PhD Proposal: Optimal Control of Epidemics in the Presence of Heterogeneity

Soheil Eshghi

Abstract

I seek to identify and address how different types of heterogeneity (in actors and actions) affect the optimal control of epidemic process in social, biological, and computer networks. Epidemic processes encompass a variety of models of propagation that are based on contact between agents (e.g., compartmental models, consensus dynamics, Bayesian belief propagation). Assumptions of homogeneity of actors and uniformity of actions, states, and motivations in prior literature gloss over the heterogeneities inherent to such networks and lead to the design of sub-optimal control policies. However, the added complexity that comes with a more nuanced view of such networks complicates the generalizing of most prior work and necessitates the use of new analytical methods. I will apply the mathematical theory of optimal control to heterogeneity-rich models of epidemic spread developed in epidemiology and sociology, as well as those arising from practice in the fields of communication network and security. I have shown that in some applications, e.g., heterogeneous SIR epidemics & DTN message routing, factoring heterogeneity in the control decision can improve the performance of the system substantially. In others, e.g., models of opinion dynamics, heterogeneity models an essential part of the system under study, and simplification leads to a loss of validity of the model. Therefore, addressing the various ways in which heterogeneity affects control decisions and the responses of agents in the network is a fundamental question in both theoretical and applied network science. I seek to understand how heterogeneity affects optimal controls in various applied contexts/models of epidemics, and to use that insight to propose practical control policies that achieve optimal performance.

I. Introduction

An epidemic occurs when a disease spreads rapidly among a target population. More generally, any process that involves spreading via interaction can be thought of as an epidemic. Examples of epidemic or epidemic-like processes include the spread of a virus among the human or animal population, malware over a computer network, information over a communication network, and a rumor on social media.

Mathematical models for epidemics, such as those put forth by Daniel Bernoulli [10], predate the germ theory of disease by as much as 100 years. These models, which can be either deterministic or stochastic, seek to track and predict the number of infected individuals. Of these models, deterministic ones have received the most attention in recent years, both due to their relative analytical straightforwardness and due to limit results.[1] It was Hamer [21] who first postulated that the rate of spread of an epidemic is a function of both the populations of infected individuals and those yet to be infected, which is the celebrated mass-action model. This means that the spreading process is non-linear.[2]

While initial work in epidemic modeling was focused on understanding the evolution of an epidemic, intervention policies were soon to follow [22], [43], [60], [61]. These policies seek to stop the spread of an epidemic given limitations on possible actions, such as the limitations that the availability of vaccines, hospital beds, and healthcare workers impose on the control of biological epidemics. Wickwire [61] and Behncke [8] laid the ground-work for most optimal control approaches to date. However, these approaches are limited to homogeneous epidemics, where all nodes are assumed to have the same characteristics (e.g., contact rates, types, importance) and to have identical behavior (i.e., identical control policies).

[1] E.g., those obtained by Kurtz [32] that show an equivalency between the two given some general conditions.

[2] This nonlinearity complicates the analysis of epidemic processes, and leads to interesting behavior such as the Basic Reproduction Number (R_0) threshold results on the terminal spread of an epidemic (c.f., [4]).

A. Motivations for Heterogeneity

In practice, however, most epidemics are not homogeneous. Many epidemics spread *non-homogeneously* among the target population, infecting some more frequently and faster than others. In viral epidemics, this can be due to biological, geographical, behavioral, cultural, or socio-economic reasons [13]. I will examine three sources of heterogeneity in turn:

1) Rate-Heterogeneity: One of the primary ways in which an epidemic can be heterogeneous is when it has different effects and rates of spread in sub-populations.[3] Policies can similarly be non-homogeneous given a dependence on the heterogeneous sub-populations. These sub-populations, or clusters, may result from a variety of reasons, relating to the *nature* of the network: 1- **Locality:** In this case, *rate-heterogeneity* arises because contact rates among distant nodes are less than those among closer ones. This is most natural assumption in most types of biologic and social epidemics (i.e., where the epidemic spreads via physical contact) and has led to the study of *ecoepidemics* [41]. 2- **Clique/cluster formation:** With the rise of data networks, physical proximity is no longer necessary for the propagation of malware and social epidemics. Users of the same clique can be regarded as the same type with the rate of contact within cliques and across cliques differing depending on the relative sizes of the cliques and their contact rates. Alternately, in cluster (or grid, or volunteer) computing [3], each cluster of CPUs in the cloud constitutes a type. Any two computers in the same cluster can communicate at faster rates than those in different clusters. 3- **Behavioral patterns:** In malware epidemics, agents can be clustered based on their security-consciousness, creating safe and risky types based on usage history [66]. Security-savvy users may use more secure protocols, avoid executing untrustworthy code or mass forwarding a received message. The rate of propagation of the malware is therefore the lowest among safe users, higher between safe and risky users, and highest among the risky users. Clustering can also arise naturally in the contexts of technological adoption, fads, opinions [18], [51], [52], where social contact between adopters of various options and the undecided (infection propagation/ immunization) can lead to their spread. 4- **Software/Protocol diversity:** Studies have shown that a network that relies on a homogeneous software/protocol is vulnerable to an attack that exploits a common weakness (e.g., a buffer overflow vulnerability) [35], [47], [62]. In practice, mobile nodes use different operating systems and communication protocols. Such heterogeneities lead to dissimilar rates of propagation of malware among different types, where each type represents a specific OS, platform, software, protocol, etc.

2) Resource-Heterogeneity: Furthermore, epidemics may spread heterogeneously based on *naturally fluctuating resource-states* in the system that are not inherent to the node (e.g., remaining battery-power in nodes), which leads to fluid types, in contrast to most of the inherent types discussed above. Specifically, the composition of each type of nodes will evolve with time. In these cases, resource constraints limit the ability of particular nodes to perform a certain function, thus stratifying nodes based on their remaining resources. For example, in a Delay-Tolerant Network, or DTN, the ability of a node to relay a message towards its destination depends on its remaining energy reserves. However, message-forwarding consumes energy in the sender and the receiver, which impacts the nodes' future ability to forward further messages. Thus, nodes will be naturally stratified based on the number of messages that they can pass, which is a function of their remaining energy (*stratification due to resource-heterogeneity*).

