is satisfied when \(\kappa_r \geq 1\). Recall that the coefficients of the costs were rescaled so that the coefficient of the cost of patching is normalized. Thus, this means when the instantaneous cost of per unit reduction of communication rates (quarantining) is no less than per unit patching. The [13]partial derivative w.r.t time, only because of the dependence also on the initial values for the states. Otherwise, \(t\) is the only independent variable.
other parameters in $\kappa_r \geq \frac{\beta_0 S_0}{\beta_2}$ refer to the cases of relatively small initial susceptible pool, and a relatively fast healing rate. Intuitively, when the healing rate is slow compared to the propagation rate of the infection, it might not be prudent to relax the communication rates of the nodes to normal soon, which is compatible with the condition of the theorem.

**Proof.** Recall from the proof of Theorem 7.2.2 that $\psi^{N_r}(t)$ and $\psi^{N_i}(t)$ each have at most one zero-crossing point and $\psi^{N_r}(t)$ terminates in a negative, and $\psi^{N_i}(t)$ terminates in a positive value at $T$. We now show that the value of $\psi^{N_i}(t)$ at a potential zero-crossing point of $\psi^{N_r}(t)$, is strictly negative.

$$\psi^{N_r} = (\lambda_I - \lambda_S)\beta_0 IS - \kappa_r = 0 \Rightarrow \lambda_I = \frac{\kappa_r}{\beta_0 IS} + \lambda_S,$$

then:

$$\psi^{N_i} = R_0 - \lambda S \beta_1 R_0 S - \lambda_1 A_2 R_0 I = R_0 - \lambda S \beta_1 R_0 S - \lambda_2 A_0 I (\frac{\kappa_r}{\beta_0 IS} + \lambda_S)$$

$$= R_0 (1 - \beta_2 \frac{\kappa_r}{\beta_0 S}) - \lambda S \beta_1 R_0 S - \lambda S \beta_2 A_0 I$$

According to lemmas 7.1.1 and 7.2.3, the last two terms are strictly negative. The first term is negative following the condition of the theorem (i.e., $\kappa_r \geq \frac{\beta_2 S_0}{\beta_0}$) and the fact that $S$ is a non-increasing function of time. Similarly, at a potential zero-crossing point of $\psi^{N_i}(t)$, we have $\psi^{N_r}(t) = -\lambda S (-\frac{\beta_0 \beta_1 S^2}{\beta_2} - \beta_0 IS) + \frac{\beta_0 S}{\beta_2} - \kappa_r$, which is strictly negative again following lemmas 7.1.1 and 7.2.3 and the sufficient condition of the theorem. The theorem follows from the continuity of $\psi^{N_i}(t)$ and $\psi^{N_r}(t)$ and by referring to (7.2.4) and (7.2.5).

Note that the case of $t_2 = 0$ occurs when $\psi^{N_i}$ does not have a zero-crossing point and is hence non-negative throughout $[0, T]$. In this case, the immunization/healing effort is never launched.

### 7.2.4 Structure of the saddle-point attack strategy

The saddle-point attack has a simple **first-amass, then slaughter** structure in the special case that the worm benefits from killing only through the final tally of the dead (i.e., $\kappa_D = 0$), and the patches can only immunize the susceptibles, but can not heal the infectives (i.e., $\beta_2 = 0$). Specifically:
Theorem 7.2.5. For the saddle-point attack strategy $u^M(\cdot)$, there exists a time $t_3$, $0 \leq t_3 < T$ such that $u^M(t) = 0$ for $0 < t < t_3$, and $u^M(t) = u^M_{\text{max}}$ for $t_3 < t < T$.

Thus, the worm does not kill any infective during the initial amass period of $(0, t_3)$ when it uses them to spread the infection; it slaughters them at the maximum rate subsequently. The intuition behind this structure is as follows. Once the worm infects a host, it never loses it to the recovery process, and thus, since it benefits from killing a host only because this enhances the final tally of the dead, it ought to kill hosts towards the end and utilize them before. The proof follows.

Proof. Note that $\psi^M(T) = K_I I(T) > 0$ (because of lemma 7.1.1). Thus, as in the proof of Theorem 7.2.2, the result follows if we can show that $\psi^M(t)$ crosses zero at most once. We establish this slightly differently: we show that $\dot{\psi}^M$ is strictly positive at its zero-crossing point (as opposed to showing it for all $t$). But this is also sufficient to conclude $\psi^M$ has at most one zero-crossing point.

$$\dot{\psi}^M = I(\dot{\lambda}_D - \dot{\lambda}_I) + I \dot{\psi}^M = \kappa_I - \kappa_D + u^M(\lambda_D - \lambda_I) - \beta_2 \lambda_I u^N_i + S \beta_0 u^N_r (\lambda_I - \lambda_S) + I \dot{\psi}^M$$

At a zero-crossing point of $\psi^M$, the last term vanishes. Now, $\kappa_D = \beta_2 = 0$, and the remaining terms are all non-negative because of (7.2.6) and lemma 7.2.3. The result follows since $\kappa_I > 0$. \hfill \square

The saddle-point attack strategy may however be more involved when either $\beta_2 > 0$ or $\kappa_D > 0$. For example, fig. 7.14 depicts the saddle point strategies and the state evolution in an example scenario where $\kappa_D = 13$, $\beta_2 = 4.47$. The malware starts killing the nodes from the beginning, but then it stops the killing and infects the newly accessible susceptible nodes, boosting the fraction of the infective and towards the end, starts to kill them all again.
Figure 7.14: State evolution and saddle-point strategies. The parameters of the game are as follows: $\kappa_I = 10$, $\kappa_D = 13$, $\kappa_u = 10$, $\kappa_r = 5$, $K_I = K_D = 0$, $\beta_2 = \beta_1 = \beta_0 = 4.47$, $\pi = 1$, and initial fractions $I_0 = 0.15$, $R_0 = 0.1$, $D_0 = 0$, and $T = 4$.

7.3 Performance evaluation

Advantage of Dynamic Strategies We will assess the advantage of considering a dynamic game and implementing saddle-point strategies as robust defense against a dynamically optimizing malware. We now measure the gap between the maximum value of the incurred damage if the defense parameters, i.e., $u^{N_r}$ and $u^{N_i}$, do not change with time, and that when saddle-point defense strategies are used. We will refer to the former as static strategies. Fig. 7.18 depicts the maximum damages incurred by the best static and dynamic saddle-point defense strategies for different values of the initial fraction of infective nodes (i.e., $I_0$ is between 0.1 to 0.6) when the other parameters are the same as those reported in the caption of fig. 7.15. By best static, we mean the fixed reception rate, as well as the fixed dissemination rate of patches are those that achieve the least damage among all possible fixed choices. Saddle-point defense strategies result in a 220% to 270% reduction in the overall damage.

The effect of parameters of the network on the saddle-point defense policy We established that both of the controls of the defense, i.e., reducing the reception gain and disseminating security patches follow a bang-bang structure with only one jump (though in opposing directions).
Figure 7.15: Saddle-point defense and attack strategies for the game considered in §7.3. Here, $\kappa_I = 10$, $\kappa_D = 20$, $\kappa_u = 10$, $\kappa_r = 15$, $\beta_1 = \beta_0 = 0.109$, $\beta_2 = K_I = K_D = 0$, and initial fractions $I_0 = 0.1$, $R_0 = 0.1$, $D_0 = 0$, and $T = 4$.

Hence the saddle-point defense strategy is completely identified by these two jump points. In figures 7.16(a) through 7.16(d) we can see how varying $I_0$ and $\beta$, respectively, affects the value of these jump points. Note that the reduction of reception gains is effective only when there are both a considerable number of susceptibles and infectives in the network. For higher initial fraction of infectives, the damage from malware will be higher, calling for more intense defense. However, higher initial fractions of infectives mean lower fractions of susceptibles to be immunized which renders prolonging the quarantine pointless. For these opposing effects, in general, the jump points do not exhibit any specific trends with respect to the initial level of infection. However, we observe that the jump points increase with increase in $\beta$ since higher $\beta$ renders the infection more potent. Also as we observe, the jump point in $u^N_i$ is mostly less than the jump point in $u^N_r$, that is, the reception gain of the susceptibles returns to normal before the patching is stopped.

Note that this is the same property that is prescribed in Theorem 7.2.4, however, for none of the set of parameters selected in figures 7.16, the sufficiency condition of the theorem is met. Also here, the normalized $\kappa_r$ is $5/10 = 0.5$ and $S_0 \geq 0.5$ and for $\pi = 1$, $\beta_0 = \beta_2 = \beta$. This shows that the structural result of theorem 7.2.4 mostly holds even when its condition is not satisfied.

**Robustness to parameter estimation** Calculation of the jump points and hence identifying the saddle-point defense strategy assumes knowledge of the parameters of the system. Specifically,
the initial penetration of the infection \((I_0)\) and its diffusion rate \(\beta\). In practice, however, the network operator may only have access to a rough estimate of these values. Figures 7.16(a) through 7.16(d) also suggest that the defense recipe does not change drastically for a slight variation in the parameters of the system, \(I_0\) and \(\beta\). Here, we specifically investigate the sensitivity of the overall damage with respect to the estimation of \(I_0\) and \(\beta\). In figures 7.17(a) and 7.17(b), the actual value of \(I_0\) and \(\beta\) is the value in the center, i.e., \(I_0 = 0.2\) and \(\beta = 4\). The defense saddle-point policies are, however, calculated based on estimated values of \(I_0\) and \(\beta\) (the x-axes, respectively). The attacker is assumed to know the exact values to obtain a worst-case scenario. As we can see, the increase in the overall damage as a result of erroneous estimations of \(I_0\) and \(\beta\), up to 50% error, is less than 2%. This shows that not only our dynamic saddle-point defense strategies are robust against the killing strategy of the attacker, but also they are robust against errors in the estimation of the parameters of the network and attack.

Appendix: Proof of Lemma 7.1.1 Statement: Any pair of strategies \((u^N(\cdot), u^M(\cdot))\) that satisfy the control constraints (7.1.4a), (7.1.4b), satisfy the state constraints (7.1.2) and ensure that \(I(t) > 0, S(t) > 0\) for all \(t \in [0, T]\).

Proof. All \(S, I\) and \(D\), resulting from (7.1.1) (and thus any continuous functions of them) are continuous functions of time. Since \(0 < I_0 < 1\), the initial conditions in (7.1.1) ensure that the state constraints \(S > 0\) and \(I > 0\) are strictly met at \(t = 0\). The continuity of \(S\) and \(I\) functions ensure that there exists an interval of nonzero length starting at \(t = 0\) on which both \(S\) and \(I\) are strictly positive. Thus, from (7.1.1c) and since \(u^M(t) \geq 0, \dot{D} \geq 0\) in the above interval. Thus, since \(D(0) = 0, 0 \leq D\) in this interval as well. Since \(\frac{d}{dt}(S+I+D)|_{t=0} = -\beta_1 u^{N_1}(0)R_0 S(0) - \beta_2 u^{N_2}(0)R_0 I(0) \leq 0\) and \(S(0) + I(0) + D(0) = 1\), there exists an interval after \(t = 0\) over which the constraint of \(S(t) + I(t) + D(t) \leq 1\) is met.

