The Impact of Hierarchy on Bluetooth-Based Malware Spread in Mobile Tactical Networks

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

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

ABSTRACT

Cyber-attacks in military 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 among mobile devices, thereby circumventing traditional cyber network defenses and evading detection. Because of its reliance on close physical proximity between devices in order to spread, the propagation of such malware is strongly dependent on the spatial and temporal properties of device movement. Mobility of military units in particular follows a well-defined organizational hierarchy and tactical doctrine. While this hierarchy of command has been studied extensively in order to maximize effectiveness and safety in the physical layer, its impact on security in the cyber layer is poorly understood and too often neglected. In this paper we develop an agent-based simulation model to study the impact of hierarchy on a mobile tactical network suffering a propagating cyber attack. We compare the dynamics of malware spread under a military-inspired mobility model to that of other more commonly-used mobility models.

Author Keywords

Hierarchy; mobile; tactical; Bluetooth; malware; spread

ACM Classification Keywords

I.6.3 SIMULATION AND MODELING: Applications

INTRODUCTION

Cyber attacks are a growing threat to mobile network security. Many examples of malware have been observed which take advantage of security gaps in wireless networking protocols to gain control of critical services by propagating an attack from a single point of entry to targeted assets [31, 29, 10, 11, 21]. Worms such as Cabir and CommWarrier, introduced in 2004 and 2005, respectively, demonstrated the ability of self-propagating malware to target popular mobile operating systems such as Android and Windows Mobile by spreading over Bluetooth. Since then, Bluetooth-based attacks have advanced in sophistication and potency. Attacks such as BlueBump and BlueSnarf can allow an attacker to gain complete read-write access to a target machine and can be run autonomously [8]. [13, 15, 14] present surveys of mobile malware threats, including several sophisticated multi-function worms. Of particular note is Android.Obad.OS, a trojan which, once loaded on a host, is able perform several different functions such as remotely performing commands in the console, sending SMS messages to premium-rate numbers, downloading additional malware via a botnet repository, and remote forwarding of custom malware payloads over Bluetooth [22]. Furthermore, Bluetooth communication is rarely observed by network security monitors and host-based security tools, making Bluetooth-based attacks even more dangerous [19].

Mobile tactical networks (MTNs) can be especially vulnerable to cyber attack. MTNs have become ubiquitous in military operations, supporting communication, coordination, and information dissemination between human and autonomous assets [4, 32]. MTNs are decentralized and heterogeneous, often consisting of a mix of mobile devices, sensors, vehicle-mounted computing and communication platforms, and autonomous robotic assets [34]. From the perspective of complex network theory, the study of these networks is important as their dynamic topology provides a clear-cut example of hierarchical spatial networks [7, 27]. Specifically, the movement of military units often obeys patterns dictated by the structure of the organizational hierarchy and chain of command. The unique characteristics of movement within MTNs is reflected in their patterns of communication and differentiates them from mobile networks in other contexts. It is therefore critical to develop domain-specific mobility models in order to test and validate assumptions regarding the spread of malware on military networks.

In this paper, we focus on modeling the movement and communication of military units performing reconnaissance and peace-keeping operations in a synthetic battlefield. Each soldier is equipped with a Bluetooth-enabled device that is vulnerable to infection by self-propagating malware which can be planted on devices by enemy cyber hackers. Through this model, we seek to answer the following questions:

- What patterns are formed by the propagation of Bluetooth-based malware in mobile tactical networks?
- How do these propagation patterns differ between hierarchical and other mobility models?
- What security approaches can be implemented to combat Bluetooth- or other proximity-based malware spread in MTNs?