3) Heterogeneity of Epidemics: Finally, multiple epidemics may evolve in tandem, with possible correlations in their infected targets. These epidemics may either: 1) compete for the same nodes, as is the case in multiple strains of a viral epidemic [24], [25] and memes in a world with a limited attention span [59] , 2) have an amplifying effect on each others' spread, as is the case with the HIV/TB co-epidemic [23], or 3) they may spread *in conjunction* with each other, where their relative spread is coordinated. In computer networks, this last case can model the case where there are multiple malware types/variants available to the attacker (possibly with different capabilities), and thus the network is attacked by an amalgamation of closely-interlinked malware. For example, variants of a particular malware

[3]In literature, these settings have been described by terms such as stratified, structured, clustered, multi-class, multi-type, multi-population, compartmental epidemic models, and sometimes loosely as heterogeneous, inhomogeneous or spatial epidemic models.

may execute different policies at certain time as a means of balancing other objectives (e.g., stealth) against the immediate damage that they inflict. In particular, malware such as Stuxnet [33] have had multiple variations that were released at different times with differing functionalities to achieve a unified goal. This is a third type of non-homogeneity - that of the *epidemic* itself.

B. Agenda

Models of epidemics need to capture these heterogeneities to be able to form a clear picture of the spreading mechanism.[4] However, prior work has focused on the control of homogeneous epidemics, and thus is deficient in describing real-world epidemics. Multidimensional optimal control formulations, which seek to find optimal *functions* rather than variables, are usually associated with the pitfall of amplifying the complexity of the optimization. This added complexity means that prior approaches will not, in general, yield results for the control of a heterogeneous epidemic. In addition, consideration of heterogeneity will give rise to a wealth of possible structural results for these *vectors of optimal controls* that can be derived and exploited by the controller. Thus, the control of heterogeneous epidemics is a novel, necessary, and natural topic of study that has many real-world applications.

In this proposal, I aim to understand how heterogeneity in contact rates, resources, and epidemics themselves can be leveraged to improve the control of epidemics and epidemic-like processes. In particular:[5]

- I seek to derive a theory of optimal control of *type-heterogeneous* epidemics with a focus on SIR models of malware spread (§II). These models divide agents into compartments based on their infection status: Infected (I) agents have already contracted the malware, Susceptible (S) individuals have yet to contract the malware but are not immune to it, and Recovered (R) agents are not susceptible to the malware, either due to inherent immunity or pre- or post-infection patching. Subsequently, these models utilize a mass-action model of interaction to capture the spreading dynamics of the epidemic.[6] I will concentrate on optimal control policies for classes of defenders that may have different sensitivities to infection (i.e., perceived or real damage) and differing control mechanisms at their disposal.
- I aim to develop a theory of optimal control of *resource-heterogeneous* epidemics, focusing on a case where resource-heterogeneity results from differences in the remaining energy of nodes in the process of message delivery in a a Delay-Tolerant Network, or DTN (§III). In this case, the resource-state is available to the node, and can be factored into its message-forwarding decision. I concentrate on understanding the structure of these forwarding decisions, as well as their dependence on the energy-states in settings which guarantee a certain Quality of Service (QoS).
- Finally, I seek to put forth a theory for the optimal control of cases where the *epidemic* itself is *heterogeneous*. In particular, I investigate stealth-aware optimal spread of malware in §IV, where there is an inherent heterogeneity to the *infections*. In this case, an attacker balances the need for stealth against the traditional aim of damaging a network, as has been seen in some recent malware [33]. Here, I aim to understand the structure of the optimal decisions of the malware developer, given a range of possible assumptions on the capabilities at their disposal, and to characterize the optimal spread of the epidemic both on its own and in the presence of a network defense mechanism.

II. Rate-Heterogeneity: Optimal Control of Clustered Malware Epidemics[7]

I consider the spread of a malware epidemic in a heterogeneous environment where nodes are stratified based on their respective contact rates. In the environments, immunization/healing/patching policies need to

[4]The limit results of Kurtz [32] were extended to the multi-type setting by Ball and Clancey [6], allowing the use of deterministic multi-type models.

[5]Here and subsequently, "I" and "my" are used in description of the work while acknowledging the contributions of my co-authors M.H.R. Khouzani, Saswati Sarkar, Santosh S. Venkatesh, and Ness B. Shroff, who contributed to some or all of the work.

[6]These models are very closely related to the Lotka-Volterra predator-prey ecological model (c.f., [41].)

[7]Presented in the Information Theory and Applications Workshop (ITA) 2012, to appear in IEEE Transactions on Networking 2014.

cater to the specific stratum to ensure maximal efficacy. In malware epidemics, as opposed to biological ones, the healing mechanism (i.e., patching) can be replicative, which means that patched nodes may be able to spread the patch to other nodes. This possible secondary spread of immunity also arises in some of the other rate-dependent heterogeneous epidemic models (see §I-A1). I consider the immunization/healing/patching rates as dynamic controls that evolve with time. The aim of this investigation was to find optimal, custom trade-offs between the damage sustained by the network and the resources spent in patching it against the malware utilizing the heterogeneity in contact-rates among nodes in the network. The gains from these *rate-heterogeneous* approaches, however, usually come at a cost (in terms of computation, storage, sensitivity, etc.) which depends on the nature of the network. Characterizing these costs and the resulting optimal immunization/healing/patching structures determine whether the controller should make use of such mechanisms. I seek to quantify the changes that arise from such an approach as compared to simpler ones that assume a homogeneous network. In particular, I seek to answer the following questions:

- How can the the spread of an epidemic in a rate-heterogeneous environment, and the corresponding response of the network be *modeled* to capture the various real-world malware epidemic scenarios described?
- How can the vector of optimal patching controls, that determine the patching action within each cluster be *computed*?
- Is there an underlying *structure* to these optimal controls, and how do they perform *compared* to simple heuristic homogeneous policies?