Now, suppose by contradiction that \(t_0 \leq T\) be the first time after \(t = 0\) at which, at least one of the constraints of \(0 \leq S, I\) and \(S + I + D \leq 1\) becomes active, or \(0 \leq D\) becomes violated
right after it. That is, at \( t_0 \), we have (1) \( S = 0 \) OR (2) \( I = 0 \) OR (3) \( S + I + D = 1 \) OR (4) there exists an \( \epsilon > 0 \) such that \( D < 0 \) on \((t_0 \cdots t_0 + \epsilon)\); AND throughout \((0, t_0)\), we have \( 0 < S, I \) and \( S + I + D < 1 \) and \( D \geq 0 \). Hence, for \( 0 \leq t < t_0 \) from (7.1.1a) we have \( \dot{S} \geq -\beta_0 S - \beta_1 R_0 \). Hence, \( S(t) \geq S(0) e^{-(\beta_0 + \beta_1 R_0)t} \) for all \( 0 \leq t < t_0 \). Since \( S(0) > 0 \), \( I(0) > 0 \), neither (1) nor (2) could have happened. Also, \( \frac{d}{dt}(S + I + D) \leq \beta_2 u_N(t) R_0 S(t) - \beta_2 u_N(t) R_0 I(t) \leq \beta_1 R_0 S(0) e^{-(\beta_0 + \beta_1 R_0)t} - \beta_2 R_0 I(0) e^{-(\beta_0 + \beta_2 R_0)t} < 0 \) throughout \([0 \cdots t_0]\). Since \( S(0) + I(0) + D(0) = 1 \) we have \((S + I + D)|_{t=t_0} < 1 \), showing that (3) is impossible. Moreover, from (7.1.1c), and since \( I(t_0) > 0 \), and \( I \) is continuous, there exists an \( \epsilon' \) such that \( \dot{D} \geq 0 \) over \((t_0 \cdots t_0 + \epsilon')\). From continuity of \( D \), \( D(t_0) \geq 0 \). Thus, \( 0 \leq D \) over \((t_0 \cdots t_0 + \epsilon')\), dismissing the possibility of (4). This negates the existence of \( t_0 \) and the lemma follows.

\[ \text{(a) varying } I_0, \pi = 0 \quad \text{(b) varying } I_0, \pi = 1 \]
\[ \text{(c) varying } \beta, \pi = 0 \quad \text{(d) varying } \beta, \pi = 1 \]

Figure 7.16: The effect of variation of the parameters of the system \((I_0, \beta \text{ and } \pi)\) on the nature of the saddle-point strategy, specifically, the jump point in \( u_N^t(t) \) (marked with circles) and jump point in \( u_R^t(t) \) (marked with triangles). The other parameters of the system, i.e., the parameters of the damage function are as follows \( k_I = 10, k_D = 15, k_r = 5, k_u = 10 \).
Figure 7.17: In fig. 7.17(a) the actual value of $I_0$ is the center value, i.e., $I_0 = 0.2$. Similarly, in fig. 7.17(b), the real value of $\beta$ is 4. The x-axes respectively represent the values of $I_0$ and $\beta$ that the system estimates. The attacker is assumed to know the exact values to obtain a worst-case scenario. The increase in the overall damage as a result of erroneous estimations of $I_0$ and $\beta$, up to 50% error, is less than 2%. The rest of the parameters are $k_I = 10$, $k_D = 13$, $k_r = 5$, $k_u = 10$.

Figure 7.18: Comparison of the maximum damage for the best static choice of defense parameters and dynamic saddle-point defense strategies.
Part IV

Generalization and Applications
8.1 Introduction

In previous chapters, we demonstrated how our mathematical framework based on optimal control theory can be utilized to investigate countering the spread of a malware in a communication network. Specifically, we showed how one can extract substantial information about the structure of the optimal (attack and defense) strategies without having access to a closed-form solution. In this section, we demonstrate the extent of generality of our model and our techniques through diverse examples.

A special case of the epidemic evolution in fig. 8.19 captures propagation of messages in Delay Tolerant Networks (DTNs). A server may seek to broadcast a message to as many nodes as possible, before a deadline, by employing minimal resources such as energy and bandwidth. In this case, susceptibles are the nodes that are yet to receive the message, and the recovered are the ones which have received it. Dissemination of the message may either be performed in non-replicative or replicative manner. In either case, the decision problem is whether (and at what rate) should a recipient of a message transmit it upon contact to other mobile nodes which do not have a copy of the message, before the deadline for delivery of the message is passed and the message is dropped. Infectives and dead nodes are absent in this problem. The overall ‘cost’ is (i) decreasing in the number of recovered (i.e., recipient) nodes, and is (ii) increasing in the transmission rates of the activated disseminators. Again, dynamic optimal control can be utilized to resolve a problem of practical importance in the context of networking.

The epidemiological evolution has natural analogues in the spread of a contagious disease in a human society, with the caveat that the inoculation and healing processes are (to the best of our knowledge) non-replicative. The cost is aggregation of infective and dead individuals and the overall human-hour of trained staff [27]. Application of the optimal control of epidemiological evolution in social context is, however, not restricted to the containment of contagious diseases.

Another noteworthy problem is dynamic management of advertising resources in adoption
of a new technology. We discuss two practical examples which we refer to as Reclamation and Rivalry cases, respectively. First, consider a simple scenario where (at least initially) most individuals in a society are subscribed to a specific technology through incumbent company A (e.g., Comcast for cable TV in Philadelphia) - they are the susceptibles. A new technology/company B (e.g., DTV) aims to capture the market. They win over some customers, who constitute the converts (infectives). Social exchanges (contacts) between infectives and susceptibles (converts and subscribers) may convert the latter. Company A seeks to regain the share of the market, by recapturing (healing) the infectives and re-confirming (immunizing) the susceptibles, say via offering lucrative long-term contracts (patches) - the resulting pledged subscribers constitute the recovered. New contracts are long-term and thus the recovered are immune to further change in subscription. The reclamation occurs through the efforts of advertising agents (disseminators) who communicate to the infectives and susceptibles through tele-marketing, e-marketing and/or word of mouth. The disseminators may either be from an initial pool (non-replicative dispatch), or may include the recovered nodes as well, e.g. by offering pledged subscribers additional service discounts through referral rewards, etc. (replicative dispatch). There is however no “death” in this setting. The overall ‘cost’ for company A is (i) increasing in the number of infectives, as they are the only lost subscribers to A, and is (ii) increasing in the number of active agents and the amount of discounts they offer in order to make the contracts appealing. Thus, optimal (dynamic) control of activating agents and selecting discount rates maximizes the net profit for company A, where profit equals the income generated through subscription minus the cost incurred in marketing/advertising over time.

For the second case (Rivalry), suppose that both competing companies enter the market for a new technology at around the same time. Now, susceptibles are those who are yet to choose either, infectives encompass those who have chosen B (the rival), and recovered are those who have chosen A. Both infectives and recovered may convert susceptibles (the undecided) to their respective groups whenever the respective pairs contact, e.g., through social communications -
the dispatch is therefore replicative. It is also possible that some infectives can not be healed as both companies may offer long-term contracts. The overall cost for company $A$ is similar, except that it is now decreasing (hence the revenue is increasing) in the number of recovered, as only recovered are subscribed to company $A$ in this case.

To capture all of these scenarios and to provide versatility, we provide a unified non-linear optimal control framework based on a deterministic epidemic model, which is a generalized version of the problems considered in §6.1. We consider both replicative and non-replicative dispatch scenarios and minimize a general aggregate costs by dynamically selecting the activation of the disseminators and their distribution rates. This generalized model also captures some attributes of the patching problem in the context of network security which we did not consider in Chapter 6. Specifically, the cost of patching is §6.1 was motivated based on the bandwidth overhead of patching, in which the product of the fraction of the activated dispatchers and the communication rate of each one affects the cost. Thus, only one optimal control function representing the product was sufficient to obtain optimal patching policies. Our generalized model in this section captures the energy overhead in distribution of patches as well. Then the cost of patching, and hence the system objective, cannot be characterized by the product of the fraction of activated patches and their rate of communication. Therefore, two separate optimal control functions are necessary to obtain optimal patching policies which need to be jointly optimized.

In both non-replicative and replicative settings, we analytically verify that the simple structural results introduced in §§6.2, 6.3 are preserved. Specifically, using the abstract notion of “patch” to refer to vaccinations, messages, promotion packages, security patches etc. depending on the context, we show that when the resource consumption cost is concave, until a certain time, all disseminators are activated and they distribute patches at the maximum possible rate, and subsequently no disseminator is activated until the end of the system operation period (§§8.3.1 and 8.4.1). Optimality of a bang-bang control (that is the property that it assumes only either its minimum or maximum possible values at any given time) and quantifying the maximum
possible number of jumps to be one are despite the facts that the network state evolutions do not constitute monotonic functions of time, involve non-linear dynamics, the cost functions are not assumed to be linear in the control or the states and the control (activation fraction, transmission rate) is a two-dimensional function. When the resource consumption cost is strictly convex, the optimal activation fraction function has the same structure. The optimal transmission rate function has similar behavior except that its potential transition from the maximum to minimum values is strict, but continuous rather than abrupt. The generality of the model allows for a unified theoretical framework for optimizing a sundry of problems of practical importance in diverse scenarios. Moreover, the simplicity of the structure of the optimal controls makes them amenable to implementation in practice.

### 8.2 System model

We first present the state evolution as a deterministic epidemic and formulate the cost minimization goal as an optimal control problem at an abstract level. Later, in §8.2.3, we motivate the model by instantiating each of these terms in the different settings discussed in the introduction (§8.1-A).

#### 8.2.1 Dynamics of non-replicative dispatch

A susceptible is infected whenever it is in contact with an infective. We assume homogeneous mixing, that is, an infective is equally likely to contact with any other entity and with the same inter-meeting delay distribution. Hence an infective meets with each susceptible at the same rate. At any given $t$, there are $n_S(t)n_I(t)$ infective-susceptible potential pairs. Susceptibles are therefore transformed to infectives at a rate proportional to $n_S(t)n_I(t)$.

The system manager controls the resources consumed in distribution of the patches by dynamically activating a fraction of the disseminators, as well as determining the patch distribu-
tion rates of the activated disseminators. Let the fraction of activated disseminators at time $t$ be $\varepsilon(t)$, and each transmits a patch at rate $u(t)$. The disseminators distribute their patches to infectives and susceptibles upon contact, which has similar connotations as for the spread of infection. The patches immunize the susceptibles, and thus susceptibles recover at a rate proportional to $\varepsilon(t)R_0n_S(t)u(t)$ at each $t$. Clearly,

$$0 \leq \varepsilon(t) \leq 1, \quad 0 \leq u(t) \leq 1 \quad \text{at each } t.$$ (8.2.1)

The last upper bound follows by normalization. The efficacy of the patch may be lower for infectives than for susceptibles. We capture the above possibility by introducing a coefficient $0 \leq \pi \leq 1$: $\pi = 0$ occurs when the patch is completely unable to heal the infectives and only immunizes the susceptibles, whereas $\pi = 1$ represents the other extreme scenario where a patch can equally well immunize and heal susceptibles and infectives. If the patch heals an infective, its state changes to recovered, otherwise, it continues to remain an infective. Thus, the infectives recover at a rate proportional to $\pi R_0\varepsilon(t)u(t)n_I(t)$ at each $t$.

Each infective dies at rate $\delta$, where $\delta \geq 0$, and the overall death rate is $\delta n_I(t)$ at each $t$. Note that $\delta = 0$ corresponds to systems without death. If the total number of entities $(N)$ is large (barring some technicalities), then $S(t)$, $I(t)$ and $D(t)$ converge to the solution of the following system of differential equations:

$$\dot{S}(t) = -\beta_0 I(t)S(t) - \beta_1 R_0\varepsilon(t)u(t)S(t)$$ (8.2.2a) 
$$\dot{I}(t) = \beta_0 I(t)S(t) - \pi \beta_1 R_0\varepsilon(t)u(t)I(t) - \delta I(t)$$ (8.2.2b) 
$$\dot{D}(t) = \delta I(t)$$ (8.2.2c)

with initial constraints:

$$I(0) = \lim_{N \to \infty} n_I(0)/N = I_0, \quad 0 < S(0) < 1 - I_0, \quad D(0) = 0,$$ (8.2.3)

and which also satisfy the following constraints at all $t$:

$$0 \leq S(t), I(t), D(t) \quad \text{and} \quad S(t) + I(t) + D(t) \leq 1.$$ (8.2.4)
Figure 8.19: State transitions for non-replicative case. The only difference in the replicative case is that transition rates from $S$ to $R$ is at rate $\beta_1 \varepsilon u RS$ and from $I$ to $R$ at rate $\pi \beta_1 \varepsilon u RI$ instead.

Thus, $(S(\cdot), I(\cdot), D(\cdot))$ constitutes the system state function and $(\varepsilon(\cdot), u(\cdot))$ constitutes the (2-dimensional) control function. For the case of $I_0 = 0$, the infectives stay at zero, thus WLOG, we assume $\beta_0 = \pi = \delta = 0$. If $I_0 > 0$, we assume $\beta_0 > 0$. Henceforth, wherever not ambiguous, we drop the dependence on $t$ and make it implicit. Fig.8.19 illustrates the transitions between different states of nodes and the notations used.

