Slowing the Spread of Bluetooth-based Malware in Mobile Tactical Networks

Brian Thompson
U.S. Army Research Lab
Adelphi, MD 20783
Email: bthompso8784@gmail.com

James Morris-King
U.S. Army Research Lab
Adelphi, MD 20783
Email: james.r.morris-king.ctr@mail.mil

Richard Harang
U.S. Army Research Lab
Adelphi, MD 20783
Email: richard.e.harang.civ@mail.mil

***Abstract*—Cyber-attacks in mobile tactical networks are increasingly being recognized as a threat to mission assurance and tactical capability. Some recent cyber-attacks have exploited short-range radio communication such as Bluetooth to propagate malware, thereby circumventing traditional cyber network defenses and evading detection. The spread of such self-propagating malware in mobile tactical networks is strongly impacted by the spatio-temporal properties of networked devices. In this paper, we use a hierarchical model to represent the coordinated, structured movement of military units, and evaluate the effectiveness of several defensive strategies in slowing the spread of Bluetooth-based malware using agent-based simulation.**

I. Introduction

Mobile tactical networks (MTNs) have become ubiquitous in military operations, supporting communication, coordination, and information dissemination among human and autonomous assets [1], [2]. MTNs are decentralized and heterogeneous, often consisting of a mix of mobile devices, sensors, human and vehicle-mounted computing and communication platforms, and autonomous robotic assets [3]. MTNs may take the form of ad-hoc or mesh networks, where individual nodes are mobile, transient, and rely on unstable communication links. Achieving security across such a diverse collection of devices in an evolving battlefield is challenging. In addition, understanding the effects of complex cyber defense policies in such an environment is difficult since few tools exist which properly capture the underlying dynamics of MTNs. As new, stealthy malware attacks arise which exploit trusted or unwatched channels to propagate via close contact between vulnerable devices, the need to develop relevant defense at the tactical edge has become paramount.

Approaches for controlling malware include discouraging or blocking communication over unsecured channels, avoiding high-contact situations between susceptible devices, increasing the number of well defended cyber nodes, and enforcing compliance with cyber best practices. These approaches can be achieved through a mix of policy and technical solutions. The impact, as well as the cost and capability trade-offs, of enacting these defensive measures in realistic scenarios is difficult to gauge. For example, the effectiveness of an anti-malware policy which requires all non-essential digital devices to be powered off when entering a base depends on the level of compliance, a human factor. A technical solution such as location-sensing hardware and software which achieves the same goal may be prohibitively expensive to deploy and yield unintended negative externalities in practice. These sorts of challenges quickly exceed the scope of traditional modeling efforts and require new solutions.

Agent-based simulation is a powerful modeling methodology which leverages the actions and interactions of autonomous agents (either individually or collectively) to assess their effects on a dynamic system. The hierarchical spatial structures which facilitate malware transmission in MTNs arise from the dynamic interaction of humans, machines, communication protocols, and policy. As demonstrated in [4], the interplay between such structured mobility patterns and proximity-based propagating malware cannot be easily captured by traditional mathematical models for epidemic disease spread.

In this paper, we study the effectiveness of various defensive strategies in slowing the spread of malware through an MTN consisting of users carrying vulnerable mobile devices (such as phones, tablets, or laptops). We focus on malware designed to propagate quickly using short-range radio communication that is difficult to detect by traditional host-based processes, since this situation represents a worst-case scenario for battlefield operations. We seek to answer the following questions:

- What defensive strategies can help slow the spread of malware in mobile tactical networks?
- How does the level of adoption of a defensive policy or technology impact its effectiveness?
- What is the trade-off between the effectiveness of each strategy in combating malware and its detrimental effects on other capabilities?

