

Optimal Malware Attack and Defense in Mobile Wireless Networks

M.H.R Khouzani

I. 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 [1]), or even alter the network traffic and hence destroy the integrity of the information, such as unauthorized access and session hijacking attacks [2], [3]. Malware outbreaks like those of Slammer [4] and Code Red [5] 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 [6]. Recognizing the above, specific attacks such as the wormhole [7], sinkhole [1], and Sybil [8], that utilize vulnerabilities in the routing protocols in a wireless sensor network, and their counter-measures, have been investigated before they were actually launched. In this dissertation research, we pursue the complementary but closely related goals of (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 [9], 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. While identifying fundamental limits of the attack (defense, respectively), we assume that the counter-measure (attack, respectively) parameters are chosen statically and are known to the attack (defense, respectively).

The last step in the investigation is to determine the attack and counter-measure policies when both are chosen dynamically, and reactively (i.e., in response to each other).

II. SYSTEM STATE EVOLUTION

Worms spread during data or control message transmission from nodes that are infected (*infectives*) 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 [10] could re-flesh 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 [11], while StackGuard programs [12] immunize the susceptibles by removing the buffer overflow vulnerability that the worms exploit, specialized security patches [13] 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.

III. 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 cognisant of the counter-measures [14]. Killing an infective host sooner rather than later maximally 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. 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. It is therefore interesting to determine the instantaneous rate of killing that maximizes the damage inflicted by the worm.

Another important decision of the worm pertains to its optimal use of the available energy of the infective nodes. 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 choice however depletes their energy reserves which are limited as those of any other nodes in wireless networks, which in turn limits the spread of the infection and also their other functionalities such as eavesdropping, traffic destruction, *etc.*

IV. DECISION PROBLEMS OF THE DEFENSE

The counter-measure focuses 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 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 frequency of contacts between the mobile nodes and thus suppress the spread of the infection. 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 [15]. Such a trade-off also exists in the case of a mobile wireless network: reducing the communication range of nodes can deteriorate the QoS offered by the network, as the end-to-end communication delay increases. 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 tradeoff between QoS and damage due to infection.

The susceptible nodes can be immunized and infectives can be healed through security patches. However, the distribution of the patch relies on the same resources of the network. Hence, the propagation and dispatching of a security patch, if not carefully controlled, 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 [16], [17]. 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 crashing and slowing systems. An important decision problem of the counter-measure is to decide the rate at which such security patches should be propagated 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 stationary) 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-propagative* and *propagative* patchings. The decision of the defense policy is that at each given time, what portion of the propagators of the security patch, or *patchers*, are activated, and the rates at which they should transmit the security patches. Activation of more of such nodes and increase of their rates of transmission accelerates the spread of the security patch, however, at the expense of consuming underlying resources of the mobile wireless network such as the ever-demanded bandwidth, battery and process time of the nodes.

V. SUMMARY OF THE RESULTS ALREADY OBTAINED

A. Formulation of maximum damage attack

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 [18]. 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. We allow the function to be fairly general, in that it can be either linear or non-linear, and consider that the worm seeks to maximize the damage subject to satisfying certain constraints on the energy consumption of its hosts by dynamically selecting its killing rates and energy usages of its hosts 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 turns out to be an elegant optimal control problem which can be solved numerically by applying Pontryagin's Maximum Principle [19]–[21] - an effective tool that so far has been rarely used in the context of network security. Both the formulation and the tools constitute novel contributions in this context.

Second, we seek to 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 are surprising and 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. We first investigate the case where the worm selects the killing rates dynamically and the energy consumption strategies statically (i.e., once at the beginning of network operation). We prove that the optimal killing rate has the following simple structure: 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. Thus, 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 to no disruptive behavior might well be stacking infective hosts for the imminent carnage. In optimal control terminology [19]–[21], we have proved that the optimal strategy has a *bang-bang* structure, that is, at any given time, the killing rate is either at its minimum or maximum possible values, and has at most one jump which necessarily culminates at the maximum possible value. Optimality of this simple strategy for this nontrivial problem is in fact quite surprising.

We next investigate the complementary problem where the worm selects only the optimal energy consumption rate dynamically. We prove that when the energy consumption costs are 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. Our numerical computations reveal that when both the killing rates and energy usages are selected dynamically, the optimal strategies follow the above structures as well.

B. Formulation of the Maximum Efficacy Countermeasure

1) *Reception Gain Reduction*: 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. Using Pontryagin’s Maximum Principle, we devise a framework for computing the optimal communication range as a function of infection level in the network. We identify several structural characteristics of the optimal solution by examining the analytical properties of the solution for different classes of the cost function [22], [23].

2) *Immunization*: We first construct a mathematical framework which models the effect of the decisions of the defense policy on the dynamics of the spread of the worm and their resulting trade-offs through a combination of epidemic models

and a cost function [24]. As in the attack model, the cost inflicted by the worm is a cumulative function increasing in the number of infected and dead hosts, both of which change with time. The network administrator seeks to minimize the cost by dynamically selecting the activation rate of the patchers assuming knowledge of the network parameters and the propagation parameters of the worm. The cost minimization problem is cast as an optimal control problem which can be solved numerically by applying Pontryagin’s Maximum Principle.