### 8.2.2 Dynamics of replicative dispatch

In the replicative model, all recovered nodes become disseminators, and hence the fraction of disseminators grows to $R(t)$ at time $t$, whereas in the non-replicative model, the fraction of disseminators continue to be $R_0$ at all times. The dynamics in (8.2.2) hence needs to be modified. First, since $S(t) + I(t) + R(t) + D(t) = 1$ at any given time, we can represent the system using any three of the above states. In the non-replicative case we chose $(S(t), I(t), D(t))$, whereas in the replicative case we adopt $(S(t), I(t), R(t))$ instead. The specific choices make the analyses more convenient in each case.

\[
\begin{align*}
\dot{S}(t) &= -\beta_0 I(t)S(t) - \beta_1 \varepsilon(t) u(t) R(t) S(t) \quad (8.2.5a) \\
\dot{I}(t) &= \beta_0 I(t)S(t) - \pi \beta_1 \varepsilon(t) u(t) R(t) I(t) - \delta I(t) \quad (8.2.5b) \\
\dot{R}(t) &= \beta_1 \varepsilon(t) u(t) R(t) S(t) + \pi \beta_1 \varepsilon(t) u(t) R(t) I(t) \quad (8.2.5c)
\end{align*}
\]
with initial constraints: \( I(0) = I_0, R(0) = R_0, S(0) = 1 - I_0 - R_0 \), and as before, \( 0 \leq I_0 \leq 1, 0 < R_0 < 1, I_0 + R_0 < 1 \). Also similarly, \( 0 \leq S(t), I(t), R(t) \) and \( S(t) + I(t) + R(t) \leq 1 \). If \( \delta = 0 \), the latter holds as an equality.

The following lemma, which we prove next, shows that the state constraints in both non-replicative and replicative models hold for any control-pair that satisfies (8.2.1), thus these constraints can be ignored henceforth, i.e., we can deal with optimal control problems with no state constraints.

**Lemma 8.2.1.** (A) In non-replicative case, for any control function pair \((\varepsilon(\cdot), u(\cdot))\) that satisfies (8.2.1), \(((S(t), I(t), D(t)))\), satisfies the state constraints for the non-replicative case in the \([0, T]\) interval, i.e.,

\[
0 \leq S(t), I(t), D(t) \text{ and } S(t) + I(t) + D(t) \leq 1. \text{ Moreover, (i) } S(t) > 0 \text{ for all } t \in [0, T], \text{ (ii) if } I_0 > 0, I(t) > 0 \text{ for all } t \in [0, T], \text{ and (iii) if } \delta > 0, D(t) > 0 \text{ for all } t \in [0, T].
\]

(B) Similarly, in the replicative case, for any control function pair \((\varepsilon(\cdot), u(\cdot))\) that satisfies (8.2.1), \(((S(t), I(t), R(t)))\), satisfies the state constraints for this case, i.e., \(0 \leq S(t), I(t), R(t)\) and \(S(t) + I(t) + R(t) \leq 1\) in the \([0, T]\) interval. Moreover, (i) \(R(t), S(t) > 0 \text{ for all } t \in [0, T]\), (ii) if \(I_0 > 0\), \(I(t) > 0 \text{ for all } t \in [0, T]\), and (iii) if \(\delta = 0\), \(S(t) + I(t) + R(t) = 1\).

**proof** We provide the proof for the non-replicative case. The proof for the replicative case follows almost identically.

We first consider the case of \(I_0 > 0\). The case of \(I_0 = 0\) is discussed in the end. Also for now, assume \(\delta > 0\). Since \(0 < I_0 + R_0 < 1, I_0, R_0 > 0\) the initial conditions in (8.2.3) ensure that all constraints (8.2.4) are strictly met at \(t = 0\), except that \(D(0) = 0\). The lemma follows if we show that all constraints in (8.2.4) are strictly satisfied in \((0, T]\). All \(S(\cdot), I(\cdot)\) and \(D(\cdot)\), resulting from (8.2.2) are continuous functions of time. Thus, since \(S(0), I(0) > 0\) and \(S(0) + I(0) + D(0) = 1 - R_0 < 1\), there exists an interval \((0, t_0)\) of nonzero length on which both \(S(t)\) and \(I(t)\) are strictly positive and \(S(t) + I(t) + D(t) < 1\). Hence, from (8.2.2) and (8.2.3), \(\dot{D}(t) > 0\) in \([0, t_0]\). Thus, from (8.2.3), \(D(t) > 0\) in \((0, t_0)\). Therefore, (8.2.4) is strictly satisfied in \([0, t_0]\).
Now, suppose that the constraints in (8.2.4) are not strictly satisfied in $(0, T]$. Then, there exists a time $t_1$ which is the first time after $t = 0$ at which, at least one of the constraints in (8.2.4) becomes active. That is, we have (i) $S(t_1) = 0$ OR (ii) $I(t_1) = 0$ OR (iii) $D(t_1) = 0$ OR (iv) $S(t_1) + I(t_1) + D(t_1) = 1$ AND throughout $(0, t_1)$, we have $0 < S(t), I(t), D(t)$ and $S(t) + I(t) + D(t) < 1$.

Thus, for $0 \leq t < t_1$ from (8.2.1), (8.2.2), (8.2.3) and since $R_0 < 1$, we have $\dot{S}(t) \geq -(\beta_0 + \beta_1)S(t)$. Hence, $S(t) \geq S(0)e^{-(\beta_0 + \beta_1)t}$ for all $0 \leq t < t_1$. Since $S(.)$ is continuous, $S(t_1) \geq S(0)e^{-(\beta_0 + \beta_1)t_0}$.

Similarly, we can show that $I(t_1) \geq I(0)e^{-(\beta_1 + \delta)t_0}$. Thus, since $S(0) > 0$, $I(0) > 0$, (i) and (ii) are ruled out. Next, from (8.2.2), $\dot{D}(t) > 0$ in $(0, t_1)$. Thus, from the continuity of $D(.)$ and since $D(t) > 0$ in $(0, t_1)$, (iii) is ruled out. Again, $\frac{d}{dt}(S(t) + I(t) + D(t)) \leq 0$ in $(0, t_1)$. Thus, from the continuity of $S(.)$, $I(.)$, $D(.)$ and since $S(t) + I(t) + D(t) < 1$ in $(0, t_1)$, (iv) is ruled out as well. This negates the existence of $t_1$. Thus, by contradiction, the constraints in (8.2.4) are strictly satisfied in $(0, T]$.

If, on the other hand, $\delta = 0$, from (8.2.2) and (8.2.3), $D(t) = 0$ for all $t \in [0, T]$. Using similar arguments we can show that $S(t), I(t) > 0$ and $S(t) + I(t) < 1$ for all $t \in [0, T]$. The lemma follows.

Now consider the case of $I_0 = 0$. In this case, we have $I(t) = D(t) = 0$ for all $t \in [0, T]$. $0 < S_0 < 1$, thus the constraint $S > 0$ and $S + I + R < 1$ are strictly met at $t = 0$. Since $S$ is continuous in time, there exists an interval $(0, t_0)$ of nonzero length on which $S(t)$ is strictly positive and $S(t) + I(t) + D(t) = S(t) < 1$. Now, suppose there exists a time $t_1$ which is the first time after $t = 0$ at which $S(t) = 0$ OR $S(t) = 1$ AND throughout $(0, t_1)$, we have $0 < S(t) < 1$.

Thus, for $0 \leq t < t_1$ from (8.2.1), (8.2.2), (8.2.3) and since $R_0 < 1$, we have $\dot{S}(t) \geq -\beta_1S(t)$, which implies $S(t) \geq S(0)e^{-\beta_1 t}$ for all $0 \leq t < t_1$. Since $S(.)$ is continuous, $S(t_1) \geq S(0)e^{-\beta_1 t_0} > 0$.

Also, $\dot{S}(t) < 0$ in $(0, t_1)$, thus, from the continuity of $S(t)$ and since $S(t) < 1$ in $(0, t_1), S(t_1) < 1$. Therefore, $t_1$ could not exist. Thus, by contradiction, $0 < S(t) < 1$ in $(0, T]$. \qed
8.2.3 Motivation of the models and instantiation

In the introduction section (§8.1), we described the motivations for the models presented in previous section through different examples from which interpretation of each of the corresponding states is straightforward. Here, and we add more comments on the nature of interactions in each example. First thing to point out is that, except for the case of infectious disease, both the replicative and non-replicative scenarios are conceivable.

Delay Tolerant Networks (DTNs): Contact occurs when two nodes roam into communication range of each other. There is no infective or dead nodes. This can be modeled by setting $I_0 = D_0 = \pi = \beta_0 = \delta = 0$ in our system dynamics equations.

Marketing-Reclamation/Rivalry: There is no dead state in these cases, which correspond to $\delta = 0$. Here, contacts constitute social interactions such as meetings, phone communications or email exchanges. The non-replicative case arises when only agents of the incumbent/rival attempt to persuade the customers, while in the replicative mode, each convert/subscriber advertises for the service through word of mouth as is incentivised by referral-based rewards/discounts. $\pi = 0$ represents the case in which customers are also pledged to the competitor and cannot be claimed by the incumbent/rival. Intermediate values of $\pi$ corresponds to different resistance (inertia) of customers to switch.

8.2.4 The objective function

We seek to minimize the overall cost in a time window $[0, T]$, where $T$ is a parameter of choice. At any given time $t$, the system incurs costs at the rates of $f(I(t))$, $g(D(t))$ and benefit at the rate of $L(R(t))$ where $f(\cdot), g(\cdot), L(\cdot)$ are non-decreasing and differentiable functions such that (WLoG) $f(0) = g(0) = L(0) = 0$. We assume $f'(x) > 0$ for all $x \geq 0$. In addition, each activated disseminator charges, or consumes resources at the rate $h(u(t))$ at time $t$ since it uses a distribution rate of $u(t)$, and $\varepsilon(t)R_0$ fraction of the nodes are the activated disseminators at time $t$. Here, $h(x)$ is a
twice-differentiable and increasing function in $x$ such that $h(0) = 0$ and $h(x) > 0$ when $x > 0$. Note that the assumptions on $f(\cdot), g(\cdot), h(\cdot)$ are mild and natural, and a large class of functions satisfy them. The aggregate system cost therefore is

$$J = \int_0^T f(I(t)) + g(D(t)) - L(R(t)) + \varepsilon(t)R_0 h(u(t)) \, dt$$

$$+ \kappa_I I(T) + \kappa_D D(T) - \kappa_R R(T). \quad (8.2.6)$$

Replacing $R_0$ with $R(t)$ in (8.2.6) gives the overall cost for the replicative case, as here, activated disseminators at time $t$ constitute $\varepsilon(t)R(t)$ (instead of $\varepsilon(t)R_0$) fraction of the total nodes. For both cases, at least one of the function $f$, $g$ or $L$ is not the null function, and $h$ is either a concave, linear or a convex function of $u$.

**Problem Statement:** The system seeks to minimize the aggregate cost in (8.2.6) by appropriately regulating $\varepsilon(\cdot), u(\cdot)$ at all $t$ subject to (8.2.1), when the states evolve (A) as per (8.2.2) for non-replicative, and (B) as per (8.2.5) for replicative dispatch, and satisfy the respective initial state conditions.

Note that we use open loop policies, which are control policies that they directly depend on time, as opposed to the states of the system (closed-loop policies). However, since we have mean-field convergence (for large enough $N$), the system is deterministic and open loop policies perform as well as closed-loop policies.

Here we briefly motivate the cost model for each of our different settings. Our cost model in (8.2.6) (and its replicative counterpart) is general enough to capture all of the cases.

**Network Security:** As we mentioned before, this unified model can generalize our optimal patching problem, discussed in Chapter 6, to cases in which the dominant cost of patching is its energy overhead. In what follows we describe this generalization. Each activated disseminator consumes power and/or bandwidth at rate $h(u(t))$ at time $t$ for transmission of patches. The total number of activated disseminators at time $t$ is respectively $N\varepsilon(t)R_0$ and $N\varepsilon(t)R(t)$ for non-replicative and replicative dispatch. Infective and dead (dysfunctional) nodes incur accumulative
costs to the network as well (represented by \( f \) and \( g \) functions respectively). Also \( \kappa_I \) and \( \kappa_D \) respectively represent the (scaled) cost per infective and dead node at the end of the network operation (i.e., time \( T \)). In this case, \( L(R) = 0 \) and \( \kappa_R = 0 \).

**Delay Tolerant Networks (DTNs):** Activation and transmission of disseminators consume power, which is especially critical in energy constrained DTNs. Here, there are no infective or dead nodes and hence, \( f = g \equiv 0 \) (also \( \kappa_I = \kappa_D = 0 \)). There is reward associated with increasing the total number of nodes which have received a copy of the disseminated message. Also, the sooner the message is disseminated, the better, hence the integration of \( L(R(t)) \) over time (note that the negative sign convert the minimization problem to a maximization one). \([69, \text{appendix-A}]\) directly relates the integral over time of the fraction of recovered nodes to the probability that a message is delivered to a sink before deadline \( T \). Hence the minimum delay problem is transferred to maximization of \( \int_0^T R(t) \, dt \), which corresponds to the special case of linear \( L(x) = -x \) in our setting (also ref. \([2, 3, 52]\)). If \( T \), as in \([2, 3, 52, 69]\), represents the deadline before the disseminated message reaches a (set of) destination(s), then \( \kappa_R = 0 \). If however, the objective is broadcasting a message by time \( T \) to many nodes, then \( \kappa_R \) represents the scaled benefit per node which has received the message at time \( T \).