We answer these questions using agent-based simulation of an MTN suffering a viral malware epidemic over Bluetooth communication services. We consider a scenario in which infantry squads equipped with Bluetooth-enabled devices perform reconnaissance and peace-keeping operations on a synthetic battlefield. Our agent model reflects the hierarchical properties of the tactical edge including a military inspired unit structure and communication model. Our contributions are (1) design and implementation of an agent-based model representing hierarchical mobility patterns, Bluetooth communication, self-propagating malware, and defensive strategies in a synthetic battlefield, and (2) evaluation and comparison of the effectiveness of various defensive strategies in slowing malware spread. The remainder of the paper is organized as follows: Section II presents related work. Section III discusses

our model for synthetic battlefield simulation and Bluetooth worm propagation. Section IV describes our simulation experiments and presents the results. Section V concludes the work and suggests future research.

II. Related Work

A. Mobile Network Defense

From the perspective of complex network theory the dynamic topology of an MTN is a clear-cut example of hierarchical spatial networks [5], [6]. The behavior of nodes in an MTN is strongly affected by terrain features, the presence of friendly or adversary units, and the parameters of the mission. Malware, especially computer worms, are an open threat to these networks which increasingly incorporate off-the-shelf technologies with widely publicized vulnerabilities which can be targeted by a determined adversary.

While general approaches to MTN defense are discussed in [7], [8], [9], [10], we focus on an epidemiological view of mobile network worm defense raised in [11]. Typically, worms spread during data or control message transmission from mobile nodes that are infected (infectives) and those that are vulnerable, but not yet infected (susceptibles). Depending on the attack goals and exploit pattern (wormhole, sinkhole, system crash, eavesdropping, spoofing, etc.), different defensive measures should be enacted [12], [13]. Counter-measures, such as security patches, can be launched either by automated process or by users. These countermeasures may operate at one or many layers of the MTN (physical, network, user, etc.), but are typically implemented as one of the following actions: blocking/quarantining, healing, or immunization [14]. Indeed, the application of epidemic control to network defense has typically focused on implementing some version of the previously mentioned actions [15], [16], [17]. While this metaphor is useful, it fails to capture strategies which focus on modifying behavior to avoid exposure to malware in the first place, rather than reacting to the infection itself.

B. Bluetooth Malware

While numerous examples of malware targeting mobile platforms exist, a select few have been observed which take advantage of security gaps in Bluetooth protocols to penetrate systems, gain control of critical services, and propagate the attack to nearby devices [18], [19], [20], [21], [22]. This sort of attack exploits the fact that Bluetooth radio is rarely observed by network security monitors and host-based security tools [23].

Su et al. use trace-drive simulations drawn from real life sampling of over 10,000 devices in a commuter train station to examine the propagation dynamics of Bluetooth worms, showing that Bluetooth worms can infect a large population of vulnerable devices relatively quickly, in just a few days [24]. Wang et al. model the mobility of mobile phone users to study the spreading patterns of a theoretical Bluetooth worm, noting that while infection time is low, discovery time for susceptible targets is slow and strongly influenced by individual mobility patterns (i.e. the contact rate between susceptible carriers is low) [25]. Gao and Liu study a two-layer virus-propagation model for smartphone networks (Bluetooth and SMS) [26], finding that Bluetooth is an effective transport medium for targeting hosts less likely to respond to tainted SMS communications. [27], [28], [14], [29], [30] present surveys of mobile malware threats, including emergent multi-function worms. In these examples, Bluetooth security is treated as an effective, unwatched gateway for an attacker to take full ownership of a target system.

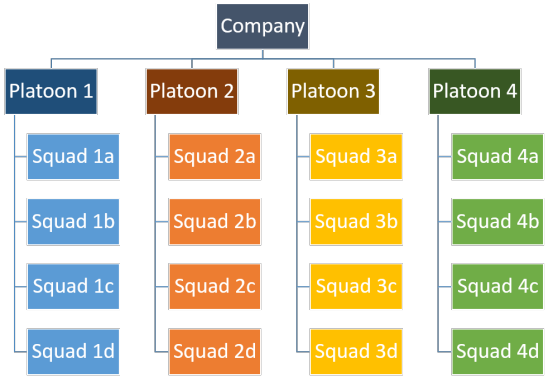


Fig. 1: Unit hierarchy in our model. A company contains four platoons, each of which contains four squads.