SummerSim-SCSC, 2016 July 24-27, Montreal, Québec, Canada

Our main contributions are:

- An agent-based model of unit movement and communication in mobile tactical networks which reflects a military-inspired hierarchical command structure and group mobility model
- Implementation of our model for a synthetic battlefield in which military units equipped with Bluetooth-enabled mobile devices conduct excursions into a town
- Comparison of the dynamics of malware spread on MTNs operating under three different mobility models, including our model, using agent-based simulation

The remainder of the paper is organized as follows: We first provide a survey of related work. Next we present our model for synthetic battlefield simulation and cyber worm propagation. In the following section, we describe our simulation experiments and discuss the results. Finally, we conclude the work and suggest future research.

RELATED WORK

Mobility Models

Hong et al. propose the Reference Point Group Mobility (RPGM) model, in which each group's macro-scale movement is governed by the trajectory of a reference point, and each individual's micro-movements are described by random motion within a bounded region centered at its group's reference point, so that the coordinate system of each group member's movement maintains the reference point's current position as its origin [20].

Blakely et al. propose the Structured Group Mobility Model (SGMM), which replaces the random motion of group members in the RPGM model with pre-defined structured movement to represent fixed movement patterns often used in tactical contexts [6].

Fongen et al. propose the Hierarchical Group Mobility (HGM) model as a generalization of RPGM from a two-level to a multi-level hierarchy [16]. In HGM, relationships between moving entities are expressed through a hierarchy, represented as a rooted directed forest, and the net movement of an entity is the aggregation of all its ancestors' individual movements (including itself). HGM allows for units at different levels or even different units at the same level of the hierarchy to operate under different mobility models. This flexibility is useful for modeling movement within a tactical environment, as different groups of soldiers and vehicles may at times be assigned to the same high-level task, and at other times may be assigned supporting tasks requiring them to move individually or in smaller groups.

We adapt ideas from all of the above models, but loosen the requirement that entities must inherit the motion of their ancestors in the hierarchy. Instead, each unit in the hierarchy may have a location, trajectory, and mission objective, and subunits may either inherit directly from their supervising units or define their own objectives and movement based on knowledge of the objectives and movement of their supervisors. This better represents real-world tactical networks, in which command flows down the organizational hierarchy, but subordinate units often have some degree of autonomy in determining their own behavior while working toward a larger mission objective.

Models of Malware Spread

Some previous research on cyber attacks in MTNs has focused on identifying the impact of detection, routing protocols, and social engineering [1, 2]. Of those focusing on the dynamics of malware propagation, limited consideration is paid to the role of mobility and spatial proximity, often relying on homogeneity assumptions and compartmental models [23]. Yang et al. and Gao et al. show that such compartmental models greatly overestimate the epidemic spreading speed due to their implicit homogeneous mixing assumption and lack of user models [35, 18].

When mobility is considered, it is often expressed through popular models such as the Random Waypoint model, which neither realistically mimic human mobility nor capture the inherent structure of military operations [28, 16]. Moreover, military networks are often deployed in areas deemed otherwise unsuitable for civilian telecommunication networks, meaning a higher degree of network sparsity and likelihood of environmental or adversarial disruption. Likewise, military units often shift between tactical objectives such as holding a location, ordered group formations, and reactive, sometimes chaotic movement (such as when engaged in combat or conducting searches). These real-world complexities make simple statistical models unsuitable for modeling the propagation of malware in MTNs.

Bluetooth-Based Malware

Several factors differentiate the spread of Bluetooth malware from that of traditional malware propagating over Wi-Fi or other wireless channels. Bluetooth-based attacks are reliant on short-range peer-to-peer interaction, mimicking the behavior of infectious diseases that spread by contact [5]. The range of Bluetooth radios is approximately 10 times smaller than the range of Wi-Fi radios, sometimes no more than 10-15 feet depending on the environmental conditions, and Bluetooth piconets are rarely larger than 9 or 10 nodes, as opposed to the hundreds which might comprise a Wi-Fi network.