**Marketing-Reclamation:** The optimizer in this case is the incumbent who incurs a cost of \( J \). Here, \( g, L \equiv 0 \), as infectives are the only group of customers who are not subscribed to the incumbent. That is, the incumbent incurs a cost only through infectives, since their converting away results in reduction of revenue (cessation of their subscription fee) over time. This loss is captured by integration of \( f(I) \) over time. Among the individuals who are contacted, only those who are persuaded by the offers will switch back. The cost for advertisement, captured by integration of the term involving \( h(\cdot) \), is associated with the amount of discount offers and rewards provided to lure the customers back. The incumbent seeks to minimize its overall loss due to the entrance of the competitor, by dynamically determining the fraction of the individuals who should be selected for a special offer and how much discount should be provided, which in
turn determines the efficacy $u$ of the switch to the incumbent. Here, $\kappa_D = \kappa_R = \kappa_I = 0$.

**Marketing-Rivalry:** The optimization here, is from the viewpoint of one of the rivals. There is no dead state in this model, hence, similar to the reclamation case, $g \equiv 0$. However, $f \equiv 0$ instead of $L$, since only recovered are those customers who subscribe to the company of the optimizer (susceptibles are not subscribed to either). The revenue comes from the subscription fee of the recovered nodes, and is represented through integration of the $L(R)$ function over time. The cost for advertisement is similar to the Reclamation case. Here, $\kappa_I = \kappa_D = \kappa_R = 0$.

### 8.3 Optimal non-replicative dispatch

We apply Pontryagin’s Maximum Principle to obtain a framework for solving the optimal control problem as posed in Problem Statements (A) and (B). Let $((S, I, D), (\varepsilon, u))$ be an optimal solution to the problem posed in problem statement (A) in the previous section, consider the Hamiltonian $H$, and corresponding co-state or adjoint functions $\lambda_S(t)$, $\lambda_I(t)$ and $\lambda_D(t)$, defined as follows:

$$
H = f(I) + g(D) - L(R) + \varepsilon R_0 h(u) + (\lambda_I - \lambda_S)\beta_0 IS
- \beta_1 R_0 \varepsilon u \lambda_S - \pi \beta_1 R_0 \varepsilon u \lambda_I + (\lambda_D - \lambda_I)\delta I.
$$

(8.3.1)

where $R = 1 - S - I - D$.

$$
\dot{\lambda}_S = -\frac{\partial H}{\partial S} = -L'(R) - (\lambda_I - \lambda_S)\beta_0 I + \beta_1 R_0 \varepsilon u \lambda_S
$$

$$
\dot{\lambda}_I = -\frac{\partial H}{\partial I} = -L'(R) - f'(I) - (\lambda_I - \lambda_S)\beta_0 S + \pi \beta_1 R_0 \varepsilon u \lambda_I - (\lambda_D - \lambda_I)\delta
$$

$$
\dot{\lambda}_D = -\frac{\partial H}{\partial D} = -L'(R) - g'(D).
$$

(8.3.2)

along with the transversality conditions:

$$
\lambda_S(T) = \kappa_R, \quad \lambda_I(T) = \kappa_I + \kappa_R, \quad \lambda_D(T) = \kappa_D + \kappa_R.
$$

(8.3.3)

Then according to Pontryagin’s Maximum Principle (e.g., [24, P. 109, Theorem 3.14]), there exist continuous and piecewise continuously differentiable co-state functions $\lambda_S, \lambda_I$ and $\lambda_D$, that at
every point \( t \in [0 \ldots T] \) where \( \epsilon \) and \( u \) is continuous, satisfy (8.3.2) and (8.3.3). Also,

\[
(\epsilon, u) \in \arg \min_{\epsilon, u \text{ admissible}} H(\vec{X}, (S, I, D), (\epsilon, u)).
\] (8.3.4)

8.3.1 Structure of the optimal non-replicative dispatch

We establish that the two-dimensional optimal controls of patching in the non-replicative case have simple structures:

**Theorem 8.3.1.** In the problem statement (A), for either one of the following two cases: (i) \( L \equiv 0, \beta_0 > 0 \) and \( f(.) \) is convex, (ii) \( \delta = 0 \) and \( L \not\equiv 0 \), an optimal control \((\epsilon(\cdot), u(\cdot))\) has the following simple structure:

1. When \( h(\cdot) \) is concave, \( \exists t_1 \in [0 \ldots T] \) such that (a) \( u(t) = 1 \) for \( 0 < t < t_1 \), and (b) \( u(t) = 0 \) for \( t_1 < t < T \).

2. When \( h(\cdot) \) is strictly convex, \( \exists t_0, t_1, 0 \leq t_0 \leq t_1 \leq T \) such that (a) \( u(t) = 1 \) on \( 0 < t \leq t_0 \), (b) \( u(t) \) strictly and continually decreases on \( t_0 < t < t_1 \), and (c) \( u(t) = 0 \) on \( t_1 \leq t \leq T \).

In both cases, for all \( t \in (0, T) \), except possibly for \( t = t_1 \) when \( h(\cdot) \) is strictly concave, \( \epsilon(t) = 1 \) if and only if \( u(t) > 0 \), and \( \epsilon(t) = 0 \) otherwise.

The above results are somewhat surprising in that the activation fraction \( \epsilon(\cdot) \) is completely specified by \( u(\cdot) \), and hence the two-dimensional control is reduced to a one-dimensional solution. The practical implication is that the activation scheme is *all or none*, and it is not optimal to activate a portion of the dispatchers. When \( h(\cdot) \) is strictly concave, the optimum transmission range, and hence the entire solution, is bang-bang and has at most one jump from 1 down to 0, and it is optimal to patch as aggressively as possible early on (as soon as the infection is detected and the patch is produced) and halt the patching after a certain time. When \( h(\cdot) \) is strictly convex, \( \epsilon(\cdot) \) continues to be bang-bang and has at most one jump from 1 down to 0, but \( u(\cdot) \) has a strict but continuous descent to 0.
proof} Let function \( \varphi(t) \) be defined as follows:

\[
\varphi := \beta_1 (\lambda_S S + \pi \lambda_I I) \tag{8.3.5}
\]

\( \varphi(.) \) is thus a continuous function of time, which according to (8.3.3) has the following final value:

\[
\varphi(T) = \beta_1 (\kappa_R S(T) + \pi \kappa_R I(T) + \pi \kappa_I I(T)). \tag{8.3.6}
\]

Also, as we prove in §8.3.2:

**Lemma 8.3.2.** \( \varphi(t) \) is a strictly decreasing function of \( t \) for \( t \in [0, T) \).

We can rewrite the Hamiltonian in (8.3.1) as:

\[
H = f(I) + g(D) - L(R) + (\lambda_I - \lambda_S) \beta_0 IS + (\lambda_D - \lambda_I) \delta I + \varepsilon R_0 (h(u) - \varphi u). \tag{8.3.7}
\]

From (8.3.4), for each admissible control \((\varepsilon, u)\) and for all \( t \in [0, T] \),

\[
\varepsilon(t) (h(u(t)) - \varphi(t)u(t)) \leq \varepsilon(t) (h(u(t)) - \varphi(t)u(t))
\]

\[
\implies (\varepsilon(t), u(t)) \in \arg \min_{y \in [0,1]} x (h(y) - \varphi(t) y). \tag{8.3.8}
\]

Since \((\varepsilon, u) \equiv (0,0)\) is an admissible control, we have for all \( 0 \leq t \leq T \):

\[
\varepsilon(h(u) - \varphi u) \leq 0. \tag{8.3.9}
\]

Note that whenever either \( u \) or \( \varepsilon \) is zero, irrespective of the other, \( \varepsilon u = 0 \), and since \( h(0) = 0 \), \( \varepsilon h(0) = 0 \). Thus, the state dynamics and the instantaneous cost incurred do not depend on the value of the other control function at these epochs. Thus, whenever one control function assumes a zero value, we can, WLoG, choose zero value for the other.

Next, consider a \( t \) at which the minimizer of \( h(y) - \varphi y \) in \( y \in [0,1] \) is unique. If this unique minimizer is 0, then \( \varepsilon = u = 0 \) at \( t \). In order to show this, we only need to show that \( u = 0 \) at \( t \).

Otherwise, if at \( t, u > 0 \), then \( \varepsilon > 0 \) at \( t \), and \( h(u) - \varphi u > h(0) - \varphi 0 = 0 \). This contradicts (8.4.6).
If this unique minimizer is positive, then at $t$, $\min_{y \in [0,1]} (h(y) - \varphi y) < 0$, and thus from (8.3.8), $\varepsilon = 1$ and $u$ equals this unique minimizer. Thus, at any $t$ at which the minimizer of $h(y) - \varphi y$ in $y \in [0,1]$ is unique, $u$ equals this unique minimizer, and $\varepsilon = 1$ if and only if $u > 0$, and $\varepsilon = 0$ otherwise.

For establishing the structure of optimal $u$, we separately consider the cases of concave and strictly convex $h(.)$.

$h(.)$ concave

When $h(.)$ is concave (i.e., $h'' \leq 0$), at each time $t$, $h(x) - \varphi(t)x$ is a concave function of $x$, and thus, for any time $t$ such that $\varphi(t) \neq h(1)$, the unique minimum is either at $x = 0$ or $x = 1$. Then,

$$
\varepsilon(t)u(t) = \begin{cases} 
0, & \varphi(t) < h(1) \\
1, & \varphi(t) > h(1). 
\end{cases} \quad (8.3.10)
$$

Following lemma 8.3.2, there can be at most one $t$ at which $\varphi(t) = h(1)$ in $[0,T]$. Moreover, lemma 8.3.2 implies that if such $t$ exists, say $t_1$, then $\varphi(t) > h(1)$ for $t \in [0,t_1)$, and $\varphi(t) < h(1)$ for $t \in (t_1,T]$. The theorem follows from (8.3.10).

$h(.)$ strictly convex

Since $h(.)$ is strictly convex (i.e., $h'' > 0$), the minimizer of $h(y) - \varphi(t)y$ in $y \in [0,1]$ is unique irrespective of $t$. Thus, $\varepsilon(t) = 1$ if and only if $u(t) > 0$, and $\varepsilon(t) = 0$, otherwise. When $h(.)$ is strictly convex (i.e., $h'' > 0$), (8.3.8) implies that, if $\frac{\partial}{\partial x} (R_0 h(x) - \varphi(t)x)_{|x=y} = 0$ at a $y \in [0,1]$, then $u(t) = y$, else $u(t) \in \{0,1\}$. Then,

$$
u = \begin{cases} 
0, & \varphi \leq R_0h'(0) \\
h^{-1}(\frac{\varphi}{R_0}), & R_0h'(0) < \varphi \leq R_0h'(1) \\
1, & R_0h'(1) < \varphi. 
\end{cases} \quad (8.3.11)
$$
Thus, from continuity of $\varphi$ and $h'$, $u$ is continuous at all $t \in [0, T]$. Since $h(\cdot)$ is strictly convex, $h'(\cdot)$ is a strictly increasing function - hence, $h'(0) < h'(1)$. Thus, following lemma 8.3.2, there exist $t_0, t_1$, $0 \leq t_0 \leq t_1 \leq T$, such that $\varphi > R_0 h'(1)$ on $0 < t \leq t_0$, $R_0 h'(0) < \varphi \leq R_0 h'(1)$ on $t_0 < t < t_1$, and $\varphi \leq R_0 h'(0)$ on $t_1 \leq t \leq T$. The theorem follows from (8.3.11).

8.3.2 Proof of lemma 8.3.2

**proof** The state and co-state functions, and hence the $\varphi$ function, are continuous at each time $t \in [0, T)$ and differentiable at each time at which the $(\epsilon, u)$ function is continuous. Since $(\epsilon, u)$ is piecewise continuous, the lemma follows if we can show that $\dot{\varphi}$ is negative at each such $t$. Noting that $\beta_1 > 0$, at each such $t \in [0, T)$ we have:

$$
\frac{\dot{\varphi}}{\beta_1} = \frac{1}{\beta_1} \frac{d}{dt} \varphi = \lambda_S S + \lambda_S \dot{S} + \pi \lambda_I I + \pi \lambda_I \dot{I} \\
= -\lambda_I \beta_0 IS + \pi \lambda_S \beta_0 IS - \pi f'(I) I - \pi \lambda_D \delta I - L'(R)(S + \pi I) \\
= -(\lambda_I - \lambda_S) \pi \beta_0 IS - (1 - \pi) \lambda_I \beta_0 IS - \pi \lambda_D \delta I - \pi f'(I) I - L'(R)(S + \pi I) \quad (8.3.12)
$$

The right hand side is negative at each $t \in [0, T)$ since $I, S > 0$ at all $t \in [0, T]$ (lemma 8.2.1-A), $\beta_0 > 0$, $\delta \geq 0$, $0 \leq \pi \leq 1$ and $f'(x), L'(x) \geq 0$ for all $x$ (since $f(\cdot)$ and $L(\cdot)$ are non-decreasing functions), and because:

**Lemma 8.3.3.** For all $0 \leq t < T$, we have $\lambda_D \geq 0$, $\lambda_I > 0$, and $(\lambda_I - \lambda_S) > 0$.

This finishes the proof of the theorem, if we prove the above lemma, which we do next.