One common approach in the aforementioned theoretical studies of Bluetooth worms is the reliance on compartment models for simulation which do not account for the emergent dynamics in mobile networks. In our survey we found little relevant literature which explores these dynamics in military networks using agent-based simulation. Yang et al. and Gao et al. show that such differential equation models greatly overestimate the epidemic spreading speed due to their implicit homogeneous mixing assumption and lack of user models [31], [32]. Moreover, military units are often deployed in areas deemed unsuitable for civilian telecommunication networks, meaning that MTNs exhibit higher degree of network sparseness even before accounting for environmental or adversarial disruption. Likewise, military units shift between predictable, highly planned activities, such as ordered group movement, and reactive, sometimes chaotic activity. These properties make mathematical models which generalize behavior and mobility unsuitable for modeling the propagation of malware in MTNs.

III. Methods

A. Model

In order to study the propagation of malware in a MTN, we develop an agent-based model to represent the mobility patterns of military units. We base the organizational structure of our model on the U.S. Army's unit hierarchy. A company in the U.S. Army is usually made up of three to five platoons, and a platoon typically consists of two to four squads of 8-10 soldiers each, depending on each unit's type and designated function [33]. For simplicity, we do not distinguish between different types of companies, platoons, or squads; we model a company as consisting of four platoons, each containing four squads. Because soldiers in a squad typically stay in close physical proximity to one another, for the purpose of this paper we consider the squad to be an atomic unit and do not model behavior at the scale of individual soldiers. Figure 1 illustrates the unit hierarchy used in our model.

Each squad takes actions according to mission directives assigned by its commanding unit. Mission directives flow from the highest to the lowest levels of the military hierarchy, at each level adding greater specificity in support of the larger mission. In particular, we consider a scenario in which several companies are stationed at outposts around the periphery of a town harboring enemy soldiers. Their mission, as given to them by their superiors in the chain of command, is to secure the town by conducting excursions into the town seeking out and engaging with enemy soldiers. After resting at its designated outpost for some amount of time, a platoon leader will choose a target location in the town, and all squads in that platoon will travel to the location together. Once there, each squad will operate independently following the instructions of its squad leader, spreading out from the other squads in the platoon in order to cover more ground as they investigate the nearby area. After some period of time, the platoon leader will instruct the squads to return to their company's outpost to rest before being sent out again.

Each soldier carries a mobile device that facilitates short-range wireless communication, such as Bluetooth, on the battlefield. Each device regularly scans the environment for other nearby devices. When two devices come within communication range, they automatically connect, enabling data transmission. Due to its prevalence among mobile devices, we base our implementation on Bluetooth technology and will use that as our running example.

In an attempt to infiltrate the allied cyber network, the enemy plants a device infected with a self-propagating Bluetooth worm somewhere in the town. When a soldier comes within communication range of an infected device – either the planted enemy device or an already-infected device carried by a friendly soldier – the two devices connect and the malware spreads to the soldier's device. Figure 2 gives a screenshot of the simulation environment in Repast Simphony, the agent-based modeling and simulation platform we use for our experiments.

B. Defensive Strategies

We consider three classes of defensive strategies, consecutively more robust but potentially also more costly or inconvenient:

- Fortified Outposts: Resources are allocated to prevent malware from spreading to or from devices carried by units located at an outpost.
- Fortified Noncombat: Resources are allocated to prevent malware from spreading to or from devices carried by units that are not currently in combat (i.e. at an outpost or in transit).
- Fortified Always: Resources are allocated to prevent malware from spreading to or from devices carried by units at all times.

