Evaluation of Malware Spreading in Wireless Multihop Networks with Churn

Vasileios Karyotis(✉) and Symeon Papavassiliou

Institute of Communications and Computer Systems (ICCS),
School of Electrical and Computer Engineering,
National Technical University of Athens, Zografou, 15780 Athens, Greece
vassilis@netmode.ntua.gr, papavass@mail.ntua.gr

Abstract. Modeling malware spreading in wireless networks has attracted significant interest lately, since this will increase the robustness of such networks that constitute the lion's share of Internet access nowadays. However, all of previous works have considered networks with fixed number of devices. In this work, we focus on users that can dynamically join and leave the network (node churn) as a result of the effects of malware, or their own operation, i.e. energy depletion. We adopt and adapt a queuing-based model for malware spreading for the case of wireless distributed networks with churn. The corresponding methodology captures the dynamics of SIS-type malware, where nodes are always prone to receive new or already spreading infections over a long period. The employed framework can be exploited for quantifying network reliability and study network behavior, which can be further used for increasing the robustness of the system against the most severe attacks.

Keywords: SIS malware · Network churn · Wireless multihop networks · Product-form queuing networks · Network robustness

1 Introduction

The wireless communications market has expanded massively in the last decade, constituting nowadays the most preferred way for Internet access by users around the world. Following suit, wireless services and applications, software and wireless devices' technologies have also proliferated, orders of magnitude compared to the ones available ten years ago. Unfortunately, since the emergence of the first computer virus and the corresponding malicious software (malware) targeting mobiles (cabir bluetooth virus in 2004 [1]), malware spreading in wireless networks has exhibited exponential growth (see [2] and references therein).

Modeling accurately the dynamics of malware spreading is of high research and practical importance with numerous associated benefits, especially for wireless networks where the impact of malware can be more severe. In this paper, we focus on exactly this aspect of modeling malware dynamics and in fact, contrary to the majority of other research works, we address this problem in dynamic networks, where nodes join and leave the network (denoted as node churn).

N. Mitton et al. (Eds.): ADHOCNETS 2014, LNICST 140, pp. 63–74, 2014.
DOI: 10.1007/978-3-319-13329-4_6

Such networks with "node churn" emerge in most of the applications of wireless multihop topologies, e.g. ad hoc, sensor, vehicular, etc., and from this perspective, the contribution of this paper is of great interest for the aforementioned applications of wireless distributed networks.

In the past, various attempts to model malware in general have emerged (see [3] and references therein), each aiming at different objectives. Furthermore, diverse modeling approaches have employed various analytical tools for their purposes. These earliest attempts to model malware spreading in the Internet and wireless networks were based on deterministic methodologies adopted from epidemics [4], while the majority did not consider the possibility of network churn at all. Lately, some notable effort has been devoted to the macroscopic dynamics of malware propagation, especially in wireless decentralized networks [5,6]. Macroscopic modeling refers to the generic study of malware propagation for a long time period, where different types of attacks spread and present recurring behavior, i.e. users become infected repeatedly after their recoveries.

In this paper, we will extend the above direction and study the macroscopic modeling of malware propagation for wireless distributed networks with churn. Based on a closed queuing network model, the transitions of states of legitimate nodes attacked by malicious users are evaluated, while legitimate nodes might enter/leave the network due to exhausting their energy/recharging and/or the impact of malware. We adopt a closed queuing network model, initially developed in [7], based on which a product-form solution is obtained through the Norton equivalent methodology. We use this framework to study and analyze the behavior of wireless distributed networks attacked by a single attacker. The results can be used for assessing the robustness of the network, and can be further exploited in increasing network reliability against the worst possible outbreaks.

The rest of this paper is organized as follows. Section 2 summarizes related works and distinguishes our contribution from them, while Section 3 presents concisely the employed queuing model along with relevant analysis. Section 4, provides quantitative results for the networks of interest and finally, Section 5 concludes the letter.