**Proof.** First, we note that $\lambda_D(T) = \kappa_D + \kappa_R \geq 0$ and at any $t \in [0, T]$ at which $(\epsilon, u)$ is continuous, $\dot{\lambda}_D(t) = -g'(D(t)) - L'(R(t)) \leq 0$. Thus, since $(\epsilon, u)$ is piecewise continuous, $\lambda_D(t) \geq 0$ for all $0 \leq t \leq T$. For proving the other two inequalities, we again use the following simple real analysis properties which we proved in §6.2.2 as properties 5 and 6 respectively.
Property 7. Let \( \psi(t) \) be a continuous and piecewise differentiable function of \( t \). Let \( \psi(t_1) = L \) and \( \psi(t) > L \) for all \( t \in (t_1, t_0] \). Then\(^{14} \) \( \psi(t^+) \geq 0 \).

Property 8. For any convex and differentiable function, \( \nu(x) \), which is 0 at \( x = 0 \), \( \nu'(x)x - \nu(x) \geq 0 \) for all \( x \geq 0 \).

In the rest of the proof for simplicity, we consider the case in which \( \kappa_I = \kappa_D = \kappa_R = 0 \).

We proceed in the following two steps:

**Step-1.** \( \lambda_I(T) = 0 \) and \( (\lambda_I(T) - \lambda_S(T)) = 0 \). \( \dot{\lambda}_I(T) = (\dot{\lambda}_I(T) - \dot{\lambda}_S(T)) = -L'(R(T)) - f'(I(T)) < 0 \).

Therefore, \( \lambda_I(t) \) and \( (\lambda_I(t) - \lambda_S(t)) \) are positive in an open interval of nonzero length ending at \( T \).

**Step-2.** Proof by contradiction. Let \( t^* \geq 0 \) be the last time before \( T \) at which (at least) one of the other two inequality constraints is active, i.e.,

\[
\lambda_I(t) > 0, \quad (\lambda_I(t) - \lambda_S(t)) > 0 \quad \text{for} \quad t^* < t < T,
\]

and \( \lambda_I(t^*) = 0 \) OR \( \lambda_I(t^*) - \lambda_S(t^*) = 0 \)

First, suppose that \( \lambda_I(t^*) = 0 \) and thus \( (\lambda_I(t^*) - \lambda_S(t^*)) \geq 0 \). Now,

\[
\lim_{t \downarrow t^*} \dot{\lambda}_I(t) = -L'(R) - f'(I) - (\lambda_I - \lambda_S)\beta_0S - \beta_D\delta \quad \text{[\( \cdot \)(8.3.2)]} \tag{8.3.13}
\]

we thus observe that \( \lim_{t \downarrow t^*} \frac{d}{dt} \lambda_I(t) < 0 \). This contradicts Property 7 for function \( \lambda_I(t) \). Hence, \( \lambda_I(t^*) > 0 \). Now let \( \lambda_I(t^*) - \lambda_S(t^*) = 0 \). Then, from (8.3.2),

\[
\lim_{t \downarrow t^*} (\dot{\lambda}_I(t) - \dot{\lambda}_S(t)) = -f'(I) + \pi\beta_1R_0\varepsilon u\lambda_I - (\lambda_D - \lambda_I)\delta - \beta_1R_0\varepsilon u\lambda_S \quad \text{[\( \cdot \)(8.3.2)]} \tag{8.3.13}
\]

\[
= -f'(I) - (1 - \pi)\beta_1R_0\varepsilon u\lambda_I - (\lambda_D - \lambda_I)\delta \tag{8.3.14}
\]

For the case of \( \delta = 0 \), since we showed \( \lambda_I(t^*) > 0 \), the remaining terms are negative, which contradicts Property 7 for the function \( \lambda_I - \lambda_S \), and hence negates the existence of \( t^* \) and lemma\(^{14} \)For a general function \( \psi(x) \), the notations \( \psi(x^+_0) \) and \( \psi(x^-_0) \) are defined as \( \lim_{x \downarrow x_0} \psi(x) \) and \( \lim_{x \uparrow x_0} \psi(x) \), respectively.

173
follows. For the case of $\delta > 0$ we need a more elaborate argument, as follows. The system is autonomous, i.e., the Hamiltonian and the constraints on the control (8.2.1) do not have an explicit dependency on the independent variable $t$. Thus, [47, P.236]

$$H(S(t), I(t), D(t), (\varepsilon(t), u(t)), \lambda_S(t), \lambda_I(t), \lambda_D(t)) \equiv \text{constant} \quad (8.3.15)$$

Thus, from (8.3.3) and recalling that for the case of $\delta > 0$, we assumed $L(R) \equiv 0$, we have:

$$H = H(T) = f(I(T)) + g(D(T)) + \varepsilon(T)R_0h(u(T)).$$

Also, $\dot{D} = \delta I \geq 0$, and $g(.)$ is a non-decreasing function, thus $g(D(T)) \geq g(D(t))$ for all $t \in [0 \ldots T]$. Hence:

$$H - g(D(t)) \geq f(I(T)) + R_0\varepsilon(T)h(u(T)) > 0. \quad (8.3.16)$$

The positivity follows since according to lemma 8.2.1-A and the assumptions on $f$, $h$: (i) $I(T) > 0$ and hence $f(I(T)) > 0$ and (ii) $R_0\varepsilon(T)h(u(T)) \geq 0$.

Therefore:

$$\lim_{t \downarrow t^*} \left( \dot{\lambda}_I(t) - \dot{\lambda}_S(t) \right) = -f'(I) + \pi\beta_1 R_0\varepsilon u\lambda_I - (\lambda_D - \lambda_I)\delta - \beta_1 R_0\varepsilon u\lambda_S$$

$$- \frac{H}{I} + \frac{f(I)}{I} + \frac{g(D)}{I} - \frac{L(R)}{I} + \frac{\varepsilon R_0}{I}(h(u) - \varphi u) + (\lambda_D - \lambda_I)\delta \quad [\because (8.3.7)]$$

$$= \frac{1}{I}[f(I) - f'(I)I] - \frac{H - g(D)}{I} - (1 - \pi)\beta_1 R_0\varepsilon u\lambda_I + \frac{\varepsilon R_0}{I}(h(u) - \varphi u) \quad (8.3.17)$$

From the supposition on $t^*$ and continuity of $\lambda_I(t)$, $\lambda_I(t^{*+}) \geq 0$. Recall that for the case of $\delta > 0$, we assumed $f$ to be a convex increasing function. Now, $f(I) - f'(I)I \leq 0$ following Property 8, since $f(x)$ is convex and $f(0) = 0$ and $I > 0$ at all $t$ by lemma 8.2.1-A. Thus, from lemma 8.2.1-A and (8.2.1), (8.4.6) and (8.3.16), and since $\pi \leq 1, \beta_1, R_0 > 0$, we observe that $\lim_{t \downarrow t^*} \frac{d}{dt}(\lambda_I - \lambda_S) < 0$. This again contradicts Property 7 for function $\lambda_I - \lambda_S$ and lemma follows.

This completes the proof of lemma 8.3.2.
8.4 Optimal replicative dispatch

Similar to the non-replicative case, we define the Hamiltonian as:

\[
H = f(I) + g(D) - L(R) + \varepsilon R h(u) + (\lambda_I - \lambda_S)\beta_0 IS - (\lambda_S - \lambda_R)\beta_1 \varepsilon u RS - (\lambda_I - \lambda_R)\pi \beta_1 \varepsilon u RI - \lambda_I \delta I. \tag{8.4.1}
\]

where \( D = 1 - (S + I + R) \). The system of co-state differential equations is as:

\[
\dot{\lambda}_S = -\frac{\partial H}{\partial S} = - (\lambda_I - \lambda_S)\beta_0 I + (\lambda_S - \lambda_R)\beta_1 \varepsilon u R + g'(D) \tag{8.4.2}
\]

\[
\dot{\lambda}_I = -\frac{\partial H}{\partial I} = -f'(I) - (\lambda_I - \lambda_S)\beta_0 S + (\lambda_I - \lambda_R)\pi \beta_1 \varepsilon u R + \lambda_I \delta + g'(D) \tag{8.4.2}
\]

\[
\dot{\lambda}_R = -\frac{\partial H}{\partial R} = (\lambda_S - \lambda_R)\beta_1 \varepsilon u S + (\lambda_I - \lambda_R)\pi \beta_1 \varepsilon u I - \varepsilon h(u) + g'(D) + L'(R). \tag{8.4.2}
\]

and the transversality conditions as:

\[
\lambda_S(T) = 0, \lambda_I(T) = \kappa_I, \lambda_R(T) = -\kappa_R. \tag{8.4.3}
\]

Then, according to Pontryagin’s Maximum Principle ([24, P. 109, theorem 3.14]), there exist continuous and piece-wise continuous functions \( \lambda_S(t) \) to \( \lambda_R(t) \) that satisfy (8.4.2) and (8.4.3) at any \( t \) at which \( (\varepsilon(t), u(t)) \) is continuous, and the optimal \( (\varepsilon, u) \) satisfies:

\[
(\varepsilon, u) \in \arg \min_{(\varepsilon,u) \text{ admissible}} H(\hat{\lambda}, (S, I, D), (\varepsilon, u)). \tag{8.4.4}
\]

The above framework can be used for numerically computing the optimum control and the minimum aggregate cost.

8.4.1 Structure of the optimal replicative dispatch

**Theorem 8.4.1.** Consider an optimal control \( (\varepsilon(.), u(.)) \) to the problem posed in problem statement B.

The same structural properties as in Theorem 8.3.1 (i.e., for the non-replicative case) also holds here.

In the rest of the subsection, we prove Theorem 8.4.1.
proof  Consider \( \varphi \) as defined in the following:

\[
\varphi := (\lambda_S - \lambda_R) \beta_1 RS + (\lambda_I - \lambda_R) \pi \beta_1 RI
\]

Now from (8.4.4) and referring to (8.4.1), for each admissible control \((\varepsilon, u)\), and for all \( t \in [0, T] \),

\[
\varepsilon(t) (R(t)h(u(t)) - \varphi(t)u(t)) \leq \varepsilon(t) (R(t)h(u(t)) - u(t)\varphi(t))
\]

\[
\implies (\varepsilon(t), u(t)) \in \operatorname{arg\, min}_{x \in [0, 1], y \in [0, 1]} x (R(t)h(y) - \varphi(t)y).
\]

(8.4.5)

Since \((\varepsilon, u) \equiv (0, 0)\) is an admissible control, we have for all \( 0 \leq t \leq T \):

\[
\varepsilon(Rh(u) - \varphi u) \leq 0.
\]

(8.4.6)

The optimality of the \( \varepsilon(t) \) as stated in Theorem 8.4.1 follows by similar argument following (8.3.9). We prove the structure of \( u \) separately for the cases of concave and strictly convex \( h(.) \), using the following lemma, which we prove in §8.4.2.

Lemma 8.4.2. Let \( \psi(t) = \frac{\varphi(t)}{R(t)} \). Then, \( \psi(t) \) is a strictly decreasing function of \( t \) for \( t \in [0, T) \).