The intuition behind protecting outposts is that the high concentration of units in a small space facilitates the rapid propagation of malware. This is also the least likely time that Bluetooth communication would be necessary from a tactical perspective, so implementations of this strategy based on preventing Bluetooth communication entirely may not be unreasonable. Another high-risk time for malware spread is when units are in transit to or from a combat operation, since they may cover a lot of ground in a short period of time, increasing their likelihood of interacting with other units along the way. Finally, while being the most robust solution, protecting units at all times may interfere with the potentially valuable benefits of improving short-range communication between units in combat situations.

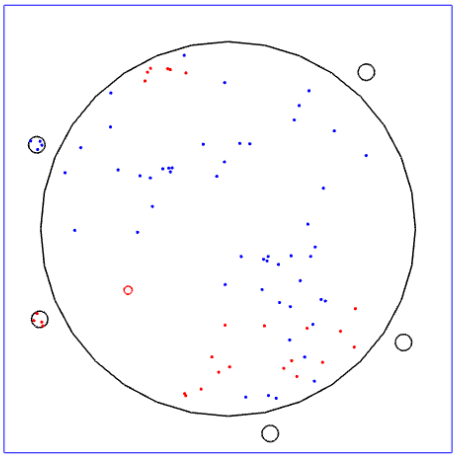


Fig. 2: Simulation environment in Repast Simphony. The large circle represents a town, the smaller circles around the town's periphery represent outposts, and the red circle represents the range of an infected enemy device. Squads are initially blue, and become red when infected, which occurs when they come within range of the infected enemy device or an already-infected squad.

In the following section, we evaluate the effectiveness of these strategies in slowing the spread of Bluetooth-based malware.

IV. Evaluation

A. Experimental Setup

We develop and implement a discrete-time agent-based simulation in Java based on the model presented in Section III-A. We use a two-dimensional spatial model and do not account for signal attenuation, reflection, nor other wireless phenomena. All experiments were conducted on an Intel Core i7 processor operating at 2.40 GHz with 16 GB of memory running Windows 10.

We consider the equivalent of five companies, or 80 squads, operating in a circular town of radius 500 m (area $\approx 785,398m^2$). Squads move at a maximum speed of 1 m/s. Mobile devices have a transmission range of 9.0 meters, a typical range for a Bluetooth signal in an unobstructed environment.

Simulations were run for 3,600 time steps, corresponding to a period of 12 hours to represent the activities of a typical day, with data collected at time intervals of $\Delta t = 12$ seconds. Results were averaged over 100 independent trials.

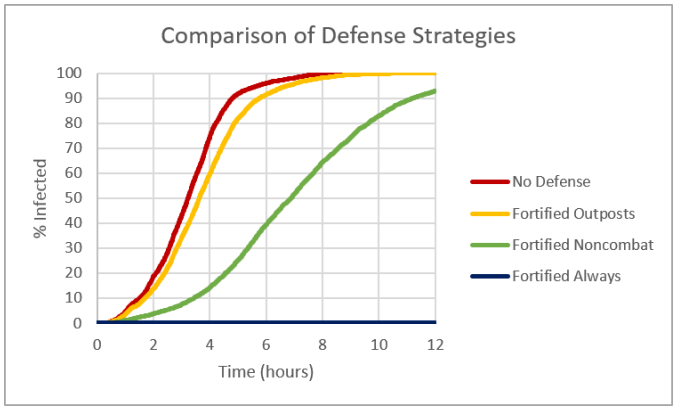


Fig. 3: Progress of the malware over time under each defensive strategy, in terms of the fraction of infected nodes.

B. Results

We now present our results comparing the effectiveness of the different strategies in slowing the spread of malware. For a baseline, we also evaluate the spread of malware when no defensive strategy is used.

Figure 3 shows the progression of the malware over time under each of the defensive strategies. The plot of the baseline No Defense strategy has the expected sigmoidal shape commonly observed when studying infectious disease spread through a population, indicating an initial exponential spread which slows down as the infection reaches the saturation point.

