General Worm Propagation Model for Wireless Ad Hoc Networks

Chen Junhua
School of Computer Science and Technology
Beijing Institute of Technology
Beijing, China
chenjunhuabj@163.com

Wei Shengjun, Peng Wu
Lab for Computer Network Defense Technology
Beijing Institute of Technology
Beijing, China
{sjwei, wpeng}@bit.edu.cn

***Abstract*—The popularity of wireless communication networks makes them an attractive target to the creators of worms and other malicious code. Indeed, recently a number of worms designed specifically to spread via these wireless networks have emerged. Based on the epidemic theory, this paper proposes a general model which predicts how a worm propagates through a wireless ad hoc network. Then the differential equations of the model is presented and a necessary condition for worms to spread in these networks is derived, which may be useful in designing a secure wireless ad hoc network. Simulation results show that the process of worm propagation in these wireless networks is sensitive to the deployment density of nodes and the energy consumption of nodes. Therefore, our study can provide insight into deriving a general model to characterize worm propagation in wireless ad hoc networks.**

Keywords-wireless network; worm; epidemiology; threshold

I. INTRODUCTION

A dramatic increase in the number of computing devices with wireless communication capability has resulted in the emergence of a new class of computer worms which specifically target such devices. The most striking feature of these worms is that they do not require Internet connectivity for their propagation but can spread directly from device to device using a short-range radio communication technology [1], [2], such as Wireless Sensor Networks (WSNs), creating in their wake an ad hoc network along which they propagate. The first worm written specially for wireless devices was detected in 2003 and within several years the number of such worms soared from one to more than 300 [3]. With wireless ad hoc networks being increasingly popular, many security experts predict that these networks will soon be a main target of attacks by worms and other type of malware.

To defend against such worms, we need to accurately understand the dynamic characteristics of worm propagation in networks. By modeling the process of worm propagation in wireless ad hoc networks, we can effectively analyze the trace of worm propagation, and precisely predict the trend of worm propagation in the future. In particular, by using a general model of worm propagation, we may estimate the time point at which worms start to quickly spread in these networks in order to take preventing measures.

The paper is structured as follows. In the remainder of the introduction, we highlight the salient features of wireless ad hoc networks and discuss related work. Section II proposes a general worm propagation model for the wireless networks. In Section III, we present differential equations of this model. In addition, we also derive a necessary condition for worms to spread in a wireless ad hoc network. In Section IV, the model simulations results and analysis are given. Conclusion of this paper and some future work are given in Section V.

A. Wireless Ad Hoc Networks Overview

Wireless ad hoc networks are a new paradigm of wireless communication for mobile hosts (which we call *nodes*). In an ad hoc network, there is no fixed infrastructure such as base stations or mobile switching centers. Mobile nodes that are within each other's radio range communicate directly via wireless links, while those that are far apart rely on other nodes to relay messages as routers. Node mobility in an ad hoc network causes frequent changes of the network topology.

Military tactical and other security-sensitive operations are still the main application of wireless ad hoc networks today. For example, military units (e.g., soldiers, tanks or planes), equipped with wireless communication devices, could form an ad hoc network when they roam in a battlefield. Since an ad hoc network can be deployed rapidly with relatively low cost, it becomes an attractive option for commercial uses such as wireless sensor networks or virtual classrooms.

But the process of worm propagation in wireless ad hoc networks has some new characteristics. For example, 1) a worm residing in a node just directly spread to its neighbors, but not through the IP addresses; 2) a node becomes a dead one when the energy of node is exhausted, the dead no longer participate in the process of worm propagation. Hence, In order to meet the uninterrupted communication between wireless ad hoc network nodes, it may be necessary to choose the right time to deploy some new nodes network.

B. Related Work

The advent of mathematical Epidemiology - the field of biology which models how diseases spread in a population - is generally credited to McKendrick and his seminal 1925 paper [4]. Previous work in applying epidemiology to modeling how computer viruses and other malware spread between machines dates back to the late 1980s/early 1990s: Kephart and White published a paper [5] on the topic in 1991.