\( h(.) \) concave

Since \( h(.) \) is concave (i.e., \( h'' < 0 \)) and \( R > 0 \) by lemma 8.2.1-B, no \( y \in (0, 1) \) attains

\[
\min_{y \in [0, 1]} (Rh(y) - \varphi y)
\]

unless \( \varphi = Rh(1) \). Thus, if at time \( t \), \( \varphi - Rh(1) < 0 \), then \( y = 0 \) is the unique minimizer of \( Rh(y) - \varphi y \) in \( y \in [0, 1] \). Thus, \( \varepsilon = u = 0 \) at any such time. If \( \varphi - Rh(1) > 0 \), \( y = 1 \) is this unique minimizer. Thus, \( \varepsilon = u = 1 \) at any such time. Thus:

\[
(\varepsilon, u) = \begin{cases} 
(0, 0) & \varphi - Rh(1) < 0 \\
(1, 1) & \varphi - Rh(1) > 0
\end{cases}
\]

(8.4.7)

Using lemma 8.4.2, we conclude that \( \varphi/R = h(1) \) at at most one time epoch in \((0, T)\), say \( t_1 \), and if such \( t_1 \) exists, \( \varphi/R > h(1) \) in \((0, t_1)\) and \( \varphi/R < h(1) \) in \((t_1, T)\). The theorem follows from (8.4.7).
Since $h(.)$ is strictly convex (i.e., $h'' > 0$), the minimizer of $R(t)h(y) - \varphi(t)y$ in $y \in [0,1]$ is unique irrespective of $t$. Thus, $\varepsilon(t) = 1$ if and only if $u(t) > 0$, and $\varepsilon(t) = 0$, otherwise. Thus, we only need to prove the requisite properties of $u$. This minimizer, and hence $u$, is:

$$
\begin{cases}
0, & \frac{\varphi}{R} \leq h'(0) \\
\lambda^{-1}(\frac{\varphi}{R}), & h'(0) < \frac{\varphi}{R} \leq h'(1) \\
1, & h'(1) < \frac{\varphi}{R}.
\end{cases}
$$

(8.4.8)

Now, since $\varphi, R, h'$ are continuous, $h'$ is strictly increasing, $R > 0$ at all $t \in [0, T]$, $u$ is continuous at all $t \in [0, T]$. $R(t) > 0$ at all $t \in [0, T]$ by lemma 8.2.1-B, and $h'(x) \geq 0$ for all $x$. During the interval on which $h'(0) < \frac{\varphi}{R} \leq h'(1)$, $\varepsilon = 1$ and hence $\dot{u}$ exists. The proof follows if we can show that $\dot{u} < 0$, when $h'(0) < \frac{\varphi}{R} \leq h'(R)$. Now, for $h'(0) < \frac{\varphi}{R} \leq h'(R)$, we have

$$
u = h'^{-1}(\frac{\varphi}{R}) \Rightarrow \dot{u} = \frac{\frac{d}{dt}(\frac{\varphi}{R})}{h''(u)}$$

According to lemma 8.4.2, this is negative. 

\qed

### 8.4.2 Proof of lemma 8.4.2

**Proof** We prove this lemma using lemma 8.4.3 which we state and prove next.

**Lemma 8.4.3.** For all $0 \leq t < T$, we have $(\lambda_I - \lambda_S) > 0$, $(\lambda_S - \lambda_R) > 0$ and $\lambda_R \leq 0$.

**Proof.** First, from (8.4.2) and lemma 8.2.1-B, at each $t$ at which $(\varepsilon, u)$ is continuous,

$$
\dot{\lambda}_R(t) = \frac{\varepsilon(\varphi u - Rh(u))}{R} + g'(D(t)) + L'(R(t))
$$

(8.4.9)

Hence, from lemma 8.2.1-B, (8.4.6) and since $g(.)$ and $L(.)$ are non-decreasing functions, $\dot{\lambda}_R \geq 0$ for all $0 \leq t \leq T$. Thus, by piecewise continuity of $\varepsilon, u$ and the continuity of $h$, $\lambda_R(t) \leq 0$ for all $0 \leq t \leq T$. 

177
We prove the other two inequalities as follows:

**Step-1.** This step is identical to **Step-1** in the proof of lemma 8.3.3.

**Step-2.** Proof by contradiction. Let \( t^* \geq 0 \) be the last time before \( T \) at which (at least) one of the other two inequalities is violated, i.e.,

\[
(\lambda_I - \lambda_S)(t) > 0, \quad (\lambda_S - \lambda_R)(t) > 0, \text{ for } t^* < t < T,
\]

and \( (\lambda_I - \lambda_S)(t^*) = 0 \) or \( (\lambda_S - \lambda_R)(t^*) = 0 \).

First, suppose that \( \lambda_I(t^*) = \lambda_S(t^*) \). Now, similar to the derivation for (8.3.14), using (8.4.2) we obtain:

\[
\lim_{t \uparrow t^*} \left( \dot{\lambda}_I(t) - \dot{\lambda}_S(t) \right) = -f'(I) + (\lambda_I - \lambda_R)\pi \beta_1 \varepsilon u R + \delta \lambda_I - (\lambda_S - \lambda_R)\beta_1 \varepsilon u R
\]

\[
= -f'(I) - (\lambda_S - \lambda_R)\beta_1 \varepsilon u R (1 - \pi) + \delta \lambda_I
\]

For the case of \( \delta = 0 \), we have \(-f'(I) < 0\) as was the assumption on \( f \), and \(-\lambda_S - \lambda_R) \leq 0\) following the definition of \( t^* \). For the case of \( \delta > 0 \), noting that the corresponding assumptions are convex \( f(.) \) and \( L \equiv 0 \), we can write:

\[
\lim_{t \uparrow t^*} \left( \dot{\lambda}_I(t) - \dot{\lambda}_S(t) \right) = -f'(I) - (\lambda_S - \lambda_R)\beta_1 \varepsilon u R (1 - \pi) + \delta \lambda_I
\]

\[
= \frac{1}{I} \left[ f(I) - f'(I) I \right] + \frac{\varepsilon}{I} (Rh(u) - \varphi u) - \frac{H - g(D)}{I} - (\lambda_S - \lambda_R)(\beta_1 - \pi \beta_1) \varepsilon u R.
\]

We can show, (i) \([f(I) - f'(I) I] \leq 0\) using Property 8, and (ii) analogous to (8.3.16), \( H - g(D) > 0 \) at all \( t \). Also, from the definition of \( t^* \), \( (\lambda_S - \lambda_R)(t^+) \geq 0 \). Now, since \( \beta_1 > 0, \pi \leq 1, \) from lemma 8.2.1-B, and (8.4.6), \( \lim_{t \uparrow t^*} \left( \dot{\lambda}_I(t) - \dot{\lambda}_S(t) \right) < 0 \). This contradicts Property 7. Hence, \( (\lambda_I(t^*) - \lambda_S(t^*)) \leq 0 \).

Now, let \( \lambda_S(t^*) = \lambda_R(t^*) \). Thus, from (8.4.2), (8.4.9) and (8.3.5):

\[
\lim_{t \uparrow t^*} \left( \dot{\lambda}_S(t) - \dot{\lambda}_R(t) \right) = -(\lambda_I - \lambda_S)\beta_3 I - \varepsilon u \frac{Rh(u) - R}{R} - L'(R)
\]
From (8.4.6), lemma 8.2.1-B, and since \( \beta_0 > 0 \), and since we show that \( (\lambda_I(t^*) - \lambda_S(t^*)) > 0 \), \( \lim_{t \to t^*} (\hat{\lambda}_S(t) - \hat{\lambda}_R(t)) < 0 \). This contradicts Property 7, and thereby negates the existence of \( t^* \).

The lemma follows. \( \square \)

From continuity of \( \varphi, R \), we need to show that \( \dot{\psi} < 0 \) at any \( t \in [0, T) \) at which \( (\varepsilon, u) \) is continuous. Now, at such a \( t \),

\[
\dot{\varphi} = (\hat{\lambda}_S - \hat{\lambda}_R) \beta_1 RS + (\lambda_I - \lambda_R) \pi \beta_1 RI + (\lambda_S - \lambda_R) \beta_1 \dot{R} S + (\lambda_I - \lambda_R) \pi \beta_1 \dot{R} I
\]

\[
+ (\lambda_S - \lambda_R) \beta_1 RS + (\lambda_I - \lambda_R) \pi \beta_1 R \dot{I}
\]

\[
= -\pi \beta_1 \beta_0 R I S \lambda_R - \beta_1 \beta_0 R I S \lambda_I + \beta_1 \beta_0 R I S \lambda_R + \beta_1 \beta_0 R I S \lambda_S
\]

\[
- \pi \beta_1 f'(I) R I + \pi \beta_1 R I \delta \lambda_R - L'(R) R \beta_1 (S + \pi I) + \varepsilon R h(u) \beta_1 (S + \pi I)
\]

\[
\rightarrow \pm \beta_0 \beta_1 R I S \lambda_S \text{ and re-arrangement } \rightarrow
\]

\[
= -\beta_0 \beta_1 (1 - \pi) R I S (\lambda_S - \lambda_R) - \beta_0 \beta_1 R I S (\lambda_I - \lambda_S) - \pi \beta_1 f'(I) R I
\]

\[
+ \pi \beta_1 R I \delta \lambda_R - L'(R) R \beta_1 (S + \pi I) + \varepsilon R h(u) \beta_1 (S + \pi I)
\]

\[
= \{ \text{negative term} \} + \varepsilon R h(u) \beta_1 (S + \pi I).
\] (8.4.11)

The expressions denoted as \{negative term\} is negative at each \( t \in [0, T) \) owing to lemma 8.4.3 and since \( \beta_1 > 0 \), and either \( \beta_0 I(t) > 0 \) or \( L \neq 0, \delta \geq 0, 0 \leq \pi \leq 1 \) by assumption and \( S, I, R > 0 \) by lemma 8.2.1-B. At any such \( t \),

\[
\dot{\psi}(t) = \frac{d}{dt} \left( \frac{\varphi}{R} \right) = \frac{\dot{\varphi} - \frac{\varphi}{R} \dot{R}}{R}
\]

\[
= \frac{\{ \text{negative term} \} + \varepsilon R h(u) \beta_1 (S + \pi I) - \dot{R} \frac{\varphi}{R}}{R}
\]

\[
= \frac{\{ \text{negative term} \} + \varepsilon (R h(u) - \varphi) \beta_1 (S + \pi I)}{R}
\]

\[
\leq \frac{\text{negative term}}{R}
\] (8.4.13)

The last inequality follows from (8.4.6), lemma 8.2.1-B and since \( \beta_1 > 0, \pi \geq 0 \). The lemma follows since the right hand side is negative at each \( t \in [0, T) \). \( \square \)
Chapter 9

Summary and Future Research

Summary

In part I we considered a future malware which can dynamically change its parameters in response to the changes in the state of the network in order to maximize its overall damage. Assuming network defense parameters are fixed a priori, we constructed an optimal-control framework which models the effect of the decisions of the attackers on the state dynamics and their resulting trade-offs through a combination of epidemic models and damage functions.

Specifically, in Chapter 3, we considered a worm which can decide the transmission rate and media access rates of the infected nodes, while being cognizant of its effect on exposition and battery depletion. Next, using Pontryagin’s Maximum Principle and simple real analyses arguments, we showed that an attacker can inflict the maximum damage by using very simple decisions. In Chapter 4, we considered an alternative attack setting where the malware can kill the nodes independently rather than through battery depletion. We investigated the joint optimal control of killing rate and media access rates of the infectives and established that very simple decisions constitute the general class of optimal policies. These dynamic policies are robust to the inaccurate estimation of the network parameters and inflict higher damages than the best static
policies. The attackers are therefore likely to prefer dynamic choices, and hence countermeasures should be designed to adequately defend against them.

In part II we assumed the viewpoint of the defender of the network, and investigated two defense mechanisms assuming that the attack parameters do not vary with time. First, in Chapter 5, we proposed reduction of reception gains of susceptible nodes for containing malware outbreaks in mobile wireless networks. Using optimal control tools, we identified the optimum policy for dynamically controlling the reception gains so as to minimize the overall network costs. We analytically proved that the optimal policies have simple structures when the cost functions are concave and convex, and can therefore be easily implemented in resource constrained devices without requiring constant coordination and information exchange.

Next, in Chapter 6, we considered the problem of disseminating security patches in a bandwidth constrained mobile wireless network. Specifically, we considered dynamically activating a controlled fraction of the dispatchers and selecting their transmission rates as an optimal dynamic control problem. We proved that the optimal policies for both non-replicative and replicative settings follow simple structures, making them suitable for distributed implementations. We numerically showed that they are robust against imprecisions in initial parameter estimations and time coordination, and consistently outperform static policies by a significant margin.

In part III, we considered the case in which both the attack and defense can be varied over time. We investigated strategic confrontations of the malware and the network through dynamic choices of reception and patching rates (network’s actions) and annihilation rate of the infectives (malware’s action). Using a dynamic game formulation, we proved that the robust defense strategies have simple structures conducive to implementation in resource constrained wireless devices. Our performance evaluations based on simulations and numerical computations revealed that the performance (minimizing the overall damage) is robust to clock drifts at nodes and is significantly better than when the reception and patching rates are fixed (i.e., are not allowed to vary with time).
Finally, in part IV, we demonstrated that the framework we developed applies to contexts beyond network security. We provided a unified optimal control framework based on a nonlinear deterministic epidemic model and generalized costs and established that our structural results still hold. We instantiated the generalized model in the context of health-care, marketing and message delivery in a DTN.