2 Related Work

Malware can be broadly classified in two main types, i.e. direct and indirect, where threats propagate via physical neighbors only [8], or via multihop infections, e.g. email viruses [9]. In this work, we will focus on the first, since the second can be implicitly analysed as a case of direct malware spreading at a higher protocol layer, e.g. users directly connected at the Application layer.

Furthermore, there are two main infection models[1], denoted by Susceptible - Infected - Removed (SIR) and Susceptible - Infected - Susceptible (SIS), corresponding to the allowed state transition sequence [10]. The SIR is more suitable for the short-term study of independent threats, e.g. CodeRed worm

[1] The term 'infection model' characterizes the discipline under which legitimate nodes become infected and recover, if so, due to malware spreading and their operation.

virus, while the SIS is more appropriate for the long-term (macroscopic) study, where nodes oscillate between susceptibility and infection due to recurrent or newly emerging malware. In this paper, we focus on the long-term and steady-state behavior of distributed wireless networks, and thus, we adopt the SIS node infection paradigm for legitimate nodes.

Traditionally, malware propagation modeling has employed epidemics mathematics [4,10], properly adapted to fit communications networks. The problem is cast as a system of ordinary differential equations with respect to the number of infected and the number of removed nodes, if applicable. Epidemics are threat-specific, i.e. more suitable for SIR infection paradigms. However, even in case of advanced epidemic models, e.g. epidemics combined with Kalman estimation [11]), the proposed models cannot describe the evolution of malware propagation in networks with dynamic node churn, such as sensor or ad hoc topologies for example.

As the attack rate increases, in accord with the importance of wireless infrastructures, more generic approaches analyzing malware propagation are required to secure commercial and critical networks. Various models have emerged towards this direction, most of which attempt to analyze malware propagation in more general settings compared to traditional epidemics techniques. Contrary to the differential equations based approach of epidemics, probabilistic tools have been mostly employed for the latest and more generic approaches. In [12], probabilistic models based on Interactive Markov Chains have been proposed, which attempt to partially capture the inherently stochastic nature of attackers over arbitrary topologies. In [13] the impact of topology on the dynamics of the propagation was identified and exploited to design effective countermeasures.

A queuing-based framework has been proposed in [14] for wireless multihop networks, and it was exploited in various capacities, e.g. study of attack strategies. The proposed model describes the macroscopic behavior of malware propagation in wireless multihop networks without churn. The approach presented in this work, adopts the same framework, but extends it in the more general scenario of dynamic networks with node churn.

A stochastic optimization approach was introduced in [15,16], where the concept of varying the transmission power in order to design effective defenses has been jointly considered with epidemic dynamics. Optimal strategies have been developed by exploiting Pontryagin Maximum Principle. However, the proposed framework has been developed for specific energy-depleting attacks and does not consider the possibility of new nodes entering the network (node churn).

Unfortunately, all previous works have not considered the most general behavior of dynamic networks, where legitimate nodes enter/leave the network due to their own operation (e.g. exhausting network energy) and/or the impact of malware. In this work, we will adopt from [7] a closed queuing-network-based methodology that extends the approach of [5] for networks with churn, and exploit it to study the behavior of wireless networks with multihop topology attacked by a single malicious user. Infected nodes can also infect their peers.

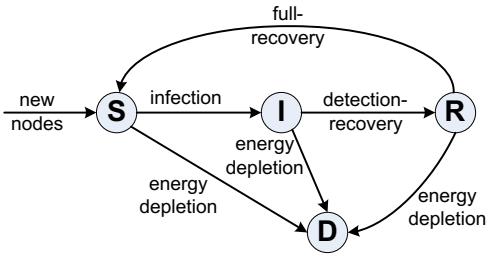


Fig. 1. State transition diagram for legitimate nodes in a network with churn

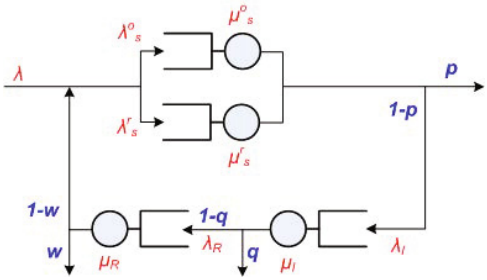
3 Queuing Based Modeling for Malware Spreading in Wireless Networks with Churn