978-1-4244-4520-2/09/$25.00 ©2009 IEEE

More recently, Zou *et al*. utilized epidemiology to model the spread of the *Code Red* across the Internet [6].

There have been a number of recent papers which model worm propagation in wireless ad hoc networks. Two notable examples include and a 2007 paper by Yan *et al*. [7] which analyze the worm propagation in Bluetooth networks and investigate the impact of mobility patterns on Bluetooth worm propagation, and a 2008 paper by Maziar Nekovee [8] which use a combination of large-scale simulations and mathematical modeling to explore epidemic spreading of wireless worms in fixed ad hoc networks.

II. MODEL DESCRIPTION

Simple wireless network worm is similar to biological viruses in their self-replicating and propagation behaviors, thus the mathematical methods can be adapted to the study of this worm propagation. Motivated by these methods (e.g., [9] and [10]), we propose a general model for wireless ad hoc networks based on [9], at the same time, we also take into the situation of new nodes joining the network account.

A. Model Assumption

The intent of our model is to predict the expected behaviors of a worm which spreads through a wireless ad hoc network. Hence we make the simplifying assumption that this initial wireless network consists of N devices, each device is called a node. All nodes are distributed in a two dimensional plane (e.g. an $H*H$ area) which communicate using short-range radio transmissions. The energy of each node is provided by batteries with limited power, and the batteries may not be recharged. In addition, we consider that temporal characteristics of the underlying wireless network such as processing delays are likely to have a significant effect on the propagation of worms. In the current study we model the processing time required by a worm to complete the infection of a node as a constant value of one clock tick, and assume that the wireless transmission time of worm packets can be considered instantaneous (or at least is much smaller than the processing time).

We classify all nodes in the network as falling into one of the following four sets (states):

Susceptible node set S: the nodes in S have not been infected by any worm in the network and these nodes are vulnerable to the worms.

Infectious node set I: the nodes in I have been infected by worms in the network and they may infect some nodes in S.

Recovered node set R: the nodes in R used to be infected by worms, they are cleaned of worms and are immune to the same type of cleaned worms; However, recovered nodes may be infected by new worms occurring in the network in the future.

Dead node set D: the nodes in D never work with their energy exhausted. Thus any worm cannot infect these nodes. Usually, the set D includes the nodes which cannot work from now on. For example, the nodes which have exhausted their energy or which are physically destroyed or which are logically removed from the network, and so forth.

Further, we assume that all of worms only reside in some nodes in I; in a unit time the state of each node is one of the four states. A node transits from its current state to another with the *S->I->R->S* mechanism of worm propagation.

Table I lists all parameters and notations in this model.

TABLE I. NOTATIONS USED IN THIS PAPER

Symbol	***Explanation***
β	Probability with which a node in S becomes a node in I
γ	Probability with which a node in I becomes a node in R
λ	Probability with which a node in R becomes a node in S
δ_1	Probability with which a node in S becomes a node in D
δ_2	Probability with which a node in I becomes a node in D
δ_3	Probability with which a node in R becomes a node in D
h	Wireless communication radius of each node
H	Edge with which nodes are deployed in a square area
M	Number of new nodes deployed into the wireless ad hoc network (initial value $M = 10$).
$A(t)$	Number of susceptible neighbors of each node at given unit time t
$S(t)$	Number of vulnerable nodes at given unit time t in the whole network ($S(0)$ is number of vulnerable nodes at the initial time, initial value $S(0) > 0$, e.g. $S(0) = 50000$)
$I(t)$	Number of infectious nodes at given unit time t in the whole network (initial value $I(0) > 0$, e.g. $I(0) = 1$)
$R(t)$	Number of recovered nodes at given unit time t in the whole network (initial value $R(0) = 0$)
$D(t)$	Number of dead nodes at given unit time t in the whole network (initial value $D(0) = 0$)

B. Transition Relationship between Node States

Based on the above assumptions and the epidemic theory [11], at the same time, we suppose that the initial state of M nodes newly deployed is susceptible every time, so the nodes state transition relationships can be shown in Fig. 1 below in a wireless ad hoc network.