A. Contributions

- I *modeled* this *contact-rate heterogeneity* by considering logical clusters of nodes where each cluster constitutes a *type*. Nodes of the same type homogeneously mix with a rate specific to that type and nodes of different types contact each other at rates particular to that pair of types, with SIR epidemic dynamics that evolve according to these pairwise contact rates. The model can therefore capture any communication topology between different groups of nodes. I considered both *non-replicative* and *replicative* patching: in the former, some of the hosts are pre-loaded with the patch, which they transmit to the rest. In the latter, each recipient of the patch can also forward the patch to nodes that it contacts by a mechanism similar to the spread of the malware itself. In my model, patching can immunize susceptible nodes and may or may not heal infective nodes. The dynamics of the model can be seen in Fig. 1.
- I proposed a formal framework for *computing dynamic optimal* patching policies that leverage heterogeneity in the network structure to attain the minimum possible aggregate cost due to the spread of malware and the overhead of patching. The framework in each case relies on optimal control formulations that cogently capture the effect of the patching rate controls on the state dynamics and their resulting trade-offs. I accomplished this by using a combination of damage functions associated with the controls and a *stratified* mean-field deterministic epidemic model in which nodes were divided into different types. Above and beyond, it can exploit the inhomogeneity in the network to enable a better utilization of the resources. Such higher patching efficacy is achieved by allowing the patching controls to depend on node types, which in turn gives rise to *multidimensional (dynamic)* optimal control formulations. These formulations lead to a solution framework derived from Pontryagin's Maximum Principle, which characterizes necessary conditions for the optimality of vectors of controls.
- I proved that for both non-replicative and replicative settings the optimal control associated with each type has a simple *structure* provided the corresponding patching cost is either concave or convex. These structures were derived using Pontryagin's Maximum Principle and analytic arguments specific to this problem. This derivation reveals that the structure of the optimal control for a specific type depends only on the nature of the corresponding patching cost and not on those of other types. This fact (correspondence of the nature of the optimal patching control in a type to the convexity

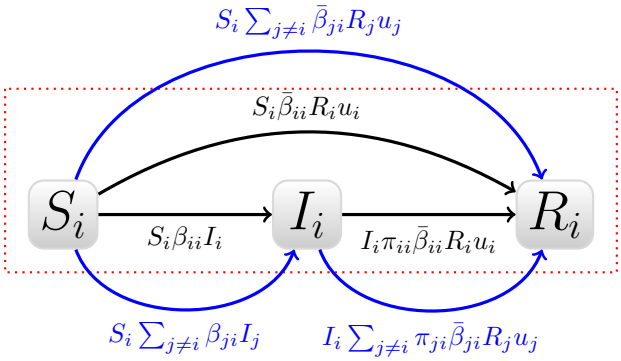

Fig. 1. This figure captures the SIR dynamics within each agent type, as well as the interactions between types. The numbers on the arrows indicate rates. Blue arrows indicate inter-type contacts, while black ones represent contacts that happen within each type. Notice that the communication rates (denoted by β) between susceptible agents of a certain type i and the infected nodes of type j can be different from their communication rate with recovered notes of the same type, a situation that may arise due to the nature of the system (e.g., in the case of two competing infections) or because of provisions taken by either the attacker or the defender (i.e., $\beta_{ij} \neq \beta_{ji}$). u_j denotes the dynamic control of the defender on the propagation of patches by type j, while π_{ji} (static) represents the extent to which infected agents of type i can be healed by agents of type j.

or concavity of the patching cost in that particular type and not that of others) is surprising, as the control for each type affects immunization and healing in other types and the spread of the infection in general. Specifically, if the patching cost associated with the control for a given type is concave, irrespective of the nature of the patching costs for other types, the corresponding optimal control turns out to be a bang-bang function with at most one jump: up to a certain threshold time (possibly different for different types) it selects the maximum possible patching rate and subsequently it stops patching altogether. If the patching cost is strictly convex, the decrease from the maximum to the minimum patching rate is continuous rather than abrupt, and monotonous. Note that each of these bang-bang controls can be represented by one point (the threshold), and thus the vector of control functions can be expressed as a vector of scalars of the same size, which simplifies their computation and storage. Furthermore, the simplicity of these structures makes them suitable for implementation, while also providing a benchmark for other policies that may require fewer network parameters. The optimal controls were compared to heuristic and homogeneous alternatives over real-world traces and numerical simulations in a variety of sample topologies. As expected, it was seen that as contact rates become more varied within a topology, homogeneous approximations to the optimal controls become very inefficient. This experimentally validated the premise of considering rate-heterogeneity in the choice of the patching controls.

B. Literature Review

Epidemic models, and especially SIR epidemic models, have been used extensively to model the spread of malware and the propagation of information in computer networks, beginning from Murray [44] and Kephart and White [26]. Recent work on malware and information epidemics has focused on how these epidemics can be controlled [1], [30], [37]. However, the work on the propagation of information (such as [1], [37]) has focused on two-hop routing with no adversaries, which does not apply to malware defense and a host of other applications such as technology adoption. On the other hand, works on malware defense, such as [30] have modeled healing and immunization as contact-independent exogenous processes that are uniform among all nodes, which are very limiting assumptions. Recognizing the constraints of the defender, works such as [27], [28] have included the cost of patching in the aggregate damage of the malware and have characterized the optimal dynamic patching policies that attain desired trade-offs between the patching efficacy and the extra taxation of network resources. Similarly, Li *et al.* [36] and Altman *et al.* [2] have characterized optimal dynamic transmission control policies for two-hop and multi-

hop messages. These results, however, critically rely on the *homogeneous* mixing assumption: that all pairs of nodes have identical expected inter-contact times. Thus, there will only be one optimal control for the system. While this assumption may serve as an approximation in cases where detailed information about the network is unavailable, studies [12], [34], [42], [48], [57] show that the spread of malware in mobile networks can be very inhomogeneous, owing primarily to the non-uniform distribution of nodes. Thus, a uniform action may be sub-optimal.

C. Positioning of the work with respect to existing literature

To the best of my knowledge, my work was the first that considers the control of a general stratified epidemic and provides analytical structural guarantees for a dynamic patching.[8] My model is general enough to capture any clustering of the nodes with arbitrary inter-contact rates of interaction and to allow different methods of type specification. Owing to the heterogeneity of nodes, it becomes necessary to have differing controls for different strata (types), leading to a *vector* of controls as opposed to the *single* control that was derived for *homogeneous* users in prior literature. Deriving structure results for a vector of controls requires analytical arguments that are quite different from those employed for a single control. The simple structure results described for the optimal policies have not been established in the context of (static or dynamic) control of *heterogeneous* epidemics. The power of my analytical results is in the extensive generality of my model.