Despite these limitations, malware exploiting Bluetooth-based malware have shown the capability to spread quickly. Su et al. perform simulations using trace data 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 an urban environment [30]. On the other hand, Wang et al. model the spread of malware across networks of mobile phone users and observe that Bluetooth-based malware spreads slowly due to the short range of Bluetooth and therefore the relatively low contact rate between devices [33]. Channakeshava et al. demonstrate via simulation on synthetic wireless networks using activity-based models of urban population mobility that the time it takes for a Bluetooth-based worm to

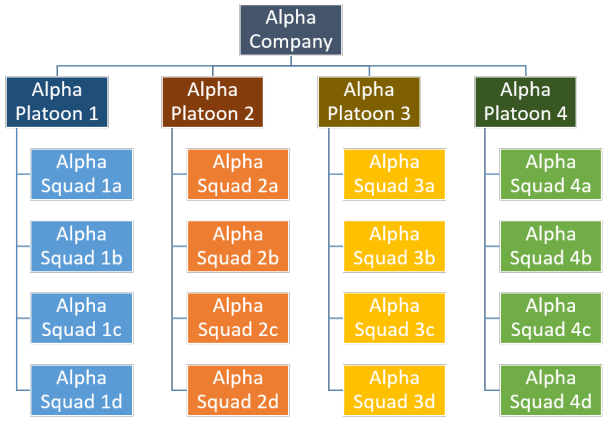


Figure 1: Unit hierarchy

spread throughout a network is highly dependent on the effectiveness of countermeasures taken within the first hour after it is introduced to the network [9]. Gao and Liu study a two-mode malware propagation model for smartphone networks (Bluetooth and SMS) and find that Bluetooth is an effective transport medium for targeting hosts less likely to respond to the tainted SMS communications [17].

In this work, we aim to develop a model that makes more realistic assumptions regarding the temporal and spatial patterns of military units, with the hope of providing useful insights into what operational steps might be taken to defend against propagating malware in a military context. Next we present our models of mobility, Bluetooth communication, and malware propagation in MTNs.

MODEL AND SCENARIO

Tactical Model

In order to examine the impact of mobility on the propagation of malware in a MTN, we first identify the properties of military operations that distinguish them from other MTN applications (and therefore should be captured by our simulation model):

- Hierarchical organizational structure: Military units are organized in a hierarchical fashion, in which large units of many soldiers are split into smaller subunits, which are further divided into subsubunits.
- Mission-driven: The actions taken by military units are decided upon by unit leaders in fulfillment of an overarching mission.
- Chain of command: Units operate under a hierarchical system of command that parallels their organizational structure, in which commands flow from the highest to the lowest levels of the military hierarchy, at each level adding greater specificity in support of the larger mission.
- Group mobility: Unit movement also parallels the organizational structure, with units that are closer to one another in the hierarchy tending to move together or have greater physical proximity.

We consider the above as motivation for a hierarchical command and control (C2) infrastructure to provide battle direction for the units in the model.

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 [12]. 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. Figure 1 illustrates the unit hierarchy used in our model, with companies labeled by Greek letters, platoons within a company indexed with Arabic numerals, and squads within a platoon indexed with lower case letters.

Cyber Model

Each soldier in our model carries a mobile device that facilitates short-range wireless communication, such as Bluetooth, on the battlefield. Each device regularly scans the environment for nearby friendly devices. When two friendly 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.

We model self-propagating malware that spreads between mobile devices over short-range communication channels. In particular, we aim to capture two important properties of Bluetooth-based malware spread:

- Short range: Bluetooth-based malware requires very close proximity to spread.
- Small payload: The malware payload is small in order to facilitate rapid transmission over low-bandwidth connections.

Whenever an infected device comes within communication range of another mobile device carried by a friendly soldier, the two devices connect and the malware spreads. For simplicity, we model malware transmission as occurring instantaneously.

Scenario

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.

Each company has an outpost that can be used by its 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.

In an attempt to infiltrate the allied cyber network, the enemy deploys a cyber hacking team somewhere in the town. When an allied soldier moves within communication range of the enemy cyber team, they hack into the soldier's device and infect it with a self-propagating Bluetooth worm, which then spreads to other allied devices as the soldiers continue carrying out their tactical objectives.