3.1 System and Malware-Spreading Models

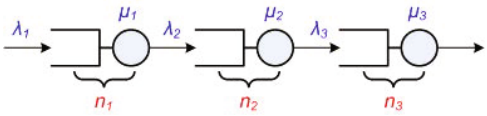
Considering the capabilities of state-of-the-art software and handheld devices that enable recurring malware threats, we focus on the long-term network operation and employ the Susceptible-Infected-Susceptible (SIS) [10] infection model to describe the steady-state behavior of users (legitimate nodes). We consider a static network and also the more general scenario, where users enter and leave the network (node churn [17]), which is often the case in wireless distributed networks, e.g. sensor, vehicular, ad hoc and tactical networks.

In a network with churn, a legitimate node will start susceptible, free of any malware piece, and the corresponding susceptible state is denoted by S (Fig. 1). At some point, a susceptible node will become infected by some spreading threat, e.g. virus, worm, etc., and within a long observation period, the node will eventually return to the susceptible state (by removing the malware). The infected state is denoted by I. In the general case of networks with churn, but also for networks without churn, the short-term behavior of nodes and their corresponding state transition may involve other intermediate states as well, as shown in Fig. 1. These intermediate transitions may involve a recovery state (denoted by R) and a state where nodes are considered dead (denoted by D). The dead state cumulatively represents nodes that cease operation due to exhausted energy or due to malware operation. Nodes that complete their recovery, return to the susceptible state, and without loss of generality, we assume that new nodes entering the network also begin their lifetime in the susceptible state. Dead nodes are completely removed from the network (potentially re-introduced in the network as new susceptibles after a long time). Consequently, the overall system follows the SIS paradigm, where it will be possible for susceptible nodes to become infected and eventually recover again to the susceptible state.

Regarding the communication model, we assume that at each time the network has n legitimate nodes, each with transmission radius R_t. For simplicity, it is also assumed that node pairs are formed only within the transmission range of nodes, as in [5,6]. More general communication models can be incorporated in a straightforward manner.



(a) Generic malware propagation queuing model.



(b) Equivalent product-form serial queuing system.

Fig. 2. Queuing models for malware spreading in networks with churn

With respect to Fig. 1, it can be observed that each user spends an amount of time in each node state that varies stochastically. Furthermore, given the succession of state transitions depicted in Fig. 1, a node entering the network at the susceptible state, might either deplete its energy and become dead with probability p or could become infected by malware and transition to the infected state. From the infected state the node might either deplete its energy as well, cease opearation due to malware and become dead with probability q, or it could transition to the recovery state. Finally, from the recovering state the user either recovers to the susceptible state and the cycle begins again, or the node depletes its energy while recovering and it is removed from the network to the dead state with probability w.

Thus, the behavior of legitimate users can be segregated in two main modes, susceptible and infected-recovering (non-operational). In the first mode, nodes could be operational (some of which might exhaust their energy and leave the network) or recharging. In the infected-recovering mode, nodes become infected and either they move to recovery until they become susceptible again or they are removed from the network. This behavior can be mapped to the operation of a queuing network as shown in Fig. 2(a), where queuing and processing correspond to the time spent by each node in each different state described before. In Fig. 2(a) the upper part corresponds to the normal operation of nodes (susceptible operational - susceptible recharging) and the lower part to the infection-recovery mode. The customers of the queuing network correspond to the nodes of the network as they change states due to malware and node churn. It should be noted that the queuing network is open due to node churn, allowing for new customers to enter (corresponding to new susceptible nodes) and customers to

leave (corresponding to nodes depleting their energy or becoming dead due to malware). The depicted input/output and service rates of the queuing network correspond to node churn rates and infection/recovery of the actual legitimate network users under attack, respectively.