III. Resource-Heterogeneity: Optimal Energy-Aware Epidemic Routing in DTNs[9]

In Delay-Tolerant Networks (DTNs), end-to-end connectivity is rare, and messages have to be passed along by intermediate nodes to reach their destination. Most importantly, message forwarding consumes energy in the intermediate nodes, which is critical as in many cases their energy supplies are non-replenishable (e.g., where communication devices are carried by disaster relief personnel and soldiers, or where they can be mounted on wandering animals). These forwarding decisions leave different nodes with different remaining energies at each time-instant, leading to an exploitable *resource-heterogeneity* in the network. This message forwarding process can accordingly be *controlled* to achieve certain objectives in terms of both the delivery of the message and the resources of the network. A fundamental question in this realm is how to balance quality of service (i.e., the probability that the message reaches its destination in a timely manner) against the use of network resources (such as node battery power and bandwidth). It is of practical importance to see whether it is possible to derive optimal controls that depend on readily-measurable resource-states of nodes (such as battery power), and to quantify the effects of this trade-off and the benefits of incorporating the additional information in the decision. In particular, it 3 questions are worth addressing:

- How can message transmission in a DTN network be *modeled* to incorporate this resource heterogeneity and the dependence of the message forwarding decision process on the remaining battery resources?
- How can the resulting resource-state-dependent optimal message forwarding decisions be *computed*?
- Finally, is there any underlying *structure* to these optimal decisions that can be exploited in their derivation, storage, and implementation? Are these optimal controls stable to errors, and how do they compare to existing solutions?

A. Contributions

- I *modeled* message transmission in a DTN as a resource-state heterogeneous controllable SI epidemic, where the forwarding policies in each node constitute the controls. I defined a node that had received

[8] Li *et al.* [37] consider a 2-type epidemic, but with no control. All other prior work has assumed *one uniform control* for one set of *homogeneous* users.

[9] Presented in IEEE MobiHoc 2012, to appear in IEEE Transactions on Automatic Control 2014.

a copy of the message and is not its destination as an *infective* (I) and a (non-destination) node that had not yet received a copy of the message as a *susceptible* (S). When an infective node contacts a susceptible at time t, the message is transmitted with a certain forwarding probability if the infective (transmitter) and susceptible (receiver) have at least s and r units of energy (s and r being the energy necessary for transmission and reception of the message). Stratifying the nodes based on their energy resource-state, I defined $S_i(t)$ (respectively, $I_i(t)$) to be the *fraction* of nodes that are susceptible (respectively, infective) and that have i energy units at time t. At any given time, each node can observe its own level of available energy, and its forwarding decision should, in general, utilize such information. Hence, upon an instance of contact between a susceptible node and an infective node, the message is forwarded with probability $u_j(t)$ ($0 \leq u_j(t) \leq 1$). I took these probabilities to be my controls $\mathbf{u}(t) = \big(u_s(t), u_{s+1}(t), \ldots, u_B(t)\big)$. If the message is forwarded, the susceptible node of energy i transforms to an infective node with $i - r$ energy units, and the infective node of energy j likewise to an infective node with $j - s$ energy units. If a message-carrying node that has sufficient energy for one transmission contacts the destination that has yet to receive the message, the message is always forwarded to the destination. These dynamics can be seen in Fig. 2. I modeled the evolution of these fractions (states) using epidemiological differential equations that rely on mean-field approximation of Markov processes. Subsequently, I formulated the trade-off between energy conservation and likelihood of timely delivery as a dynamic energy-dependent optimal control problem: at any given time, each node chooses its forwarding probability based on its current remaining energy. Since the number of relay nodes with the message increases and residual energy reserves decrease with transmissions and receptions, the forwarding probabilities vary with time. Thus, they must be chosen so as to control the evolution of network states, which capture both the fraction of nodes holding a copy of the message and the remaining battery reserves of the nodes.

- I sought to *compute* dynamic forwarding probabilities (*optimal controls*) that optimize objective functions penalizing energy depletion subject to enforcing timely message delivery. These dynamic forwarding probabilities constituted my optimal controls. The resulting optimal control problem is solved using Pontryagin's Maximum Principle, which leads to a computational framework for the optimal controls.
- Utilizing the above framework combined with arguments specific to this context, I characterized the *structures* of these resource-dependent optimal controls (i.e., forwarding decisions) and showed that they follow simple rules that can be computed in a computationally efficient manner.

  My first result was to prove that dynamic optimal controls follow simple threshold-based rules. That is, a node in possession of a copy of the message forwards the message to nodes it encounters that have not yet received it until a certain threshold time that depends on its current remaining energy. Calculating these thresholds is much simpler than solving the general problem and can be done once at the source node of the message. Subsequently, they can be added to the message as a small overhead. Each node that receives the message can retrieve the threshold times and forward the message if its age is less than the threshold entry of the node's residual energy level. The execution of the policy at each node is therefore simple and based only on local information.

  My second result was to characterize the nature of the dependence of the thresholds on the energy levels. Intuitively, the less energy a node has, the more reluctant it should be to transmit the message, as the transmission will drive it closer to critically low battery levels. However, my investigations revealed that this intuition can only be confirmed when the penalties associated with low final remaining energies are convex. In particular, I constructed a viable case with non-convex costs where the optimal thresholds did not follow this intuition.

  My optimal control provided a missing *benchmark* for forwarding policies in large networks in which no information about the mobility pattern of the individual nodes is available and a minimum QoS is desired. This benchmark allowed me to observe the sub-optimality of some simpler heuristic policies, and to identify parameter ranges in which they perform close to the optimal. Furthermore, I showed that the optimal controls were robust to estimation errors in their parameters and synchronization,

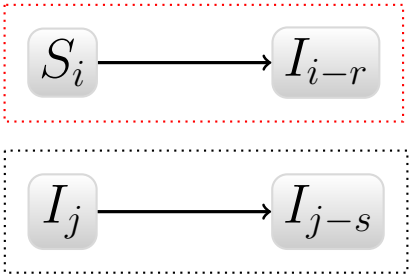

Fig. 2. This figure captures how the message transmission upon contact changes the energy levels of nodes, as well as infecting the susceptible node. The dotted boxes represent the two agents in which the simultaneous transformations that result from a message transmission occur. The susceptible agent becomes an infective while losing r units of power, while the infecting agent spends s units of energy to send the message.

and that they performed much better than heuristics in cases with more energy heterogeneity and starker penalties on energy mis-utilization. Finally, I showed that these optimal controls extended the number of messages a network could transmit before exhaustion, which is a measure of network lifetime.