Figure 3(a) gives a screenshot of our simulation environment. The large circle represents the town, the smaller circles around the town's periphery represent outposts, and the red circle represents the range of the enemy cyber hacking team. Squads are initially blue, and become red when infected, which occurs when they come within range of the enemy cyber team or an already-infected squad.

Simulation Model

We construct an agent-based simulation model in Java to represent the scenario described above of soldiers moving around in a tactical environment. Because soldiers in a squad typically stay in close physical proximity to one another, it is assumed that if one soldier's device gets infected, all devices carried by members of the squad will soon be infected. Therefore, for the purpose of simulation we consider the squad to be an atomic unit and do not explicitly model behavior at the scale of individual soldiers.

Our implementation includes Point, Region, Company, Platoon, and Squad classes and an enumerated type Action. The Point class represents a point in a two-dimensional continuous space. The Region class represents a circular region specified by a center Point and a radius. Each unit (company, platoon, or squad) in the organizational hierarchy is represented by a corresponding software agent (Company, Platoon, or Squad) that attempts to achieve goals set by the mission directives, which flow down the chain of command from Company to Platoon to Squad. A Company agent is a non-physical entity that includes a set of four Platoons and has a designated Region corresponding to the outpost to which its constituent Platoons return from combat. A Platoon agent is a non-physical entity that includes a set of four Squads and passes on movement orders from its Company leadership to its constituent Squads. A Squad agent is a physical entity that takes movement orders from its Platoon leadership, reacts to its environment, and communicates with other nearby Squad agents. The Action type takes values in the set {HOLD, TRAVEL, ATTACK}, corresponding to the three actions that a Squad may be performing at any given time.

Each Squad begins the simulation at a random location within the Region corresponding to its Company's outpost. After performing the HOLD action for a randomly chosen amount of time between 10 and 60 minutes, all four Squads in a Platoon TRAVEL to a randomly chosen waypoint within the town region. Once they reach the waypoint, the Squads go into ATTACK mode, independently moving in a random walk (see next section) to simulate responding to local stimuli. After a randomly chosen amount of time between 30 minutes and 4 hours, all four Squads in the Platoon TRAVEL back to their designated outpost, and the cycle repeats. Figure 2 shows a partial implementation of the Squad class.

```
class Squad {
    double maxSpeed;
    Point location;
    Action action;
    int duration;
    Point waypoint;
    Region target;
    boolean isInfected;

    Squad(double xInit, double yInit) {
        maxSpeed = 1.0;
        location = new Point(xInit, yInit);
        action = Action.HOLD;
        duration = 0;
        waypoint = null;
        target = null;
        isInfected = false;
    }

    boolean isActionComplete() {
        if (action == Action.HOLD)
            return (duration <= 0);
        else if (action == Action.TRAVEL)
            return (location.equals(waypoint));
        else if (action == Action.ATTACK)
            return (duration <= 0);
    }

    void move() {
        if (action == Action.TRAVEL)
            moveTowardWaypoint(waypoint);
        else if (action == Action.ATTACK)
            moveRandomlyInRegion(target);
        duration--;
    }

    ...
}
```

Figure 2: Partial implementation of Squad agent model

Comparison Models

We compare the dynamics of malware spread under the above military-inspired mobility model to that of two commonly-used mobility models, the Random Walk and Random Waypoint models.