**Future research direction**

The deterministic epidemic models considered in our models are guaranteed to accurately model the spread of the malware only when the network has a large number of nodes and the nodes mix homogeneously. Most current wireless networks have a large number of nodes. Homogeneous mixing does not however hold in some networks: a node may only be in contact with a proper subset of nodes, e.g., when the nodes are moving slowly or moving in clusters. The locality of infection may play a significant role in such networks since the infection can spread based on the contact list of the infectives. Designing maximum damage dynamic attacks when either of these assumptions is relaxed remains open.

We did not consider the effect of elevated interference as a result of higher media access attempts of the infective nodes. In a highly dense network, a malware might want to avoid jamming during its spreading period, in order not to self-throttle its propagation, and then initiate a more effective jamming attack.

Also we considered attacks with only one kind of malware and also that patching renders a node immune. Karyotis et al. [38] have analyzed attacks where different kinds of malwares are seeking to simultaneously infect the nodes, and the patching against one kind of malware does not provide immunity against others - nodes may therefore return to susceptible states after recovery. They have however considered only static choice of malwares’ parameters and only two networks states: susceptible and infective. Generalization of our proposed attack frameworks so
as to characterize the maximum damage attacks under dynamic optimal control of the malwares’ parameters in presence of multiple malwares and multiple network states (susceptible, infected, recovered, dead) constitutes another interesting direction for future theoretical research.

We have obtained the optimal control strategies when nodes are oblivious to their neighbors’ states. It may however be possible for a node to obtain potentially inaccurate estimates of the aggregate infection and recovery levels in its neighborhood by for example monitoring the media scanning activities, etc. Derivation of the control strategy that optimally utilizes local (noisy) observations which randomly evolve with time remains open for both attack and defense settings.

Similarly, our analysis of the dynamic game was directed towards capturing scenarios where neither the attack nor the defense has access to exact network state information, and the spread is homogeneous; design of (strategically) robust closed-loop defenses when node localities play significant role in the spread of malware and in presence of stochastic state information constitute directions for future research. On another note, one could make the dynamic game more accurate by including the initial delay which it takes for the network to detect the presence of the malware and develop the appropriate patches. The problem can still be modeled as a dynamic zero-sum game, however, the starting time of the malware would be earlier than that of the network.

In terms of applications, an interesting open problem is to investigate whether our proposed optimal control framework can be generalized to develop optimal policies for disseminating large files in a p2p network. A more general state evolution framework may be necessary for this purpose. Specifically, in file sharing in a peer-to-peer system, files are disseminated in parts (segments) and different nodes may possess different parts of the file. Also in a peer-to-peer system, a peer may easily learn through information exchange how many of its peers have a certain part of the file. A similar model can then be applied to optimally allocate a large computation task in a computing cloud of CPUs. Thus, designing optimal control of epidemic evolutions that allow for sharing in parts and also that allow the exploitation of potentially inaccurate local information constitutes an interesting direction of future research.
Appendix A

Model Verification

Deterministic epidemic models have been validated for mobile wireless networks through experiments as well as network simulations (see e.g. [16,74]). The convergence to such system of ODE can in fact be mathematically established if some technical assumptions are made. One of these assumptions is the homogeneous mixing, which we discussed in Chapter 2. The homogeneous mixing refers to the property that the rate of contacts for each pair of nodes in the network is the same. If further, the inter-contact times are exponentially distributed, and the events such as healing and death etc. occur after exponential random times, then the evolution of the fraction of the nodes of the same type in the system is governed by a continuous time Markov chain (CTMC). For a DTN setting where the speed of nodes is sufficiently high, the inter-contact times between each pair of nodes have been established by Groenevelt et al. in [30] for a number of mobility models such as the random waypoint and random direction model [8]. The rate of this exponential distribution is equal to \( \frac{2wE[V^*]}{\lambda} u \), where \( w \) is a constant factor pertaining to the specific mobility model, \( E[V^*] \) is the average relative speed between two nodes, and \( u \) is the communication range of the pair, which itself is proportional to the product of the transmission gain of the antenna of the transmitter and the reception gain of the antenna of the receiver.

Approximation of CTMC processes with large number of interacting entities by solutions to
deterministic differential equations, sometimes referred to as the fluid or the mean-field approximation, is well established in the literature of various contexts. Kurtz [50] provided sufficient conditions for path-wise convergence (in probability) of the fractions to the solutions of the ODEs over compact time intervals. Darling and Norris [20] generalized the conditions in [50] such as the uniform convergence of the mean drifts of the Markov chains and the Lipschitz continuity of the limiting functions. Gast et al [29] establish the convergence of Markov decision processes, composed of a large number of objects, to optimization problems on ordinary differential equations. Specifically, they show that optimizing the limiting deterministic problem yields asymptotically optimal policies in the original stochastic problem.

In what follows, we use the results in [50] to establish the mean-field convergence under the additional assumptions expressed above. We consider the non-replicative patching model in Chapter 6 as a representative example. Specifically, we prove that the fractions of the susceptible, infective and dead nodes in the model presented in §6.1.1 converge (as the total number of node in the network \(N\) grows large) to the solution of the following system of ODE:

\[
\begin{align*}
\dot{S}(t) &= -\beta_0 I(t)S(t) - \beta_1 \theta(t)R_0 S(t) \\
\dot{I}(t) &= \beta_0 I(t)S(t) - \pi \beta_1 \theta(t)R_0 I(t) - \delta I(t) \\
\dot{D}(t) &= \delta I(t)
\end{align*}
\]

(A.0.1)

with initial constraints:

\[
I(0) = I_0, \quad S(0) = 1 - I_0 - R_0, \quad D(0) = 0
\]

Under the exponentially distributed inter-event times, the state vector \((n_S(t), n_I(t), n_D(t))\) evolves according to a pure jump Markov chain (since for all \(t\), \(n_S(t) + n_I(t) + n_R(t) + n_D(t) = N\), the state of the Markov chain is in fact three dimensional). Let the transition rates between states \(\sigma_1(t)\) and \(\sigma_2(t)\) be denoted by \(\rho(\sigma_1(t), \sigma_2(t))\). We have:

\[
\rho((n_S(t), n_I(t), n_D(t)), (n_S(t) - 1, n_I(t) + 1, n_D(t))) = \beta n_S(t) n_I(t),
\]

185
\[
\begin{align*}
\rho((n_S(t), n_I(t), n_D(t)), (n_S(t), n_I(t) - 1, n_D(t) + 1)) &= \delta n_I(t), \\
\rho((n_S(t), n_I(t), n_D(t)), (n_S(t), n_I(t) - 1, n_D(t))) &= \pi \beta \vartheta(t)(NR_0)n_I(t), \\
\rho((n_S(t), n_I(t), n_D(t)), (n_S(t) - 1, n_I(t), n_D(t))) &= \hat{\beta} \vartheta(t)(NR_0)n_S(t).
\end{align*}
\]

The convergence results in [50] hold as long as the transitions rates of the Markov chain constitute Lipschitz continuous functions of the state (theorems 2.11, 3.1 in [50]). This holds in our model, provided \( \vartheta \) is a Lipschitz continuous function of the state. We however consider \( \vartheta \) to be a function of time, rather than that of the state, since, as we mentioned in Chapter 2, nodes may not know the system states. Nevertheless, the convergence results extend in our case provided \( \vartheta \) is a Lipschitz continuous function of the state. We however consider \( \vartheta \) to be a function of time, rather than that of the state, since, as we mentioned in Chapter 2, nodes may not know the system states. Nevertheless, the convergence results extend in our case provided \( \vartheta(t) \) is a piecewise Lipschitz continuous function of time, i.e., there exist an integer \( K \) and time epochs \( t_0, t_1, \ldots, t_{K-1} \) such that \( \vartheta(\cdot) \) is Lipschitz continuous in \((0, t_0), (t_0, t_1), \ldots, (t_{K-1}, T)\) and \( \vartheta(\cdot) \) may be discontinuous at \( t_0, t_1, \ldots, t_{K-1} \). This represents a broad class of control functions. Also, Theorem 6.2.1 in Chapter 6 implies that the optimal \( \vartheta(\cdot) \) belongs in this class provided \( h''(x) \) is upper bounded for \( x \in [0, 1] \) and \( f'(x), g'(x) \) are bounded for \( x \in (0, 1] \).\footnote{When \( h(\cdot) \) is concave, it follows from Theorem 6.2.1 that the optimal \( \vartheta \) is piecewise constant, and therefore piecewise Lipschitz continuous. When \( h(\cdot) \) is strictly convex, piecewise Lipschitz continuity of the optimal \( \vartheta \) follows from Theorem 6.2.1 provided we can show it is Lipschitz continuous in the interim interval of \((t_0, t_1)\). Note that (6.2.10), along with (6.2.2) establish that the time-derivative of the optimal \( \vartheta(\cdot) \) is bounded in this interval since (i) \( \vartheta(\cdot) \) and therefore \( \lambda_1, \lambda_2 \) are bounded in this interval, (ii) \( g'(\cdot) \) and hence \( \lambda_3 \) is bounded throughout, and (iii) \( h''(\cdot), f'(\cdot) \) are bounded. The result follows.}

We prove this claim first considering \( \vartheta(\cdot) \) as a piecewise constant function of time in a time horizon \([0, T]\), i.e., \( \vartheta(\cdot) \) is constant in \((0, t_0), (t_0, t_1), \ldots, (t_{K-1}, T)\) and the constants corresponding to different intervals are different. Clearly, the transition rates constitute a Lipschitz continuous function of the state in each interval. Consider a system of differential equations which is the same as (A.0.1) except that its initial states at \( t_0, t_1, \ldots, t_{K-1} \) are adjusted to those obtained from the Markov chain. We refer to the states of this system at time \( t \) as \( (\tilde{S}^N(t), \tilde{I}^N(t), \tilde{D}^N(t)) \). Since

\[
\lim_{N \to \infty} n_I(0)/N = I_0 > 0, \quad \lim_{N \to \infty} n_S(0)/N = S_0 > 0, \quad \text{and} \quad \lim_{t \to \infty} N\hat{\beta} = \beta_0 \quad \text{and} \quad \lim_{N \to \infty} N\tilde{\beta} =
\]

186
\( \beta_1 \) exist, Theorem 2.11 (alternately a slight generalization of Theorem 3.1) of [50] implies that
\[ \forall \epsilon > 0, \forall t \in [0, T], \lim_{N \to \infty} \mathbb{P}\{ \sup_{\tau \leq t} \left| \frac{n_S(\tau)}{N} - \tilde{S}^N(\tau) \right| > \epsilon \} = 0, \]
where \( n_S(\tau) \) is the actual number of susceptibles in the network at time \( \tau \). Similar results hold for \( J(\cdot), D(\cdot) \). If for all \( \tau \in [0, T] \),
\[ |\frac{n_S(\tau)}{N} - \tilde{S}^N(\tau)| < \epsilon, \]
then \( |\tilde{S}^N(\tau) - S(\tau)| < \phi_1(\epsilon, K, T) \), where \( \lim_{\epsilon \to 0} \phi_1(\epsilon, K, T) = 0 \) for any given \( K, T \). Note that the difference between \( \tilde{S}^N(\tau), S(\tau) \) arises from the adjustment of the initial states at the jump points \( t_0, t_1, \ldots, t_{K-1} \) of \( \vartheta(\cdot) \) in the differential equations generating \( \tilde{S}^N(\tau) \), and the magnitude of such adjustments is lower if \( \frac{n_S(\tau)}{N}, \tilde{S}^N(\tau) \) are closer. Thus,
\[ \forall \epsilon > 0, t \in [0, T], \lim_{N \to \infty} \mathbb{P}\{ \sup_{\tau \leq t} | \frac{n_S(\tau)}{N} - S(\tau) | > \epsilon \} = 0. \]

We next allow \( \vartheta(\cdot) \) to be a piece-wise Lipschitz continuous function of time in interval \([0, T]\). Note that given any \( \epsilon > 0 \), there exists a piece-wise constant \( \vartheta^e(\cdot) \) function that approximates \( \vartheta(\cdot) \) such that the states obtained from (A.0.1) under \( \vartheta^e(\cdot) \) and \( \vartheta(\cdot) \) differ by at most \( \epsilon \) at any \( t \in [0, T] \). Such a function can be constructed by dividing \([0, T]\) in a given number of intervals and substituting \( \vartheta(\cdot) \) in each interval by its value at the beginning of the interval - piecewise Lipschitz continuity of \( \vartheta(\cdot) \) ensures that \( |\vartheta^e(t) - \vartheta(t)| \) approaches 0 at each \( t \in [0, T] \) as the number of intervals is increased. Now, applying the convergence results we just obtained for a control that is a piecewise constant function of time, it follows that given any \( \xi > 0 \), there exists a \( \epsilon(\xi) \) such that using \( \vartheta^{e(\xi)}(\cdot) \) in the stochastic system,
\[ \forall t \in [0, T], \lim_{N \to \infty} \mathbb{P}\{ \sup_{\tau \leq t} | \frac{n_S^\xi(\tau)}{N} - S(\tau) | > \xi \} = 0, \]
where \( n_S^\xi(\tau) \) is the actual number of susceptibles at time \( \tau \) in the stochastic system with control \( \vartheta^{e(\xi)}(\cdot) \) and \( S(\tau) \) as before corresponds to the solution of (A.0.1) with the given control \( \vartheta(\cdot) \).