3.2 Analysis of Spreading in Multihop Networks with Churn

In order to analyze the generic network of Fig. 2(a), the Norton equivalent [18] of the upper part with parallel queues may be employed, so that a single queue substitutes that part of Fig. 2(a). This does not harm the analysis because in the study of robustness we are not particularly interested in which nodes are susceptible-operational and which are susceptible-recharging. We focus on the number of susceptible nodes versus the number of infected and recovering. From the Norton equivalent, the rates of the new queue will be $\mu_S = \mu_s^o + \mu_s^r$ and $\lambda_S = \lambda_s^o + \lambda_s^r$, where μ regard service rates and λ input rates in general. All μ, λ depicted in Fig. 2(a) correspond to the cumulative queue service rates, which in turn depend on the partial rates of the link infection rate in susceptible state (λ_e), service rate in the infected (μ_i) and recovering (μ_r) queues of each individual node. Without loss of generality these partial rates are considered the same for all users. It should be also noted that all initial input and services are exponential with rates as shown in Fig. 2(a).

The Norton equivalent queuing network obtained from Fig. 2(a) can be analyzed in turn using Jackson's Theorem for product form networks [19]. The latter will have a product form steady-state distribution and it is equivalent to a network of three cascade queues as shown in Fig. 2(b). The service rates of the final cascade network are directly obtained from the Norton equivalent, as $\mu_1 = \mu_S$, $\mu_2 = \mu_I$, $\mu_3 = \mu_R$. The arrival rates in the product-form network (Fig. 2(b)) can be obtained as:

$$\lambda_1 = \frac{1}{1-(1-p)(1-q)(1-w)}\lambda, \tag{1}$$

$$\lambda_2 = \frac{(1-p)}{1-(1-p)(1-q)(1-w)}\lambda, \tag{2}$$

$$\lambda_3 = \frac{(1-p)(1-q)}{1-(1-p)(1-q)(1-w)}\lambda. \tag{3}$$

as functions of the external input of susceptible nodes λ and the probabilities for customers to leave the network p, q, w.

The steady-state distribution of the cascade product-form network will be:

$$p(n_1, n_2, n_3) = p_1(n_1)p_2(n_2)p_3(n_3) \tag{4}$$

where n_1, n_2, n_3 is the number of users in the susceptible, infected and recovering states respectively and at every time instant $n_1 + n_2 + n_3 = n$, where n is the instantaneous total number of network nodes. Even though the combined inputs in Fig. 2(a) are not Poisson, thus nor are the outputs, Jackson's theorem allows to

treat each stage (queues in Fig. 2(b)) as independent M/M/r_i queues with input rate λ_i and total service rate μ_i, $i = 1, 2, 3$, where r_i is the number of parallel servers in each stage (here $r_1 = 2, r_2 = r_3 = 1$). An input policy regulating the arrival of new susceptible nodes with respect to the death/removal rates should be employed to ensure $n < \infty$, since all practical networks have finite nodes. Distribution $p_i(n_i)$ provides the number of users in each stage, and since the service rates of the two parallel queues in stage 1 are not the same, we consider the first stage as an M/M/2 queue with different service rates for the two servers and obtain its steady-state distribution as:

$$p_1(n_1) = \begin{cases} \left[1 + \frac{C}{\rho_1(1-\rho_1)}\right]^{-1}, n_1 = 0 \\ \frac{C}{\rho_1 + \frac{C}{1-\rho_1}}, n_1 = 1 \\ \rho_1^{n-2} \frac{C}{1 + \frac{C}{\rho_1(1-\rho_1)}}, n_1 \geq 2 \end{cases} \tag{5}$$

where $\rho_1 = \lambda_1/\mu_1$, C is a constant depending on λ_1, μ_1, given by:

$$C = \frac{\lambda_1^2}{2\mu_s^o \mu_s^r}, \tag{6}$$

and for the second and third stage, the distributions are respectively:

$$p_2(n_2) = \rho_2^{n_2} \frac{1-\rho_2}{\rho_2} \tag{7}$$

$$p_3(n_3) = \rho_3^{n_3} \frac{1-\rho_3}{\rho_3} \tag{8}$$

where $\rho_2 = \lambda_2/\mu_2$, $\rho_3 = \lambda_3/\mu_3$, $\rho_1, \rho_2, \rho_3 < 1$ and $n_1, n_2, n_3 \geq 0$.