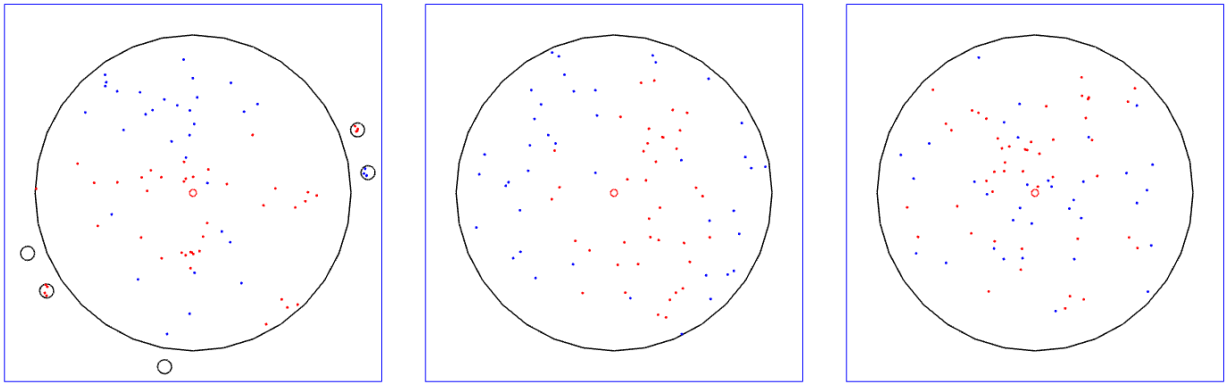
In the Random Walk model, at each time step, each agent moves in a randomly chosen direction. To model variation in terrain and other external factors, agents move at a speed randomly selected between 0 m/s and their maximum speed.

In the Random Waypoint model, each agent selects a random point in the target region and moves in the direction of that point until it has reached it, at which time the agent randomly selects a new point and continues in a similar fashion.

EXPERIMENTS

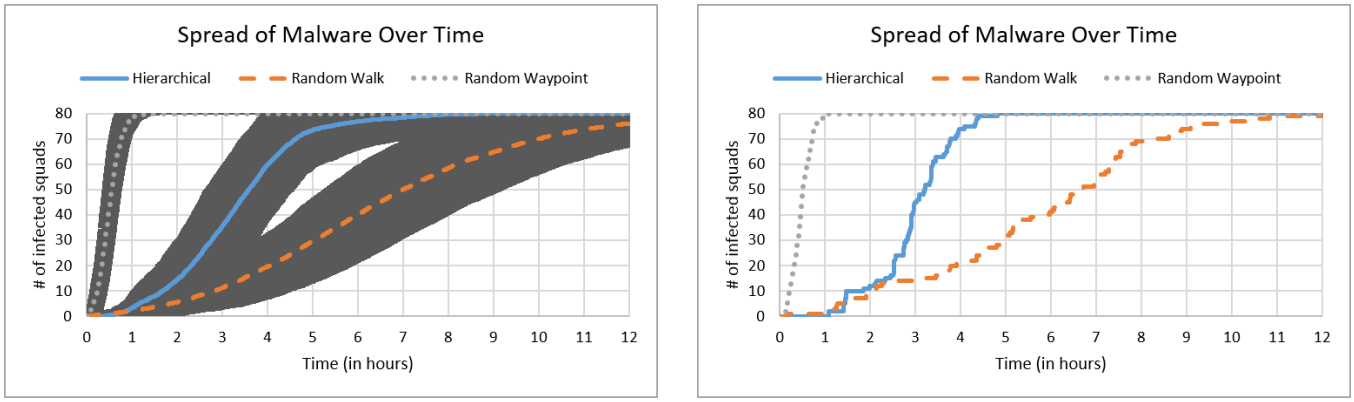
Experimental Setup

We implement our simulation model in Java and perform experiments using the Repast Simphony modeling and simulation environment [26]. All experiments are conducted on an



(a) Hierarchical (b) Random Walk (c) Random Waypoint

Figure 3: Screenshots of simulations in Repast Simphony using three different mobility models



(a) Mean and standard deviation over 100 trials (b) A single sample run of the simulation

Figure 4: Malware spread using three different mobility models: Hierarchical, Random Walk, and Random Waypoint

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 $\approx$ 785,398 m^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.