B. Literature Review

The literature on message routing in DTNs is extensive [1], [5], [7], [14], [15], [38], [39], [45], [46], [53]–[56], [58], [64]. Most notably, Vahdat and Becker [56] present a policy where each node propagates the message to all of its neighbors simultaneously ("Epidemic Routing"), while Spyropoulos *et al.* [55] propose spreading a specific number of copies of the message initially and then waiting for the recipients of these copies to deliver the message to the destination ("Spray and Wait"). Wang and Wu [58] present "Optimized Flooding", where flooding is stopped once the total probability of message delivery exceeds a threshold. Singh *et al.* [54] and Altman *et al.* [1] identify optimal and approximately optimal message forwarding policies in the class of policies that do not take the distribution of node energies into account. In summary, the state of the art in packet forwarding in DTNs comprises of heuristics that ignore energy constraints [38], [56], [64], those that consider only overall energy consumption but provide no analytic performance guarantees [7], [14], [39], [46], [55], [58], and those that do not utilize the energy available *to each node* in making forwarding decisions [1], [5], [15], [45], [53], [54]. An efficient forwarding strategy can use knowledge of the distribution of energy among nodes to its advantage, and this motivates the design of dynamic energy-dependent controls which are the subject of this work.

C. Positioning of the work with respect to existing literature

To the best of my knowledge, my work was the first work that considers message routing in DTNs as a *resource-heterogeneous* optimal forwarding problem where the forwarding decision of a node is based on its remaining energy. Furthermore, the optimal structures derived for the forwarding decisions are also a contribution of the work, given the difficulties posed by vectors of controls. Next, the threshold ordering results for the optimal controls, obtained for convex costs, are without precedent in proposition and analysis. Finally, the counter-example provided shows that convexity is a relatively strong sufficient condition for this ordering phenomenon.

IV. Epidemic-Heterogeneity: Visibility-Aware Epidemics[10]

Multiple epidemics may spread simultaneously in a network, leading to a third type of heterogeneity: *epidemic heterogeneity*. In particular, malware epidemics differ from biological ones in that multiple

[10]Submitted to IEEE CDC 2014.

variants of an epidemic can spread in a *coordinated* manner. Furthermore, these epidemics can be *designed* to respond to triggers and to act in such a way as to maximize a certain utility for the malware designer, perhaps even factoring the response of the defender (controlled evolution). This creates challenges for security professionals who have to understand the motivations and methods of these malware designers. The malware designer's control, in this model, is maintaining the mix of the malware variants in time to achieve a certain objective. Thus, the designer's decision to spread the epidemic will be dependent on the particular variant, leading to *heterogeneous control structures*.

Specifically, a new generation of malware, one that eschews damage to the network to maintain stealth, has led to new challenges in computer network security. These "surgical" strikes seek to minimize visibility, as awareness can lead the intended target to cease communication (e.g., by quarantining the targets). Stuxnet, for example, was designed to attack a specific control software used in centrifuges [17] and did not steal or manipulate data, or receive any command instructions from remote sources so as to maintain stealth [33] (cf. Duqu, Flame, and Gauss [9]). Yet, it was discovered and remedied after it spread outside its target area [49]. Thus there is a new trade-off for the attacker — that between stealth and damage. Specifically, if the malware spreads too fast, it will also be detected and remedied fast, so a slower spread may mean that it can cause more aggregate damage. Thus, in contrast to many other epidemiological contexts, aggressive policies may not be optimal.

In particular, I consider the case where two variants of a single malware spread in a network. One spreads aggressively in every contact, and is thus visible to the network due to its communications, while the other passive variant does not spread subsequent to infecting a node. As coordinating distributed attacks requires coordination and timing, which comes at the cost of added visibility due to communication and is susceptible the timing errors in the hosts, I focus on the case where distributed nodes that are infected are not asked to coordinate, as was the case in Stuxnet. The natural question that arises is to characterize the structure of optimal malware variant mix that the attacker will spread at each instant depending on her goal structures and the communication mechanisms that they may have at their disposal. I seek to answer the following questions:

- How can a visibility-conscious malware designer's decision to spread either of the potent-yet-visible or less-potent-but-less-visible variants of a malware at each time instant be *modeled*?
- How can these optimal mixing decisions be *computed* given the variety of possible mechanisms available to the designer and defender?
- Are there any particular *structures* in the optimal decisions of the designer, and are these optimal policy structures vulnerable to the effects of the network's estimation errors on its defense policy once the malware is released into the wild?

A. Contributions

- I *modeled* a network under attack by these two variants of a malware. Depending on their infection status, nodes could be divided into 4 groups: 1) *Infectives* (I) that are a fixed (potentially very small) fraction of the nodes that are the only nodes under the direct control of the attacker, 2) *Susceptibles* (S) that are nodes that have not received any variant of the malware, 3) *Zombies* (Z) that have received the aggressive malware variant and will continue to propagate it indiscriminately,, and 4) *Passives* (P) that have received the passive variant of the malware, and thus do not propagate it any further. Both zombies and infectives can contribute to damaging the network through the execution of malicious code. Zombies, however, are potentially visible to the network as they have to communicate with other nodes to spread the message. I proposed a mathematical formulation for the state dynamics governing interaction between nodes in these 4 groups and their transformation from one to the other, as well as the impact of the attacker's control. In this model, the infectives, at each encounter with a susceptible, decide whether to turn it into a zombie or a passive, or to leave it as a susceptible. I also investigated the case where I added a further mechanism of interaction whereby the infectives, upon contact with zombies, can turn them into passives (i.e., stopping them from spreading the message

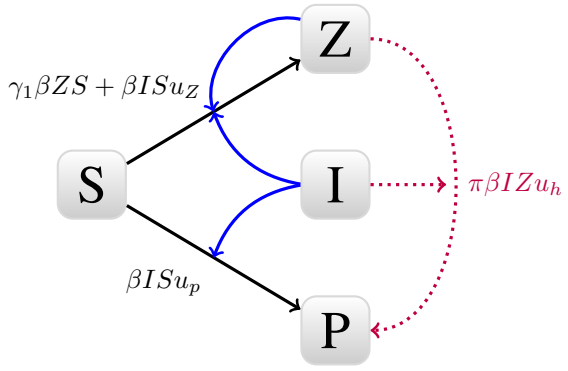

Fig. 3. The solid black arrows show the dynamics in the visibility-aware epidemic model with no killing (the ability to make zombies into passive agents upon contact). The red arrows show the additional mechanism that affects the case where killing is assumed in the model. Finally, in the case with network defense, β is replaced by $\beta(Z)$, which is a function of the number of zombies (i.e., the visibility of the epidemic). Note that the population of I never changes, and the arrows emanating from it show that some changes happen when an infective agent encounters another type of agent. As before, the numbers beside the arrows denote rates of transition.