Second, we investigate whether the optimal policies that inflict the above minimum cost are complex to execute, which could turn them impractical to implement in reality. Towards this end, we investigate structures of the optimum policies for the defense. Our results are promising: we show that minimum overall cost is archived by executing very simple strategies. In both non-propagative and propagative models, we prove that the optimal activation of dispatchers has the following simple structure: until a certain time (which can be the end time depending on the network and worm parameters), the activation is performed with maximum rate and right after that till the end of the period, no dispatcher is activated. In optimal control terminology, we have proved that the optimal strategy has a *bang-bang* structure, that is, at any given time, the activation rate is either at its minimum or maximum possible values, and has at most one jump which necessarily terminates at the minimum possible value, which is zero. Again, the optimality of this simple strategy for this nontrivial problem is indeed surprising.

VI. FUTURE RESEARCH AGENDA

We propose to explore the scenario in which both the malware and the network operator select their control parameters dynamically. The evolution of the states of the network depends on their decisions jointly. Malware and Network are thus *players* in a (finite time) *non-cooperative differential game*, where each one of them seek to maximize their personal *payoffs*.

We will try to identify the Nash Equilibria, and the structural properties of optimal *strategies* in a Nash Equilibrium, through analysis and/or numerical computations.

VII. RELATED LITERATURE

Detection and containment of malware in mobile networks from a practical viewpoint, one can consult with [25]. [26] combined a deterministic worm propagation model with a game theoretic process that involves learning, in order to incorporate decisions of users about whether or not to install a security patch in a wired network. [27] introduces heuristic strategies for dynamically adjusting the transmission power of attacker nodes in wireless networks.

Controlling the spread of the worm by reducing the rate of communication of nodes (i.e., rate-control-based measures) [28], [29], or the number of communications [30], are the closest analogs in the wired networks to reducing the communication range of the nodes in the wireless networks. The work in [28] is based on heuristics and simulations. [29] only considers a static choice of the reduced communication

rate, whereas we allow the communication range of the nodes to be dynamically modified over time as the level of infection evolves. [30] proposes a worm containment strategy which limits the total number of distinct contacts per node over the containment cycle. However, this work only applies to the initial phase of infection and their countermeasure is ineffective once the epidemic starts. [31] and [32] consider both propagative and non-propagative patching where the parameters are fixed and investigates the final (respectively, maximum) number of the infective in the system as the performance metric of the patching scheme. However, the patching rate is assumed constant, whereas in our model, we consider dynamic patching policy and a general cost.

Interestingly, tools from the optimal control theory such as the effective theorem of Pontryagin maximum Principle has rarely been used for analyzing network security. Optimal control has been applied in [33] for a delay tolerant energy-constrained wireless network with two-hop routing where a single source tries to transmit a packet to a destination before a deadline. [33] shows that the optimal transmission and activation policies follow a threshold-based structure (i.e. are bang-bang with one jump only.) However, the dynamics of the number of *infective* nodes (i.e. nodes which have received the packet) is not representative of an epidemic behavior (due to the restriction of a two-hop routing assumption) and thus their results cannot be applied in our context. [34] considers a similar setting and investigates epidemic model as well as a two-hop model and provides the optimal forwarding rate of messages to follow a bang-bang rule as well. However, the results are shown for a *monotonic* epidemic model, which means that none of the infectives loose their infection. In contrast, in the context of security, we ought to assume that there are countermeasure mechanisms which remove the infection, apart from possible mortality.