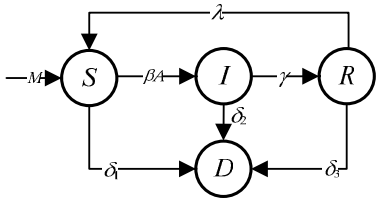

Figure 1. The graph of nodes state transition in wireless ad hoc networks.

III. MODEL EQUATIONS

According to the assumptions in Section II, we can get the communication area of each node and that of its corresponding wireless network is πh^2 and H^2, respectively. It is well known that the communication capability of each note is proportional to its density in a wireless ad hoc network. And then Denotes $\rho(t)$ as the nodes density at instant t in S, i.e. $\rho(t) = S(t)/H^2$. Hence the number of susceptible neighbors of each node is calculated by (1) at instant t.

$$A(t) = \rho(t)\pi h^2 = \frac{\pi h^2}{H^2} S(t) \quad (1)$$

Let $[t, t+\Delta t]$ be a time interval. Here, Δt is a segment of time starting from t ($\Delta t \geq 0$) and it is small enough. According to the epidemic theory and the state transition relationship of nodes (see Fig. 1), the fluctuating number of nodes in S from t to $t+\Delta t$ is calculated by (2).

$$S(t+\Delta t) - S(t) = (M + \lambda R(t) - \beta A(t) I(t) - \delta_1 S(t))\Delta t \quad (2)$$

From (1) and (2), the fluctuating number of nodes in S from t to $t+\Delta t$ is calculated by (3).

$$S(t+\Delta t) - S(t) = (M + \lambda R(t) - \frac{\pi h^2}{H^2} \beta S(t) I(t) - \delta_1 S(t))\Delta t \quad (3)$$

The total number of nodes in a large scale wireless ad hoc network could be generally very large. Hence we may believe that the number of nodes in different states continually changes within Δt . So we derive the differential equation (4) from (3).

$$\frac{dS(t)}{dt} = M + \lambda R(t) - \frac{\pi h^2}{H^2} \beta S(t) I(t) - \delta_1 S(t) \quad (4)$$

Similar to the derivation of (4), so we can derive the following differential equations (5) from Fig.1.

$$\begin{cases} \dfrac{dS(t)}{dt} = M + \lambda R(t) - \dfrac{\pi h^2}{H^2} \beta S(t) I(t) - \delta_1 S(t) \\ \dfrac{dI(t)}{dt} = \dfrac{\pi h^2}{H^2} \beta S(t) I(t) - \gamma I(t) - \delta_2 I(t) \\ \dfrac{dR(t)}{dt} = \gamma I(t) - \lambda R(t) - \delta_3 R(t) \\ \dfrac{dD(t)}{dt} = \delta_1 S(t) + \delta_2 I(t) + \delta_3 R(t) \end{cases} \quad (5)$$

In the following, we derive a necessary condition for worms to spread in a wireless ad hoc network and it may be useful in designing a secure wireless ad hoc network.

Theorem 1: For a general wireless ad hoc network, all nodes are uniformly deployed in a circle area with radius H. the initial number of susceptible nodes is $S(0)$. A worm in an infectious node may spread to any node of neighbors in the network, if and only if the condition $S(0) > \dfrac{(\gamma + \delta_2) H^2}{\beta \pi h^2}$ is satisfied. Otherwise, a worm can not spread in the network. Here, γ, δ_3 β and h are the same as ones of Table I, respectively.

Proof If a worm in an infectious node can successfully spread in a wireless ad hoc network at the initial instant $t = 0$, then the following condition must be satisfied.

$$\left.\frac{dI(t)}{dt}\right|_{t=0} > 0 \quad (6)$$

In other words, the spread rate of the worm must be greater than zero. From the 2nd equation of (5), the following condition must be satisfied.

$$\frac{\pi h^2}{H^2} \beta S(0) I(0) - \gamma I(0) - \delta_2 I(0) > 0 \quad (7)$$

From (7) and the assumptions of Section II: $I(0)>0$, the following condition is derived.

$$S(0) > \frac{(\gamma + \delta_2) H^2}{\beta \pi h^2} \quad (8)$$

Therefore, Theorem 1 is correct. We represent the right of (8) by θ as follows.

$$\theta = \frac{(\gamma + \delta_2) H^2}{\beta \pi h^2} \quad (9)$$

Theorem 1 implies when the number of the initial susceptible nodes is not greater than θ, a worm may not spread in wireless ad hoc network. Hence, we consider θ as the threshold for a worm to spread in this network.