The number of dead nodes is unimportant, since they do not participate in malware dynamics and in addition, it is assumed that new nodes are always available. The service rate of each queue in Fig. 2(b) is the equivalent service rate from Fig. 2(a), which in turn depends on the infection model, malware dynamics and the topology of a network.

The average number of users in the system is given by

$$L = L_1 + \sum_{i=2}^{3} p_{r_i} \frac{\rho_i}{(1-\rho_i)^2} \tag{9}$$

where L_i is the average number of users in each queue and $p_{r_i} = \frac{(\lambda_i/\mu_i)^{r_i}}{r_i!} p_{i,0}, i = 2, 3$. In this case, the average number of susceptible (operational) and infected legitimate nodes are respectively:

$$L_1 = \frac{C(1-\rho_1)}{\rho_1(1-\rho_1) + C} \left[1 + \frac{\rho_1(2-\rho_1)}{(1-\rho_1)^2}\right] \tag{10}$$

$$L_2 = \frac{\rho_2}{1-\rho_2}, L_3 = \frac{\rho_3}{1-\rho_3}. \tag{11}$$

Using the customer distributions (5), (7) and (8), other quantities of interest can be computed, e.g. the average throughput of stage 1 provides the average infection rate of the system. Similarly, the average throughput of stage 3 provides the average recovery rate of the system, while the average throughput of stage 2 the average healing rate of infected nodes. Weighting these throughput quantities by the corresponding loss rates p, q, w, the corresponding cumulative node churn loss rate is obtained.

Until this point the analysis is generic and applies to all types of networks with churn. However, the framework developed in Fig. 2, allows more detailed results to be obtained on a per network type case. For instance, apart from n_1, n_2, n_3, one may obtain analytical expressions of the average n_2 with respect to network parameters, such as the infection/recovery rates, node transmission radius and node densities of an ad hoc network. Such task is network type/scenario specific and depends on the topology type and operation. In the following, we will explore from a more practical perspective some of these possible results for multihop networks with churn.

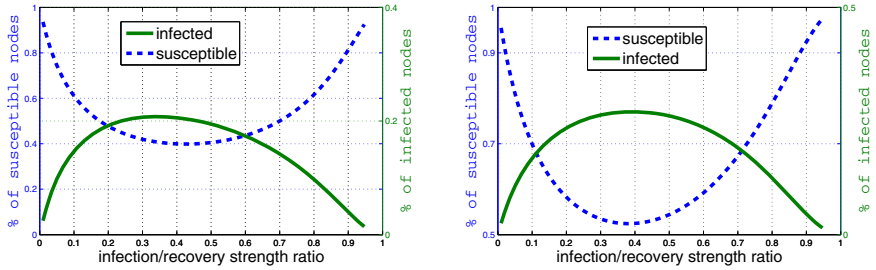
4 Behavior Evaluation in Wireless Distributed Networks

4.1 Simulation Setting

In this section we present numerical and simulation results regarding the operation and behavior of wireless distributed networks with churn, when attacked by a single attacker. Infected nodes are assumed to further propagate the infectious malware they received, while recovering nodes are prevented from doing so. This means that the spreading of malware is mainly due to the network, while the attacker has a smaller role in spreading dynamics, mostly needed to generate new infections in the event that a network manages to recover completely for an instance. Thus, the network spreading dynamics will be studied in the following.