Despite the high concentration of units at the outposts, we see that Fortified Outposts provides little improvement over the baseline. This may be because squads are most likely to coincide at an outpost with other squads in their platoon, for which there are ample other times for them to interact and spread the malware when they are not at the outpost. This would likely be different if the simulation included nights, during which all of the squads in a company are at the outpost simultaneously.

The Fortified Noncombat strategy, on the other hand, shows significant improvement over the baseline in slowing the spread of the malware, taking almost 7 hours to reach 50% infection as opposed to about 3 hours when no defensive strategy is used. Perhaps even more surprisingly, the infection curve is nearly linear rather than sigmoidal. This is less surprising, however, when considering that the small local movements of units during combat do not fit the typical homogeneous mixing assumption common to the infectious disease literature.

The Fortified Always strategy trivially achieves 0% infection because none of the units are susceptible to the malware. In practice, however, this may be hard to achieve due to logistical reasons, imperfect compliance with military policies, or the prohibitive monetary or temporal cost of maintaining up-to-date and robust security technology. Next, we consider the effectiveness of the defensive strategies when 100% adoption is not feasible.

Figure 4 shows the progression of the malware over time when only 20%, 40%, 60%, and 80% of the units are implementing a given strategy. Although the Fortified Outposts strategy does now show significant improvement with greater adoption, we see a significant flattening of the infection curves for the Fortified Noncombat and Fortified Always strategies. This is even more pronounced for the Fortified Always strategy because in addition to breaking the homogeneous mixing assumption as mentioned above, it lowers the upper bound of possible infected units because a fortified device will never get infected, and at the same time decreases the density–and therefore the interaction rate–of susceptible units. As a result, the marginal benefit of fortifying additional units *increases* as more units are fortified. This is clearly demonstrated by the plot in Figure 5, which shows the time until 50% infection increases super-linearly with respect to the fraction of units adopting the strategy.

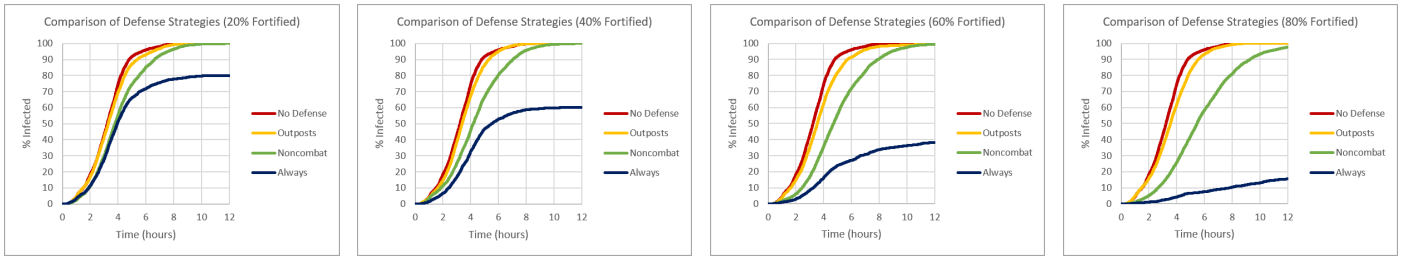
Figure 6 shows the progression of the malware over time under the Fortified Always strategy when resources are allocated at the Company, Platoon, and Squad levels. The similarity of the resulting curves indicates that the effectiveness of the defensive strategies does not depend significantly on the level of hierarchy at which it is implemented. This may be reassuring for military leaders because it is often more practical and convenient to implement policies at higher levels in the unit hierarchy.

V. Conclusions

In this work we demonstrated how agent-based simulation can be used to evaluate the relative effectiveness of defensive strategies for slowing the spread of self-propagating Bluetooth-based malware. We first presented a model of mobile tactical networks (MTNs), including hierarchical organization, mobility, and short-range communication. We then considered a cyber attack introduced by an infected Bluetooth-enabled enemy device, which then attempts to spread to the devices of allied soldiers. We suggested three classes of defensive strategies of varying robustness and cost to slow the spread of the malware: Fortified Outposts, Fortified Noncombat, and Fortified Always.