All simulations are done in two dimensions. No terrain model is used. We do not account for signal attenuation, reflection, or other wireless phenomena.

Simulations are run for a period of 12 hours to represent the activities of a typical day, with data collected at time intervals of $\Delta t = 12$ seconds.

Simulation Results

Figure 3 shows screenshots from simulations in Repast Simphony under each of the three mobility models studied. Under the Random Walk model, agents move locally but do not travel far from their points of origin. This results in the malware spreading slowly but steadily across the population in a spatial progression. Under the Random Waypoint model, agents are constantly traveling the length of the environment. This results in a high rate of pairwise interactions, with any two agents roughly equally likely to cross paths, and less spatial correlation between infected units.

Figure 4(a) shows the size of the infected population over time, averaged over 100 independent runs of the simulation, with ranges of ± 1 standard deviation. The plot confirms that malware spreads much more quickly under the Random Waypoint model than the Random Walk model. The rate of spread under our military-inspired hierarchical mobility model seems to fall between that of the Random Walk and Random Waypoint models. Furthermore, the plot indicates that on average, each of the three models yields a sigmoidal growth curve typical of the compartmental models common to the ecological and epidemiological literature, indicating an initial exponential spread which slows down as the infection reaches its saturation point [25, 24, 3]. However, the standard deviations under the Hierarchical and Random Walk models are relatively large, indicating that the behavior for different runs of the simulation may vary significantly.

To get a more fine-grained view of the dynamics of malware spread under each of the models, we examine the results of a single run of the simulation, shown in Figure 4(b). Although the growth curves were sigmoidal for all three models when averaged over many independent trials, for a single simulation run the Random Walk model yields roughly linear growth in the number of squads with infected devices, which matches our observation of the malware's spatial progression. On the other hand, the growth curve for our sample simulation run under the Random Waypoint model is still sigmoidal and very similar to the corresponding averaged growth curve, which is not surprising given the relatively small standard deviation for the Random Waypoint model, as seen in Figure 4(a).

The Hierarchical model does not exhibit either extreme of slow, almost-linear growth or fast, sigmoidal growth. Instead, it demonstrates a hybrid mix of periods of slow growth as squads come within range of one another on the battlefield along with more rapid growth as squads pass one another while traveling, punctuated by short spurts of step-wise growth as each squad returns to its outpost and propagates the malware to the other squads in its platoon and to other platoons that have returned to the outpost at the same time. This suggests that security interventions that focus on rally points or highly-traveled regions may be an effective way to combat Bluetooth- or other proximity-based malware spread in MTNs.

CONCLUSIONS AND FUTURE WORK

In this work we examine the impact of hierarchical command structure and group mobility on malware outbreaks in MTNs through an agent-based synthetic battlefield simulation. Experiments were performed using realistic parameters representing a tactical scenario in which several companies of soldiers conduct excursions into a town harboring an enemy cyber hacking team with the capability to infect nearby mobile devices with self-propagating malware. For comparison, experiments were also performed under which soldiers moved according to two commonly-used mobility models, the Random Walk model and the Random Waypoint model. The results indicate that the dynamics of malware spread are significantly different under the three mobility models examined. Malware spread under the Random Walk model progresses roughly linearly, while malware spread under the Random Waypoint model has sigmoidal growth. Simulations under our military-inspired hierarchical mobility model demonstrate that malware spread in a tactical setting exhibits more complex dynamics than is captured by the more simplistic models. This work calls for hesitancy in transferring existing results for malware spread in mobile networks to the tactical domain, and also highlights the need for more extensive research to better understand the risks that the growing threat of cyber-attack pose for military operations.