any further). Finally, I formulated state dynamics that account for the network's defense strategy. Once a defender becomes aware of a malware outbreak, she can ask nodes to limit their effective contacts as a means to limit the spread of malware. This, however, comes at a cost of stopping legitimate communication within the network. For a pictorial representation of these 3 dynamics, see Fig. 3. I quantified the damage inflicted by the malware through characterizing an overall damage function consisting of an efficacy function of the aggregate number of zombies and passives, and a visibility function of the number of zombies. In the first two models described above, the attacker chooses controls that maximize this damage. In the latter model, the effect of visibility is built into the network dynamics, as I allow the network to choose a policy based on the fraction of zombies, and so the attacker is only directly concerned with maximizing efficacy.

- I sought to *compute* dynamic malware-spread mixes (*optimal controls*) that the malware designer would employ to optimally balance her objectives of maximum damage and minimum visibility. These dynamic decisions, which determined the probability that each variant will be spread at each encounter between an infective and a susceptible, constituted my optimal controls. The resulting optimal control problem is solved using Pontryagin's Maximum Principle, which leads to a computational framework for the optimal controls.
- I showed that the attacker's optimal strategy in all of these models follows a certain *structure*: the infectives only create zombies up to a certain time, and then only create passives (including by halting zombies) from then on. That is, the optimal controls are *bang-bang* (i.e., only taking their minimal and maximum values) with only one jump. It is interesting to note that in each of the variations I considered, my analysis revealed that all the controls switch at the same point, a fact that was not at all clear *a priori*. Thus the entire control space could be described by one time-point, a fact that is invaluable for deriving the optimal controls computationally. Furthermore, the controls were easy to implement as the infectives need to be programmed with just one time instant for all of their controls. After completely characterizing the optimal controls, I investigated the effect of the network's estimation errors in the latter model for network response. I demonstrated that the model performs reasonably well even when there are small errors in the network's estimation of the number of zombies, which it uses to determines its response to the malware epidemic.

B. Literature Review

Multiple interacting epidemics that spread among a single population have been considered in the fields of biology [24], [25] and sociology [59]. In these models, these epidemics either compete for a limited pool of susceptible nodes, or cause the susceptibles to become more vulnerable to other epidemics. However,

in all these contexts, there is no mechanism to coordinate the actions of competing epidemics. In the realm of malware, on the other hand, such a coordination among multiple epidemics can not only exist, but can be intrinsic to the attack strategy of a malware designer. Furthermore, in the majority of malware epidemic models, e.g., [19], [20], [31], [40], [50], [65], two things have generally been assumed: 1- that the attacker's sole aim is to maximize the spread of the malware, and 2- that they have a mechanism to control the malware in the future (through a timer in the code, for example– for a similar framework, see [16]). As I described, these two assumptions are no longer true for the emerging generation of malware. Thus, the model presented for the spread of visibility-heterogeneous malware variants has no precedent in literature. Accordingly, the questions I asked and the solutions I obtained are substantially different to prior work. The closest work to this topic was by Khouzani and Sarkar [29]. They examined how malware spread can be maximized by controlling the transmission ranges of mobile nodes. In their model, initiation of the attack immediately leads to patching by the defender, which will not be the case for complex malware like Stuxnet that are very large and extremely hard to decipher, let alone mitigate [11], [63]. Furthermore, the optimal malware action in this model depends on distributed nodes taking an action simultaneously, which requires either communication among nodes or using the internal clock of the infected node, both risky maneuvers that can lead to detection and/or error. In my models, the attacker does not count on being able to coordinate distributed actions among nodes not under its direct control in time, and she also assumes that the communication ranges of nodes are outside her control, perhaps even being controlled by the defender as a mitigation mechanism.

C. Positioning of the work with respect to existing literature

To the best of my knowledge, my work was the first work that considers the problem of multiple coordinated malware variants spreading in a network (malware *epidemic heterogeneity*). Furthermore, the consideration of stealth as a means of stratification of the epidemics and as a goal of the malware designer is also without precedent. The optimal structures that are presented for the optimal malware spreading probabilities also constitute a contribution of the work. The simple structure of these optimal controls - that at each time, the spread of only one variant of the malware is encouraged, with only one abrupt transition in the preferred malware - holds for all the models presented. This means that it is reasonable for a network defender to assume this simple action structure for the actions of the malware designer. Finally, the numerical simulations show that the model is not sensitive to estimation errors in the fraction of visible malware (zombies) on the part of the network defender, and thus the simple defense structures assumed in the latter model can be a reasonable starting point in the derivation of optimal stable defense strategies for the network.

V. Conclusion

I aim to understand how heterogeneity, which manifests itself in contact rates, resource-states, and the nature of the epidemics themselves, can be leveraged to improve the control of epidemics and processes that can be modeled as epidemics.

I have investigated how rate-heterogeneity affects the optimal control of malware epidemics, how resource-heterogeneity can be leveraged to solve an energy-optimal message delivery problem in DTNs, and how epidemic-heterogeneity can be used to understand the design of a new breed of malware. In all of these studies, I have modeled the systems in question, and used context-specific arguments from optimal control theory to understand the optimal treatment, containment, and spreading strategies. In the remainder of my research, I aim to apply a similar approach to other types of epidemic processes, such as rumors and opinions.

These studies will help in the design of various systems: computer network designers will be able to implement the computationally-simple optimal defense policies I propose in §II, and will be able to understand and anticipate the behavior of emerging malware (like the ones in §IV). Furthermore, my work will lead to a fundamentally new approach to message delivery in delay-tolerant networks, where

the quality of service can be balanced against the life-time of the nodes (as described in §III). Finally, my work on multi-type epidemics can also give insights to disease prevention and marketing professionals in choosing their own optimal courses of action.

REFERENCES

[1] E. Altman, A. P. Azad, T. Basar, and F. De Pellegrini, "Optimal activation and transmission control in delay tolerant networks," in *INFOCOM, 2010 Proceedings IEEE*. IEEE, 2010, pp. 1–5.