In order to evaluate the effectiveness of the defensive strategies, we developed and implemented an agent-based simulation model based on a scenario in which several companies are stationed at outposts around the periphery of a town harboring enemy soldiers. Experimental results showed that with close to full adoption, the Fortified Noncombat strategy provides a significant improvement over the baseline in which no defensive strategy is used. The Fortified Always strategy showed the best results even at moderate levels of adoption, but that may come at significant cost in money, convenience, or functionality.

The strategies we considered were intentionally presented at a high level of abstraction in order to permit a variety of possible implementations. For example, any of the strategies could be implemented as a policy-based or technology-based solution. A policy-based solution might entail soldiers disabling Bluetooth capabilities on their own devices when entering an FOB or outpost, or when crossing paths with other units in a non-combat situation. Technology-based solutions might entail equipping FOBs or outposts with signal-blocking devices, or installing anti-malware software on soldiers' mobile devices.



(a) (b) (c) (d)

Fig. 4: Progress of the malware over time when only a fraction of the units are implementing a defensive strategy.

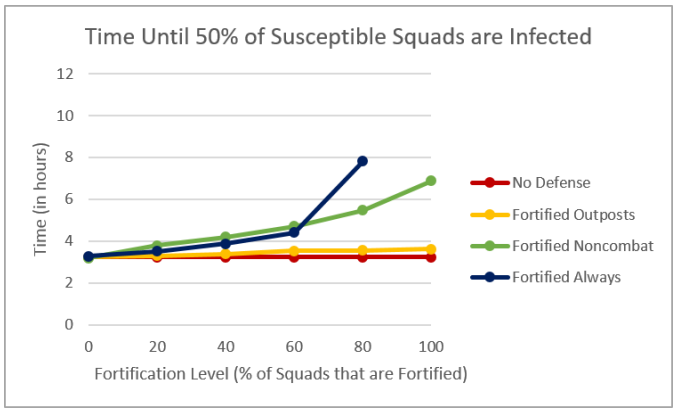


Fig. 5: Average time until 50% of the susceptible squads are infected, with fractional adoption for each of the defensive strategies. The value is undefined for the Fortified Always strategy with 100% adoption because there are no susceptible devices.

We note that the results should be interpreted qualitatively, as they are highly dependent on contextual and environmental parameters. While this initial work serves as a proof-of-concept, our core motivation is to provide methods and tools for the evaluation of defensive strategies, allowing military leaders to make more informed decisions when trying to secure MTNs against cyber attack.

A natural extension of this work is to incorporate detection and recovery procedures for infected nodes. Typically, the short-term solution to malware detection in MTNs is to fortify or quarantine infected nodes while a software fix (patch or new network protocol) is deployed. While this is a tolerable solution when network resources are not critical to an active operation or the number of infected nodes is low, it may not be practical in the heat of tactical operations. One approach to avoiding this scenario is the dynamic allocation of network security resources to stationary "strong points" or mobile recovery units on the battlefield. It may also be the case that methods such as flashing devices or purging volatile memory could provide reasonably strong protection even without permanent remediation. We intend to pursue these questions in subsequent work.

References

[1] A. O. Bang and P. L. Ramteke, "Manet: history, challenges and applications," *International Journal of Application or Innovation in Engineering & Management (IJAIEM)*, vol. 2, no. 9, pp. 249–251, 2013.

[2] J. Udhayan and R. Babu, "Lightweight vigilant procedure to implement security measures in highly roving military operations," *Journal of Computer Science*, vol. 9, no. 10, p. 1420, 2013.