We developed a discrete event simulator in Matlab to study the behavior of the attacked network. At each epoch (slot) of the simulator one event takes place, according to the current state of the system $\{n_1, n_2, n_3\}$, the topology of the network and the corresponding infection (S→I transition), recovering (I→R transition) and full-recovery rates (R→S transition). This is ensured by the nature of the system in Fig. 2.

For the multihop networks we focus on, the link infection rate λ_e of a susceptible node represents the probability that this user will become infected from a malicious neighbor. The multihop topology is considered in our case as a random geometric graph. Combining this with the link infection, a detailed analysis of the system in Fig. 2(a) yields the total infection rate, as the service rate of the single queue of susceptible nodes in the Norton equivalent (which is equal to μ_1 in the product-form equivalent). This infection rate will be $\sum_{i=1}^{n_1} k_i \lambda_e$, where k_i is the number of malicious neighbors of susceptible node i (counting both the attacker and infected legitimate nodes). The total recovering (corresponding to μ_2 in Fig. 2(b)) and full-recovery rates (corresponding to μ_3 in Fig. 2(b)) depend on n_2, n_3, and may be computed as $n_2\mu_i$, $n_3\mu_r$, respectively.



(a) Infection duration half of recovering. (b) Infection duration equal to recovery.

Fig. 3. Percentages of susceptible-infected nodes as a function of infection to recovery strength (numerical)

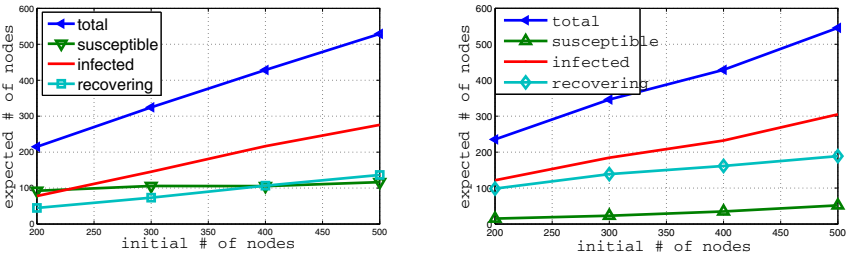
Due to space limitations we only provide some indicative results that can be used for the assessment of network reliability and attack potentials. Regarding node churn, we study the behavior of the system for positive churn, i.e. for a $\lambda/(p+q+w) > 1$, which means that the network will be growing on average. This is preferable for the study, as a decreasing network could sometimes lead to degenerate (disconnected) topologies, or even to the extinction of the network.

4.2 Numerical and Simulation Results

Fig. 3 presents some numerical results obtained from the analysis, valid for arbitrary networks, providing intuition on the behavior of the average number of nodes in the states of the system. Churn strength is equal to 1.67, which translates to a growing network. Notice the different scales in the vertical axes in both figures and for both y-axes of each figure, indicating how the expected number of susceptible and infected nodes vary with respect to the time each node is expected to spend in each of the three stages (service rates).

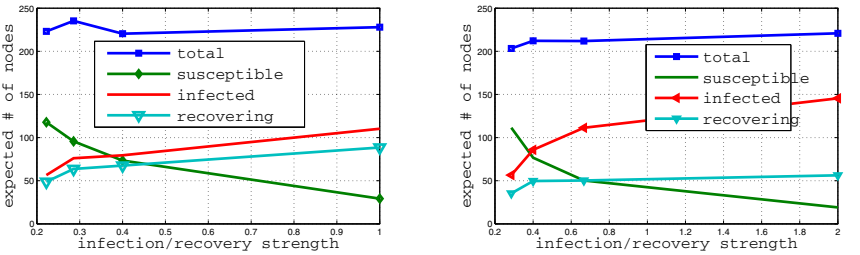
As expected, a decrease in susceptible nodes translates to an increase in the infected nodes. By comparing Fig. 3(a) and Fig. 3(b), it can be also observed that regarding the dependence on the infection/revocery strength, some symmetry (Fig. 3(b)) should be expected when the recovery (μ_i) and full recovery (μ_r) rates are the same. These results, and many similar that can be obtained from the expressions provided before, can be used to assess the robustness of the network. Malware dynamics are represented via the infection and recovery rates, while the full recovery rate represents the countermeasures' efficiency. Thus, given these parameters, the expected state of the system can be evaluated.