[2] E. Altman, G. Neglia, F. De Pellegrini, and D. Miorandi, "Decentralized stochastic control of delay tolerant networks," in *INFOCOM 2009, IEEE*. IEEE, 2009, pp. 1134–1142.

[3] M. Altunay, S. Leyffer, J. Linderoth, and Z. Xie, "Optimal response to attacks on the open science grid," *Computer Networks*, 2010.

[4] H. Andersson and T. Britton, *Stochastic epidemic models and their statistical analysis*. Springer New York, 2000, vol. 151.

[5] A. Balasubramanian, B. Levine, and A. Venkataramani, "Dtn routing as a resource allocation problem," in *ACM SIGCOMM Computer Communication Review*, vol. 37, no. 4. ACM, 2007, pp. 373–384.

[6] F. Ball and D. Clancy, "The final size and severity of a generalised stochastic multitype epidemic model," *Advances in applied probability*, pp. 721–736, 1993.

[7] N. Banerjee, M. Corner, and B. Levine, "Design and field experimentation of an energy-efficient architecture for dtn throwboxes," *Networking, IEEE/ACM Transactions on*, vol. 18, no. 2, pp. 554–567, 2010.

[8] H. Behncke, "Optimal control of deterministic epidemics," *Optimal control applications and methods*, vol. 21, no. 6, pp. 269–285, 2000.

[9] B. Bencsáth, G. Pék, L. Buttyán, and M. Félegyházi, "The cousins of stuxnet: Duqu, flame, and gauss," *Future Internet*, vol. 4, no. 4, pp. 971–1003, 2012.

[10] D. Bernoulli and S. Blower, "An attempt at a new analysis of the mortality caused by smallpox and of the advantages of inoculation to prevent it," *Reviews in Medical Virology*, vol. 14, no. 5, pp. 275–288, 2004.

[11] T. M. Chen and S. Abu-Nimeh, "Lessons from stuxnet," *Computer*, vol. 44, no. 4, pp. 91–93, 2011.

[12] Z. Chen and C. Ji, "Spatial-temporal modeling of malware propagation in networks," *IEEE Transactions on Neural Networks*, vol. 16, no. 5, pp. 1291–1303, 2005.

[13] D. J. Daley, J. Gani, and J. M. Gani, *Epidemic modelling: an introduction*. Cambridge University Press, 2001, vol. 15.

[14] E. de Oliveira and C. de Albuquerque, "Nectar: a dtn routing protocol based on neighborhood contact history," in *Proceedings of the 2009 ACM symposium on Applied Computing*. ACM, 2009, pp. 40–46.

[15] F. De Pellegrini, E. Altman, and T. Başar, "Optimal monotone forwarding policies in delay tolerant mobile ad hoc networks with multiple classes of nodes," in *IEEE WiOpt'10*, 2010, pp. 497–504.

[16] S. Eshghi, M. Khouzani, S. Sarkar, and S. S. Venkatesh, "Optimal patching in clustered malware epidemics," *arXiv preprint arXiv:1403.1639*, 2014.

[17] N. Falliere, L. O. Murchu, and E. Chien, "W32. stuxnet dossier," *White paper, Symantec Corp., Security Response*, 2011.

[18] G. Feichtinger, R. F. Hartl, and S. P. Sethi, "Dynamic optimal control models in advertising: recent developments," *Management Science*, vol. 40, no. 2, pp. 195–226, 1994.

[19] M. Garetto, W. Gong, and D. Towsley, "Modeling malware spreading dynamics," in *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*, vol. 3. IEEE, 2003, pp. 1869–1879.

[20] K. J. Hall, "Thwarting network stealth worms in computer networks through biological epidemiology," Ph.D. dissertation, Citeseer, 2006.

[21] W. H. Hamer, *The Milroy lectures on epidemic disease in England: the evidence of variability and of persistency of type*. Bedford Press, 1906.

[22] H. W. Hethcote and P. Waltman, "Optimal vaccination schedules in a deterministic epidemic model," *Mathematical Biosciences*, vol. 18, no. 3, pp. 365–381, 1973.

[23] IFRC, "The link between tuberculosis and hiv."

[24] B. Karrer and M. Newman, "Competing epidemics on complex networks," *Physical Review E*, vol. 84, no. 3, p. 036106, 2011.

[25] W. Kendall and I. Saunders, "Epidemics in competition ii: the general epidemic," *Journal of the Royal Statistical Society. Series B (Methodological)*, pp. 238–244, 1983.

[26] J. O. Kephart and S. R. White, "Directed-graph epidemiological models of computer viruses," in *Research in Security and Privacy, 1991. Proceedings., 1991 IEEE Computer Society Symposium on*. IEEE, 1991, pp. 343–359.

[27] M. Khouzani, S. Sarkar, and E. Altman, "Dispatch then stop: Optimal dissemination of security patches in mobile wireless networks," in *IEEE CDC'10*, 2010, pp. 2354–2359.

[28] ——, "Optimal control of epidemic evolution," in *IEEE INFOCOM*, 2011.

[29] M. Khouzani and S. Sarkar, "Maximum damage battery depletion attack in mobile sensor networks," *Automatic Control, IEEE Transactions on*, vol. 56, no. 10, pp. 2358–2368, 2011.

[30] M. Khouzani, S. Sarkar, and E. Altman, "Maximum damage malware attack in mobile wireless networks," *IEEE/ACM Transactions on Networking (TON)*, vol. 20, no. 5, pp. 1347–1360, 2012.

[31] J. Kim, S. Radhakrishnan, and S. K. Dhall, "Measurement and analysis of worm propagation on internet network topology," in *Computer Communications and Networks, 2004. ICCCN 2004. Proceedings. 13th International Conference on*. IEEE, 2004, pp. 495–500.

[32] T. Kurtz, "Solutions of ordinary differential equations as limits of pure jump markov processes," *Journal of Applied Probability*, pp. 49–58, 1970.

[33] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *Security & Privacy, IEEE*, vol. 9, no. 3, pp. 49–51, 2011.

[34] F. Li, Y. Yang, and J. Wu, "Cpmc: an efficient proximity malware coping scheme in smartphone-based mobile networks," in *INFOCOM, 2010 Proceedings IEEE*. IEEE, 2010, pp. 1–9.

[35] Y. Li, P. Hui, D. Jin, L. Su, and L. Zeng, "Optimal distributed malware defense in mobile networks with heterogeneous devices," *Mobile Computing, IEEE Transactions on*, vol. 13, no. 2, pp. 377–391, 2014.