[3] P. Wang, M. C. González, R. Menezes, and A.-L. Barabási, "Understanding the spread of malicious mobile-phone programs and their damage potential," *International Journal of Information Security*, vol. 12, no. 5, pp. 383–392, 2013.

[4] B. Thompson and J. Morris-King, "The impact of hierarchy on bluetooth-based malware spread in mobile tactical networks," in *Summer Computer Simulation Conference (SCSC)*, 2016.

[5] S. Boccaletti, V. Latora, Y. Moreno, M. Chavez, and D.-U. Hwang, "Complex networks: Structure and dynamics," *Physics Reports*, vol. 424, no. 4, pp. 175–308, 2006.

[6] E. Ravasz and A.-L. Barabási, "Hierarchical organization in complex networks," *Physical Review E*, vol. 67, no. 2, p. 026112, 2003.

[7] K. Lund, T. Hafsøe, and F. T. Johnsen, "A survey of middleware with focus on application in network based defence," *FFI Report*, vol. 2683, 2007.

[8] J.-H. Cho and A. Swami, "Towards trust-based cognitive networks: A survey of trust management for mobile ad hoc networks," DTIC Document, Tech. Rep., 2009.

[9] D. Kidston, L. Li, H. Tang, and P. Mason, "Mitigating security threats in tactical networks," DTIC Document, Tech. Rep., 2010.

[10] B. Rai and A. Jain, "Survey of attacks and security schemes in manet," *Universal Journal of Computers & Technology (UJCT)*, vol. 1, no. 1, pp. 1–8, 2016.

[11] G. Zyba, G. M. Voelker, M. Liljenstam, A. Méhes, and P. Johansson, "Defending mobile phones from proximity malware," in *Proceedings of the 28th Conference on Computer Communications (INFOCOM)*. IEEE, 2009, pp. 1503–1511.

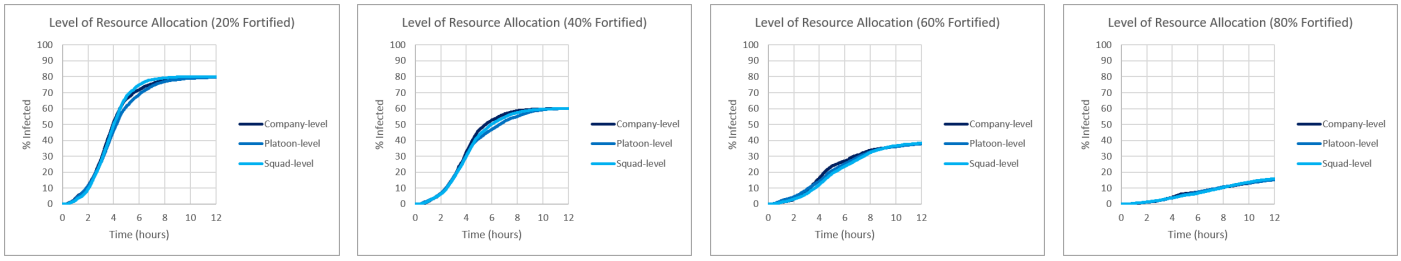
[12] C. Cowan, C. Pu, D. Maier, J. Walpole, P. Bakke, S. Beattie, A. Grier, P. Wagle, Q. Zhang, and H. Hinton, "Stackguard: Automatic adaptive detection and prevention of buffer-overflow attacks." in *Usenix Security*, vol. 98, 1998, pp. 63–78.

[13] Z. Zhu, G. Cao, S. Zhu, S. Ranjan, and A. Nucci, "A social network based patching scheme for worm containment in cellular networks," in *Handbook of Optimization in Complex Networks*. Springer, 2012, pp. 505–533.

[14] A. P. Felt, M. Finifter, E. Chin, S. Hanna, and D. Wagner, "A survey of mobile malware in the wild," in *Proceedings of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices*. ACM, 2011, pp. 3–14.