The following results have been obtained through simulations, in which a square deployment region with size $L = 1000m$ was employed and all devices used a transmission radius $R_t = 150m$. Fig. 4 presents the expected number of nodes in each state of the system as a function of network density (we fixed the deployment region and increased progressively network nodes). Fig. 4(a) regards a network with uneven recovery-full recovery rates, $\mu_i - \mu_r$ respectively.



(a) Uneven recovery-full recovery rates. (b) Even recovery-full recovery rates.

Fig. 4. Expected number of nodes in each state of the network with respect to network density



(a) Even recovery-full recovery rates. (b) Uneven recovery-full recovery rates.

Fig. 5. Expected number of nodes in each state of the network with respect to infection/recovery rates

This means that the mean infection and recovery times will be uneven as well. Fig. 4(b) shows the corresponding results for even rates.

It is observed that as the network density increases, so do the expected number of nodes in each state, and such increase is almost linear. However, the corresponding increase rates are different for uneven recovery-full recovery rates and similar for even rates. In both cases, the infection to full recovery strength is $\lambda_e/\mu_r = 2$. This also explains the fact that the number of infected nodes is the smallest compared to infected and recovering nodes, revealing potential vulnerabilities for the network with respect to the specific malware dynamics and the network structure, as it was also possible to do with the numerical results we presented before.

However, different trends emerge regarding the expected number of nodes in each state with respect to the infection/recovery strength, as shown in Fig. 5. As before, the expected number of susceptible nodes has a complementary behavior to the expected number of infected and recovering nodes. The trend though is not linear. In fact, the number of recovering nodes, especially in Fig. 5(b) seems to saturate for increasing infection/recovery strength. Such results can be again

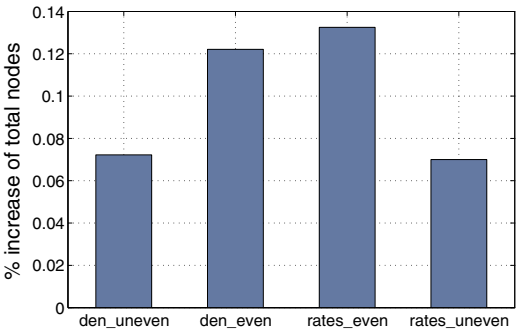


Fig. 6. Expected percentage variation of the total number of nodes with respect to node density and infection/recovery strength

used to evaluate the robustness of the network with respect to the expected behavior under various attack-countermeasure parameters.

Finally, Fig. 6 shows the average percentage difference of network size for equal/unequal infection/recovery strengths and with respect to node density and the intensity of the infection/recovery strength. As expected, this difference is positive (even though small in some cases, since the churn strength was set slightly higher than 1 in all scenarios to ensure a proper topology). The first two bars in Fig. 6 are the average node increase as the density of the network increases, while the last two bars represent the average node count increase for increasing infection/recovery strength. It can be observed that in general even infection-recovery strengths yield higher increase than uneven ones. Equal infection/recovery rates corresponds to strategies providing countermeasures that match the effect of malware at the same time scales, which in turn allow the network to maintain more nodes on average by preventing some I→D transitions (infected nodes becoming dead) due to malware.

5 Conclusions

In this work, we exploited and adapted a queuing framework for modeling malware spreading in wireless multihop networks that exhibit node churn due to malicious attacks and/or energy depletion/recharging. We obtained general expressions for the number of infected nodes in the steady-state of such systems and studied the potentials of the network behavior for possible varying attack profiles. These outcomes can be exploited for enhancing network robustness and security against a broad spectrum of attacks and for various network topologies. Our future work will focus on obtaining spreading optimal controls for malware non-propagative and propagative wireless distributed networks both from the attackers' and network's perspectives.