REFERENCES

- [1] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," *Ad Hoc Networks*, vol. 1, no. 2-3, pp. 293–315, 2003.
- [2] D. Welch and S. Lathrop, "Wireless security threat taxonomy," in *Information Assurance Workshop, 2003. IEEE Systems, Man and Cybernetics Society*, pp. 76–83, 2003.
- [3] A. Herzog, N. Shahmehri, and C. Duma, "An ontology of information security," *International Journal of Information Security and Privacy*, vol. 1, no. 4, pp. 1–23, 2007.
- [4] D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, and N. Weaver, "Inside the slammer worm," *IEEE Security & Privacy*, vol. 1, no. 4, pp. 33–39, 2003.
- [5] 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*, pp. 138–147, ACM New York, NY, USA, 2002.
- [6] E. Filiol, M. Helenius, and S. Zanero, "Open problems in computer virology," *Journal in Computer Virology*, vol. 1, no. 3, pp. 55–66, 2006.
- [7] Y. Hu, A. Perrig, and D. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," in *IEEE INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies*, vol. 3.
- [8] J. Douceur, "The sybil attack," in *Peer-to-Peer Systems, First International Workshop, IPTPS 2002, Cambridge, MA, USA, March 7-8, 2002, Revised Papers*, pp. 251–260.
- [9] J. Walters, Z. Liang, W. Shi, and V. Chaudhary, "Wireless sensor network security: A survey," *Security in Distributed, Grid, Mobile, and Pervasive Computing*, p. 367, 2007.
- [10] F.-S. C. T. Page, "F-secure virus descriptions : Cih." <http://www.f-secure.com/v-descs/cih.shtml>.
- [11] D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, and N. Weaver, "Inside the slammer worm," *IEEE Security & Privacy*, vol. 1, no. 4, pp. 33–39, 2003.
- [12] C. Cowan, C. Pu, D. Maier, H. Hinton, J. Walpole, P. Bakke, S. Beattie, A. Grier, P. Wagle, and Q. Zhang, "StackGuard: Automatic adaptive detection and prevention of buffer-overflow attacks," in *Proceedings of the 7th USENIX Security Conference*, vol. 78, San Antonio: USENIX Press, 1998.
- [13] Symantec, "W32.sqlslp.worm," (02.13.2007).
- [14] N. Weaver and V. Paxson, "A worst-case worm," in *Proc. Third Annual Workshop on Economics and Information Security (WEIS04)*, 2004.
- [15] N. Ries, "Public health law and ethics: lessons from SARS and quarantine," *Health Law Review*, vol. 13, no. 1, pp. 3–6, 2004.
- [16] E. Schultz, "The MSBlaster worm: going from bad to worse," *Network Security*, vol. 2003, no. 10, pp. 4–8, 2003.
- [17] F. Castaneda, E. Sezer, and J. Xu, "WORM vs. WORM: preliminary study of an active counter-attack mechanism," in *Proceedings of the 2004 ACM workshop on Rapid malware*, pp. 83–93, ACM New York, NY, USA, 2004.
- [18] M. Khouzani, S. Sarkar, and E. Altman, "Maximum Damage Malware Attack in Mobile Wireless Networks," *To appear in Infocom 2010*.
- [19] D. Grass, A. Vienna, J. Caulkins, and P. RAND, *Optimal Control of Nonlinear Processes*. Springer-Verlag Berlin Heidelberg, 2008.
- [20] D. Kirk, *Optimal Control Theory: An Introduction*. Prentice Hall, 1970.
- [21] A. Seierstad and K. Sydsaeter, *Optimal control theory with economic applications*. 1986.
- [22] M. Khouzani, E. Altman, and S. Sarkar, "Optimal Quarantining of Wireless Malware Through Power Control," in *Proceedings of the Fourth Symposium on Information Theory and Applications*, University of California at San Diego, 2009.
- [23] M. Khouzani, S. Sarkar, and E. Altman, "Optimal Quarantining of Wireless Malware Through Power Control," *Submitted to TAC*.
- [24] M. Khouzani, S. Sarkar, and E. Altman, "Optimum Dispatching in Mobile Wireless Networks," *Preprint*.
- [25] A. Bose, "Propagation, Detection and Containment of Mobile Malware," 2008.
- [26] G. Theodorakopoulos, J. Baras, and J. Le Boudec, "Dynamic Network Security Deployment Under Partial Information," in *Communication, Control, and Computing, 2008 46th Annual Allerton Conference on*, pp. 261–267, 2008.
- [27] V. Karyotis and S. Papavassiliou, "Risk-based attack strategies for mobile ad hoc networks under probabilistic attack modeling framework," *Computer Networks*, vol. 51, no. 9, pp. 2397–2410, 2007.
- [28] M. Williamson, "Throttling viruses: restricting propagation to defeat malicious mobile code," in *Computer Security Applications Conference, 2002. Proceedings. 18th Annual*, pp. 61–68, 2002.
- [29] C. Wong, C. Wang, D. Song, S. Bielski, and G. Ganger, "Dynamic Quarantine of Internet Worms," in *The International Conference on Dependable Systems and Networks (DSN-2004)*, pp. 62–71, 2004.
- [30] S. Sellke, N. Shroff, and S. Bagchi, "Modeling and Automated Containment of Worms," *Dependable and Secure Computing, IEEE Transactions on*, vol. 5, no. 2, pp. 71–86, 2008.
- [31] M. Vojnović and A. Ganesh, "On the effectiveness of automatic patching," in *Proceedings of the 2005 ACM workshop on Rapid malware*, pp. 41–50, ACM New York, NY, USA, 2005.
- [32] S. Shakkottai and R. Srikant, "Peer to peer networks for defense against internet worms," in *Proceedings from the 2006 workshop on Interdisciplinary systems approach in performance evaluation and design of computer & communications systems*, ACM New York, NY, USA, 2006.
- [33] E. Altman, A. Azad, T. Basar, and F. De Pellegrini, "Optimal activation and transmission control in delay tolerant networks," *available on Arxiv (arXiv: 0907.4329)*.
- [34] E. Altman, T. Basar, and F. Pellegrini, "Optimal monotone forwarding policies in delay tolerant mobile ad-hoc networks," *Proc. of ACM InterPerf*, 2008.