While this initial work serves as a proof-of-concept, our core motivation is to provide methods and tools for securing MTNs against malicious attack. A natural extension of this work is to incorporate detection and recovery procedures for affected nodes. Typically, the short-term solution to malware detection in MTNs is to fortify or quarantine affected 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 affected nodes is low, this is often not the case, in which case such approaches may result in the entire network being lost, either to enemy action or self-imposed denial of service. One approach to avoiding this scenario is the dynamic allocation of network security resources at "strong points" in the battlefield, i.e. locations where units rally and therefore are conducive to the rapid spread of malware. We can see intuitively and from the results of simulation that enacting strong security procedures as units exit and enter common rally points may significantly limit the ability of malware to spread rapidly through the network. It may be the case that methods such as flashing devices or purging volatile memory might provide reasonably strong protection even without permanent remediation. We intend to pursue these questions in subsequent work.

REFERENCES

1. Abraham, S., and Chengalur-Smith, I. An overview of social engineering malware: Trends, tactics, and implications. *Technology in Society 32*, 3 (2010), 183–196.
2. Agre, J. R., Gordon, K. D., and Vassiliou, M. S. Practical considerations for use of mobile apps at the tactical edge. Tech. rep., DTIC Document, 2014.
3. Anderson, R. M., May, R. M., and Anderson, B. *Infectious diseases of humans: dynamics and control*, vol. 28. Wiley Online Library, 1992.
4. Bang, A. O., and Ramteke, P. L. Manet: history, challenges and applications. *International Journal of Application or Innovation in Engineering & Management (IJAIEM) 2*, 9 (2013), 249–251.
5. Barrett, C. L., Channakeshava, K., Eubank, S., Anil Kumar, V., and Marathe, M. V. From biological and social network metaphors to coupled bio-social wireless networks. *International Journal of Autonomous and Adaptive Communications Systems 4*, 2 (2011), 122–144.
6. Blakely, K., and Lowekamp, B. A structured group mobility model for the simulation of mobile ad hoc networks. In *Proceedings of the Second International Workshop on Mobility Management &Amp; Wireless Access Protocols*, MobiWac '04, ACM (New York, NY, USA, 2004), 111–118.
7. Boccaletti, S., Latora, V., Moreno, Y., Chavez, M., and Hwang, D.-U. Complex networks: Structure and dynamics. *Physics Reports 424*, 4 (2006), 175–308.
8. Carettoni, L., Merloni, C., and Zanero, S. Studying bluetooth malware propagation: The bluebag project. *IEEE Security & Privacy*, 2 (2007), 17–25.
9. Channakeshava, K., Chafekar, D., Bisset, K., Kumar, V. S. A., and Marathe, M. Epinet: A simulation framework to study the spread of malware in wireless networks. In

Proceedings of the 2nd International Conference on Simulation Tools and Techniques, Simutools '09, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering) (ICST, Brussels, Belgium, Belgium, 2009), 6:1–6:10.