[36] Y. Li, Y. Jiang, D. Jin, L. Su, L. Zeng, and D. O. Wu, "Energy-efficient optimal opportunistic forwarding for delay-tolerant networks," *Vehicular Technology, IEEE Transactions on*, vol. 59, no. 9, pp. 4500–4512, 2010.

[37] Y. Li, Z. Wang, D. Jin, L. Zeng, and S. Chen, "Collaborative vehicular content dissemination with directional antennas," *Wireless Communications, IEEE Transactions on*, vol. 11, no. 4, pp. 1301–1306, 2012.

[38] A. Lindgren, A. Doria, and O. Schelén, "Probabilistic routing in intermittently connected networks," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 7, no. 3, pp. 19–20, 2003.

[39] X. Lu and P. Hui, "An energy-efficient n-epidemic routing protocol for delay tolerant networks," in *Networking, Architecture and Storage (NAS), 2010 IEEE Fifth International Conference on*. IEEE, 2010, pp. 341–347.

[40] Z. Lu, W. Wang, and C. Wang, "How can botnets cause storms? understanding the evolution and impact of mobile botnets."

[41] H. Malchow, S. V. Petrovskii, and E. Venturino, *Spatiotemporal patterns in ecology and epidemiology: theory, models, and simulation*. Chapman & Hall/CRC Press London, 2008.

[42] J. Mickens and B. Noble, "Modeling epidemic spreading in mobile environments," in *Proceedings of the 4th ACM Workshop on Wireless Security*. ACM, 2005, pp. 77–86.

[43] R. Morton and K. Wickwire, "On the optimal control of a deterministic epidemic," *Advances in Applied Probability*, pp. 622–635, 1974.

[44] W. H. Murray, "The application of epidemiology to computer viruses," *Computers & Security*, vol. 7, no. 2, pp. 139–145, 1988.

[45] G. Neglia and X. Zhang, "Optimal delay-power tradeoff in sparse delay tolerant networks: a preliminary study," in *Proceedings of the 2006 SIGCOMM workshop on Challenged networks*. ACM, 2006, pp. 237–244.

[46] S. Nelson, M. Bakht, and R. Kravets, "Encounter-based routing in dtns," in *INFOCOM 2009, IEEE*. IEEE, 2009, pp. 846–854.

[47] H. Nguyen and Y. Shinoda, "A macro view of viral propagation and its persistence in heterogeneous wireless networks," in *Fifth International Conference on Networking and Services*. IEEE, 2009, pp. 359–365.

[48] K. Ramachandran and B. Sikdar, "Modeling malware propagation in networks of smart cell phones with spatial dynamics," in *IEEE INFOCOM'07*, 2007, pp. 2516–2520.

[49] D. Sanger, "Obama order sped up wave of cyberattacks against iran," *New York Times*, June 1st, 2012.

[50] H. C. Schramm and D. P. Gaver, "Lanchester for cyber: The mixed epidemic-combat model," *Naval Research Logistics (NRL)*, vol. 60, no. 7, pp. 599–605, 2013.

[51] S. P. Sethi, "Dynamic optimal control models in advertising: a survey," *SIAM review*, vol. 19, no. 4, pp. 685–725, 1977.

[52] S. P. Sethi and G. L. Thompson, *Optimal control theory: applications to management science and economics*. Kluwer Academic Publishers Boston, 2000, vol. 101.

[53] C. Singh, A. Kumar, and R. Sundaresan, "Delay and energy optimal two-hop relaying in delay tolerant networks," in *Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt), 2010 Proceedings of the 8th International Symposium on*. IEEE, 2010, pp. 256–265.

[54] C. Singh, A. Kumar, R. Sundaresan, and E. Altman, "Optimal forwarding in delay tolerant networks with multiple destinations," in *Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt), 2011 International Symposium on*. IEEE, 2011, pp. 228–235.

[55] T. Spyropoulos, K. Psounis, and C. Raghavendra, "Spray and wait: an efficient routing scheme for intermittently connected mobile networks," in *Proceedings of the 2005 ACM SIGCOMM workshop on Delay-tolerant networking*. ACM, 2005, pp. 252–259.

[56] A. Vahdat, D. Becker *et al.*, "Epidemic routing for partially connected ad hoc networks," Technical Report CS-200006, Duke University, Tech. Rep., 2000.

[57] P. Wang, M. C. González, C. A. Hidalgo, and A.-L. Barabási, "Understanding the spreading patterns of mobile phone viruses," *Science*, vol. 324, no. 5930, pp. 1071–1076, 2009.

[58] Y. Wang and H. Wu, "DFT-MSn: The delay fault tolerant mobile sensor network for pervasive information gathering," in *INFOCOM, Proceedings of IEEE*, 2006, pp. 1021–1034.

[59] L. Weng, A. Flammini, A. Vespignani, and F. Menczer, "Competition among memes in a world with limited attention," *Scientific Reports*, vol. 2, 2012.

[60] K. Wickwire, "Optimal isolation policies for deterministic and stochastic epidemics," *Mathematical biosciences*, vol. 26, no. 3, pp. 325–346, 1975.

[61] ——, "Optimal control policies for reducing the maximum size of a closed epidemic : I. deterministic dynamics," *Mathematical Biosciences*, vol. 30, no. 1, pp. 129–137, 1976.

[62] Y. Yang, S. Zhu, and G. Cao, "Improving sensor network immunity under worm attacks: a software diversity approach," in *Proceedings of the 9th ACM international symposium on Mobile ad hoc networking and computing*. ACM, 2008, pp. 149–158.

[63] K. Zetter, "Digital detectives deciphered stuxnet, the most menacing malware in history," *Wired Magazine*, 2011.

[64] X. Zhang, G. Neglia, J. Kurose, and D. Towsley, "Performance modeling of epidemic routing," *Computer Networks*, vol. 51, no. 10, pp. 2867–2891, 2007.

[65] C. C. Zou, W. Gong, and D. Towsley, "Code red worm propagation modeling and analysis," in *Proceedings of the 9th ACM conference on Computer and communications security*. ACM, 2002, pp. 138–147.

[66] G. Zyba, G. Voelker, M. Liljenstam, A. Méhes, and P. Johansson, "Defending mobile phones from proximity malware," in *INFOCOM 2009, IEEE*. IEEE, 2009, pp. 1503–1511.