Finally, if \( f(\cdot), g(\cdot) \) are uniformly continuous in \([0, T]\), the cost \( J \) characterized in (6.1.5) under controls \( \vartheta_1(\cdot) \) and \( \vartheta(\cdot) \) differ by at most \( \phi_2(\epsilon, T) \) if \( |\vartheta_1(t) - \vartheta_2(t)| < \epsilon \) for all \( t \in [0, T] \), where \( \lim_{\epsilon \to 0} \phi_2(\epsilon, T) = 0 \) for any \( T \geq 0 \).
Simulations

Here, we independently validate the epidemics models using simulations for a mobile wireless network under two different classes of contact processes: (i) exponential (ii) truncated power-law, for samples of attack, defense and game settings. The inter-contact times have truncated power-law distributions under the mobility pattern reported in [35] based on measurements on human mobility during INFOCOM 2005. Note that each pair is equally likely to contact in the exponential inter-contact time model. Power law distributions however arise from mobility patterns under which a pair of nodes that has been in contact in the recent past is more likely to be in contact at present as compared to a pair that has been in contact long ago: the mixing is not therefore homogeneous.

Attack We choose the battery depletion attack setting which we considered in Chapter 3. The attacker’s optimal control function $u(\cdot)$ is calculated using the optimal control framework proposed in §3.2, and with $T = 4$ hours, $\beta = 4.46, \rho = 0.8920, Q(u) = 0.1115, B(u) = 0.115\pi, \pi \in \{0,1\}, \kappa_I = 40, K_D = 50, \kappa_D = 0, K_I = 0$. We consider $Q(u), B(u)$ to be constants for simplicity. The value of $\beta = 4.46$ is selected to match the expected value of the inter-contact times, as reported in [35]. We focus on the two extreme values of $\pi : \pi \in \{0,1\}$. Note that if $\pi = 0$ security patches can only immunize the susceptibles, but if $\pi = 1$ they heal the infectives as well. Under the simulated contact processes, the damage is obtained by integrating $\kappa_I I(t)$ between 0 and $T$ and adding $K_D D(T)$ to the output of the integration, where $I(t), D(t)$ are the state processes observed in the simulations and $u(t)$ is the optimal control function calculated above.

We first describe the results for the exponential contact process with $N$ nodes. Note that homogeneous mixing holds for exponential contact processes, and we discussed, mean-field convergence results predict that as $N \to \infty$, the sample paths under exponential contact pro-

---

\footnote{We use a commercial software PROPT\textsuperscript{®} launched by Tomlab Optimization Inc, (http://tomopt.com/tomlab/ for MATLAB\textsuperscript{®}) for this purpose.}
cess will coincide with the solutions of the epidemiological differential equations (3.1.2). However, fig. A.1(a) reveals that even for a finite $N$ (e.g., $N = 500$) the simulated state fractions $(S(t), I(t), R(t), D(t))$, averaged over 100 runs, closely match the values predicted by the epidemic model. Also, fig. A.1(b) shows that the average damages obtained over 100 simulation runs closely match those predicted by the epidemic model for different values of $I_0$, and the standard deviation decreases with increase in $N$.

We next describe the results for the truncated power-law contact process (with parameter $\alpha = 0.4$ and truncated between 2 minutes and 24 hours) in a network with $N = 41$ reported in [35]. The epidemiological differential equations use $\beta = 4.46$ so that $1/\beta$ equals the expected value of the inter-contact times between any pair of nodes under the truncated power-law distribution. As fig. A.2 shows, the aggregate damage, averaged over 100 runs, follows similar trends as under the epidemic representations, despite the mixing not being homogeneous and $N$ being small.

**Defense** We run our simulations on the patching setting which we presented in Chapter 6. The optimal control function $\vartheta(t)$ is calculated using the optimal control framework proposed in §§6.2.1, 6.3.1, with $f(x) = K_Ix, g(x) = K_Dx, h(x) = K_u x$, and $T = 4 \text{ hours}$, $\beta_0 = \beta_1 = \beta = 0.103, \delta = 0.5, I_0 = 0.1, R_0 = 0.1, \pi \in \{0, 1\}, K_I = 10, K_D = 20, K_u = 10$. Now, we chose $K_I, K_D$ such that $K_D > K_I$, as otherwise the worm should not have any incentive to kill the nodes. Again, we consider the two extreme values of $\pi : \pi \in \{0, 1\}$. Under the simulated contact processes, the cost is obtained by integrating $K_I I(t) + K_D D(t) + K_u R_0 \vartheta(t)$ between 0 and $T$ in the non-replicative case ($K_I I(t) + K_D D(t) + K_u R(t) \vartheta(t)$ in the replicative case, resp.) where $I(t), D(t), R(t)$ are the state processes observed in the simulations and $\vartheta(t)$ is the optimal control function calculated above. The average cost and state evolutions over 100 runs are reported. Similar to the attack setting, our results largely reveal a close match in the state evolutions and costs predicted by the epidemiological differential equations ((6.1.2) and (6.1.7)) and those obtained from simulations of the node contacts under both replicative and non-replicative dispatch and
Figure A.1: The top two figures compare the simulated (averaged over 100 runs) and the calculated (from the epidemic model) state trajectories for a network of $N = 500$ nodes, and the bottom two figures compare the simulated and calculated damages for different values of $N$. The inter-contact times are exponentially distributed. In all the figures the dashed and the solid lines respectively represent the calculated values and the simulation results. The error-bars represent the standard deviations. The dashed and solid lines mostly overlap, and the deviations diminish as $N$ increases.
Figure A.2: Comparison of the simulated (averaged over 100 runs) damages and calculated (from the epidemic model) damages under power-law distributed inter-contact times for different value of $I_0$.

for both contact processes including when the mixing is not homogeneous.

Fig. A.3 reveals that the simulated state fractions $(S(t), I(t), R(t), D(t))$ under the exponential contact process closely match the corresponding values predicted by the epidemic model. Moreover, the comparisons reveal that even for a small (e.g., 41) number of nodes, the epidemic model yields a good approximation (at least in an expected sense). Moreover, fig. A.4 shows that the average costs obtained over 100 simulation runs closely match those predicted by the epidemic model for different values of $I_0$. Also, the error diminishes as the number of nodes increases to 400, both in terms of the matching of state trajectories (fig. A.5) and the aggregate costs (fig. A.6). Such close match is expected since homogeneous mixing holds for exponential contact processes.

We next describe the results for the truncated power-law contact process (again, with parameter $\alpha = 0.4$ and truncated between 2 minutes and 24 hours) in a network with 41 nodes as reported in [35]. As fig. A.7 and fig. A.8 show, the simulated and calculated state trajectories, and the simulated and calculated costs follow similar trends despite the mixing not being ho-
Figure A.3: Simulated and calculated trajectories of the states for a network of 41 nodes with exponential inter-contact times. The solid lines represent the trajectories obtained from the epidemic model (calculated trajectories), and the dashed lines are the averages of the trajectories over 100 simulation runs.

The values are also close, though, as expected, the match is not as good as for the exponential inter-contact process.

Game Here, we compare the overall damages predicted by the epidemic differential equations (7.1.1) and obtained through simulations in three different contexts. As for the attack and defense, we first consider a DTN with 41 nodes and exponential inter-contact times. Defense and attack strategies are saddle-point strategies calculated based on the estimated $\beta_0$ and $\beta_1$ for each $I_0$. We consider different initial fraction of the infectives, specifically $I_0 \in \{0.01, 0.02, 0.05, 0.10, 0.15, 0.20, 0.25\}$.

Fig. A.10(a) reveals that the average of the state fractions $(S(t), I(t), D(t))$ over 20 runs of the simulation closely match those predicted by the epidemic model differential equations (7.1.1). Moreover, fig. A.11(a) reveals that the average of the total damage over 20 runs of the simulation with the above parameters, closely match those predicted by the epidemic model; also as expected, the damage increases with increase in $I_0$. Similar trends and matches can be observed for random waypoint and random direction mobility models (defined in [30]).
Figure A.4: Comparison of the simulated and calculated costs for a network of 41 nodes with exponentially distributed inter-contact times. The solid lines represent the cost derived from the epidemic model (calculated cost), and the dashed lines are the averages over 100 simulation runs for different values of \( I_0 \).

Despite the lack of homogeneous mixing property, we observe that the average of 20 runs shows that the overall damage follow similar trends (fig. A.11(b)) as under the epidemic representations, with universally lower overall damages as compared with the calculated damage. This is intuitively because when homogeneous mixing does not hold, the infection tends to stay local and less frequently reaches new (susceptible) nodes,

which has a self-suppressing effect on the spread of the malware. This phenomenon can be better seen in fig. A.10(b).

Finally, we consider a cellular network composed of 400 nodes and 8 base stations. Nodes follow uniform mobility and are associated with the nearest base-station. Infective nodes try to transmit the malware to randomly chosen IDs (cell phone number) - the communication proceeds through the base stations serving the node-pair. The security patches are distributed by base stations to the mobiles via control channels. The overall data (and control message) exchange bandwidth of each base-station is divided equally among the associated nodes. Fig. A.10(c)
Figure A.5: Simulated and calculated trajectories of the states for a network of 400 nodes with exponential inter-contact times. The solid lines represent the trajectories obtained from the epidemic model (calculated trajectories), and the dashed lines are the averages of the trajectories over 100 simulation runs.

and A.11(c) show an acceptable match between our simulation and the epidemic model both for states and game values in the case of a cellular network too.

**Robustness against drifts in local times** We next evaluate the performance, i.e., the overall damage, when nodes’ clocks drift from the global clocks by different amounts, and hence they choose different threshold times (optimal threshold time + individual drift). We consider the DTN setting with uniform mobility model, and clock drifts which are statistically independent and uniformly distributed between $-A$ and $A$. Fig. A.9 depicts the overall damage as a function of $A$ averaged over 100 simulation runs. Note that even for $A$ as large as $T/2$ (i.e., 50% inaccuracy in the value of the threshold times) the increase in the overall damage is less than 9%.
Figure A.6: Comparison of the simulated and calculated costs for a network of 400 nodes with exponentially distributed inter-contact times. The solid lines represent the cost derived from the epidemic model (calculated cost), and the dashed lines are the averages over 100 simulation runs for different values of $I_0$.

Figure A.7: Simulated and calculated trajectories (i.e., sample paths) of the states for a network of 41 nodes with truncated power-law inter-contact times. The solid lines represent the trajectories obtained from the epidemic model (calculated trajectories), and the dashed lines are the averages of the trajectories over 100 simulation runs.
Figure A.8: Comparison of the simulated and calculated costs for a network with power-law distributed inter-contact times. The solid lines represent the cost derived from the epidemic model (calculated cost), and the dashed lines are the averages over 100 simulation runs.

Figure A.9: Robustness of the saddle-point strategy with respect to clock drift. The increase in the overall cost is less than 9%. 

196
Figure A.10: Average of 20 different runs of the evolution of the states under their the saddle point strategies for DTNs with homogeneous mixing (uniform mobility model) in (a), DTNs with non-homogeneous mixing (power-law inter-meeting times) in (b), and for a cellular network in (c).

Figure A.11: Average of 20 different runs of the overall damage under their respective saddle point strategies for DTNs of 41 and 123 nodes with homogeneous mixing (uniform mobility model) in (a), DTNs with 41 nodes with non-homogeneous mixing (power-law inter-meeting times) in (b), and for a cellular network of 400 nodes and 8 BST’s in (c). Fig. A.11(a) also shows that the match improves with increasing $N$. 
Bibliography


[69] T. Small and Z.J. Haas. The shared wireless infostation model: a new ad hoc networking paradigm (or where there is a whale, there is a way). In MobiHoc’03. ACM, 2003.