[15] Y. Nadji, J. Giffin, and P. Traynor, "Automated remote repair for mobile malware," in *Proceedings of the 27th Computer Security Applications Conference*. ACM, 2011, pp. 413–422.

[16] V. Vlachos and D. Spinellis, "A proactive malware identification system based on the computer hygiene principles," *Information Management & Computer Security*, vol. 15, no. 4, pp. 295–312, 2007.



(a) (b) (c) (d)

Fig. 6: Progress of the malware over time under the Fortified Always strategy, with resources being allocated at the Company, Platoon, and Squad levels.

[17] E. Hoque, R. Potharaju, C. Nita-Rotaru, S. Sarkar, and S. S. Venkatesh, "Taming epidemic outbreaks in mobile adhoc networks," *Ad Hoc Networks*, vol. 24, pp. 57–72, 2015.

[18] H. Zheng, D. Li, and Z. Gao, "An epidemic model of mobile phone virus," in *Proceedings of the 1st International Symposium on Pervasive Computing and Applications*. IEEE, 2006, pp. 1–5.

[19] O. Trullols-Cruces, M. Marco Fiore, and J. M. Barcelo-Ordinas, "Worm epidemics in vehicular networks," *IEEE Transactions on Mobile Computing*, vol. 14, no. 10, pp. 2173–2187, 2015.

[20] A. Shabtai, U. Kanonov, Y. Elovici, C. Glezer, and Y. Weiss, ""andromaly": a behavioral malware detection framework for android devices," *Journal of Intelligent Information Systems*, vol. 38, no. 1, pp. 161–190, 2012.

[21] R. G. Cole, "Initial studies on worm propagation in manets for future army combat systems," DTIC Document, Tech. Rep., 2004.

[22] M. Hypponen, "Malware goes mobile," *Scientific American*, vol. 295, no. 5, pp. 70–77, 2006.

[23] T. Herr and D. Herrick, "Military cyber operations: A primer," *American Foreign Policy Council Defense Technology Program Brief*, no. 14, 2016.

[24] J. Su, K. K. Chan, A. G. Miklas, K. Po, A. Akhavan, S. Saroiu, E. de Lara, and A. Goel, "A preliminary investigation of worm infections in a bluetooth environment," in *Proceedings of the 4th ACM Workshop on Recurring Malcode*. ACM, 2006, pp. 9–16.

[25] 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.

[26] C. Gao and J. Liu, "Modeling and restraining mobile virus propagation," *IEEE Transactions on Mobile Computing*, vol. 12, no. 3, pp. 529–541, 2013.

[27] J. P. Dunning, "Taming the blue beast: a survey of bluetooth-based threats," *IEEE Security & Privacy*, no. 2, pp. 20–27, 2010.

[28] P. Faruki, A. Bharmal, V. Laxmi, V. Ganmoor, M. S. Gaur, M. Conti, and M. Rajarajan, "Android security: a survey of issues, malware penetration, and defenses," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 2, pp. 998–1022, 2015.

[29] I. Kashefi, M. Kassiri, and M. Salleh, "Preventing collusion attack in android." *International Arab Journal of Information Technology (IAJIT)*, vol. 12, 2015.

[30] L. Carettoni, C. Merloni, and S. Zanero, "Studying bluetooth malware propagation: The bluebag project," *IEEE Security & Privacy*, no. 2, pp. 17–25, 2007.

[31] S. Gao, Z. Teng, J. J. Nieto, and A. Torres, "Analysis of an sir epidemic model with pulse vaccination and distributed time delay," *BioMed Research International*, vol. 2007, 2007.

[32] R. Yang, B.-H. Wang, J. Ren, W.-J. Bai, Z.-W. Shi, W.-X. Wang, and T. Zhou, "Epidemic spreading on heterogeneous networks with identical infectivity," *Physics Letters A*, vol. 364, no. 3, pp. 189–193, 2007.

[33] *Pamphlet 10-1: Organization of the United States Army*, Department of the Army, Washington, DC, June 1994.