References

1. Wang, P., Gonzalez, M., Hidalgo, C., Barabasi, A.: Understanding the Spreading Patterns of Mobile Phone Viruses. Science **324**, 1071–1075 (2009)
2. Peng, S., Yu, S., Yang, A.: Smartphone Malware and its Propagation Modeling: A Survey. IEEE Commun. Surv. and Tutorials **16**(2), 925–941 (2014)
3. Wang, Y., Wen, S., Xiang, Y., Zhou, W.: Modeling the Propagation of Worms in Networks: A Survey. IEEE Commun. Surv. and Tutorials **16**(2), 942–960 (2014)
4. Daley, D.J., Gani, J.: Epidemic Modelling: An Introduction. Cambridge University Press (2009)
5. Karyotis, V., Kakalis, A., Papavassiliou, S.: Malware-Propagative Mobile Ad Hoc Networks: Asymptotic Behavior Analysis. Journal of Computer Science and Technology (JCST) **23**(3), 389–399 (2008)
6. Khouzani, M., Sarkar, S., Altman, E.: Maximum Damage Malware Attack in Mobile Wireless Networks. IEEE/ACM Trans Netw. **20**(5), 1347–1360 (2012)
7. Karyotis, V., Papavassiliou, S.: Macroscopic Malware Propagation Dynamics for Wireless Complex Networks with Churn. IEEE Commun. Letters (submitted)
8. Shiu, Y.-S., Chang, S.Y., Wu, H.-C., Huang, S.C.-H., Chen, H.-H.: Physical Layer Security in Wireless Networks: A Tutorial. IEEE Wirel. Commun. Mag. **18**(2), 66–74 (2011)
9. Zou, C.C., Towsley, D., Gong, W.: Email Virus Propagation Modeling and Analysis, Technical Report: TR-CSE-03-04 (April 2004)
10. Pastor-Satorras, R., Vespignani, A.: Epidemic Spreading in Scale-Free Networks. Phys. Rev. Lett. **86**, 3200–3203 (2001)
11. Zou, C.C., Gong, W., Towsley, D., Gao, L.: The Monitoring and Early Detection of Internet Worms. IEEE/ACM Trans. Netw. **13**(5), 961–974 (2005)
12. Garetto, M., Gong, W., Towsley, D.: Modeling Malware Spreading Dynamics. In: Proc. 22nd Annual Joint Conf. IEEE Comp. and Commun. Societies (INFOCOM), vol. 3, pp. 1869–1879 (March-April 2003)
13. Ganesh, A., Massoulie, L., Towsley, D.: The Effect of Network Topology on the Spread of Epidemics. In: Proc. 25th Annual Joint Conf. IEEE Comp. and Commun. Societies (INFOCOM), vol. 2, pp. 1455–1466 (March 2006)
14. Karyotis, V., Papavassiliou, S., Grammatikou, M., Maglaris, V.: A Novel Framework for Mobile Attack Strategy Modeling and Vulnerability Analysis in Wireless Ad-hoc Networks. Int'l Journal of Security and Networks (IJSN) **1**(3/4), 255–265 (2006)
15. Khouzani, M., Sarkar, S.: Dynamic Malware Attack in Energy-Constrained Mobile Wireless Networks. In: Proc. 5th Symp. Inf. Theory and Applications, UCSD (February 2010)
16. Khouzani, M., Sarkar, S., Altman, E.: Maximum Damage Malware Attack in Mobile Wireless Networks. In: Proc. 29th IEEE Conf. on Computer Communications (INFOCOM) (March 2010)
17. Holzer, S., Pinkolet, Y.A., Smula, J., Wattenhofer, R.: Monitoring Churn in Wireless Networks. Elsevier Journal of Theoretical Computer Science **453**, 29–43 (2012)
18. Schwartz, M.: Telecommunications Networks. Addison-Wesley, USA (1987)
19. Bertsekas, D., Gallager, R.: Data Networks, Prentice Hall, 2nd edn., USA (1992)