10. Cole, R. G. Initial studies on worm propagation in manets for future army combat systems. Tech. rep., DTIC Document, 2004.
11. Cole, R. G., Phamdo, N., Rajab, M. A., and Terzis, A. Requirements on worm mitigation technologies in manets. In *Workshop on Principles of Advanced and Distributed Simulation (PADS)*, IEEE (2005), 207–214.
12. Department of the Army. *Pamphlet 10-1: Organization of the United States Army*. Washington, DC, June 1994.
13. Dunning, J. P. Taming the blue beast: a survey of bluetooth-based threats. *IEEE Security & Privacy*, 2 (2010), 20–27.
14. Faruki, P., Bharmal, A., Laxmi, V., Ganmoor, V., Gaur, M. S., Conti, M., and Rajarajan, M. Android security: a survey of issues, malware penetration, and defenses. *IEEE Communications Surveys & Tutorials 17*, 2 (2015), 998–1022.
15. Felt, A. P., Finifter, M., Chin, E., Hanna, S., and Wagner, D. 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), 3–14.
16. Fongen, A., Gjellerud, M., and Winjum, E. A military mobility model for manet research. In *Proceedings of the IASTED International Conference on Parallel and Distributed Computing and Networks* (2009).
17. Gao, C., and Liu, J. Modeling and restraining mobile virus propagation. *IEEE Transactions on Mobile Computing 12*, 3 (2013), 529–541.
18. Gao, S., Teng, Z., Nieto, J. J., and Torres, A. Analysis of an sir epidemic model with pulse vaccination and distributed time delay. *BioMed Research International 2007* (2007).
19. Herr, T., and Herrick, D. Military cyber operations: A primer. *American Foreign Policy Council Defense Technology Program Brief*, 14 (2016).
20. Hong, X., Gerla, M., Pei, G., and Chiang, C.-C. A group mobility model for ad hoc wireless networks. In *Proceedings of the 2nd ACM international workshop on Modeling, analysis and simulation of wireless and mobile systems*, ACM (1999), 53–60.
21. Hypponen, M. Malware goes mobile. *Scientific American 295*, 5 (2006), 70–77.
22. Kashefi, I., Kassiri, M., and Salleh, M. Preventing collusion attack in android. *International Arab Journal of Information Technology (IAJIT) 12* (2015).
23. Kephart, J., and White, S. Directed-graph epidemiological models of computer viruses. In *Research in Security and Privacy, 1991. Proceedings., 1991 IEEE Computer Society Symposium on* (May 1991), 343–359.
24. Kermack, W. O., and McKendrick, A. G. A contribution to the mathematical theory of epidemics. *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences 115*, 772 (1927), 700–721.
25. McKendrick, A. G., and Pai, M. K. The rate of multiplication of micro-organisms: A mathematical study. *Proceedings of the Royal Society of Edinburgh 31* (1 1912), 649–653.
26. North, M. J., Collier, N. T., Ozik, J., Tatara, E. R., Macal, C. M., Bragen, M., and Sydelko, P. Complex adaptive systems modeling with repast simphony. *Complex Adaptive Systems Modeling 1*, 1 (2013), 1–26.
27. Ravasz, E., and Barabási, A.-L. Hierarchical organization in complex networks. *Physical Review E 67*, 2 (2003), 026112.
28. Rhee, I., Shin, M., Hong, S., Lee, K., Kim, S. J., and Chong, S. On the levy-walk nature of human mobility. *IEEE/ACM Transactions on Networking 19*, 3 (2011), 630–643.
29. Shabtai, A., Kanonov, U., Elovici, Y., Glezer, C., and Weiss, Y. "andromaly": a behavioral malware detection framework for android devices. *Journal of Intelligent Information Systems 38*, 1 (2012), 161–190.
30. Su, J., Chan, K. K., Miklas, A. G., Po, K., Akhavan, A., Saroiu, S., de Lara, E., and Goel, A. A preliminary investigation of worm infections in a bluetooth environment. In *Proceedings of the 4th ACM Workshop on Recurring Malcode*, ACM (2006), 9–16.
31. Trullols-Cruces, O., Marco Fiore, M., and Barcelo-Ordinas, J. M. Worm epidemics in vehicular networks. *IEEE Transactions on Mobile Computing 14*, 10 (2015), 2173–2187.
32. Udhayan, J., and Babu, R. Lightweight vigilant procedure to implement security measures in highly roving military operations. *Journal of Computer Science 9*, 10 (2013), 1420.
33. Wang, P., González, M. C., Hidalgo, C. A., and Barabási, A.-L. Understanding the spreading patterns of mobile phone viruses. *Science 324*, 5930 (2009), 1071–1076.
34. Wang, P., González, M. C., Menezes, R., and Barabási, A.-L. Understanding the spread of malicious mobile-phone programs and their damage potential. *International Journal of Information Security 12*, 5 (2013), 383–392.
35. Yang, R., Wang, B.-H., Ren, J., Bai, W.-J., Shi, Z.-W., Wang, W.-X., and Zhou, T. Epidemic spreading on heterogeneous networks with identical infectivity. *Physics Letters A 364*, 3 (2007), 189–193.