IV. Simulation And Analysis

In this section we provide some examples of worms' behaviors and corresponding performance data for the general model, before implementing numerical simulation, we firstly define the following evaluation model.

A. Evaluation Model

In order to evaluate worm propagation in a general wireless ad hoc network, we build an evaluation model. In this model we consider three aspects as follows:

- *Metrics*: worm spread performance is defined as follows: the time taken t (X axis) and the numbers of corresponding nodes in different states (Y axis).

- *Evaluation network*: The general wireless ad hoc network is defined by the tuple: <*S*, *I*, *R*, *D*, *h*, *H*, *M*, β, λ, γ, δ_1, δ_2, δ_3>. Parameters are defined in Table I.
- *Evaluation Method*: We use Matlab Simulink tool to obtain performance data.

B. *Performance Results*

In this section, we report the performance results along with observations. Due to limitation of space, we only present a limited number of cases here.

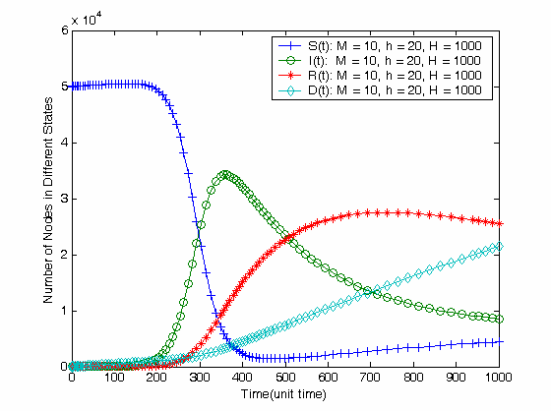

Figure 2. The number of nodes in different states.

Fig. 2 illustrates how the number of nodes falling into each of the four states evolves over time. The general wireless ad hoc network is configured as <50000, 1, 0, 0, 20, 1000, 10, 0.00065, 0.004, 0.001, 0.0001, 0.0005, 0.0008>. From this figure, we have the following observations:

- The number of infectious nodes rapidly increases at the initial spreading phase of worm propagation in this wireless network then quickly decreases, and then changes at a relatively stable level.
- The number of dead nodes slowly increases, in contrast, that of susceptible nodes quickly decreases if *M* is small or new *M* nodes not be timely deployed.

These dynamic characteristics of worm propagation in this network are very similar to ones on the Internet. The reason is obvious: the initial number of susceptible nodes is relatively large, which results in a fast increase of infectious nodes. When the total number of nodes in a wireless network has a very small change, the fast increase of infectious nodes must lead to a fast decrease of susceptible nodes.

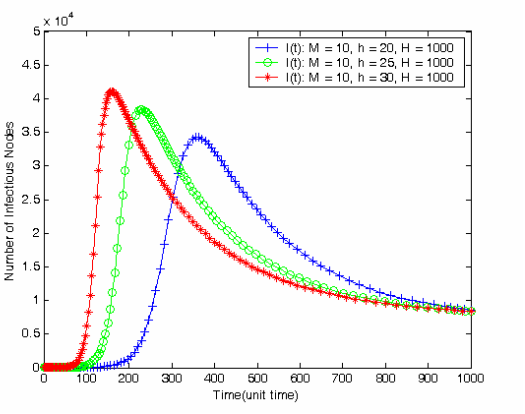

Figure 3. The number of infectious nodes in different *h*.

Fig. 3 shows the number of infectious nodes on sensitivity of worm propagation for different *h*. The general wireless ad hoc network is configured as <50000, 1, 0, 0, *, 1000, 10, 0.00065, 0.004, 0.001, 0.0001, 0.0005, 0.0008>. From this figure, we observe the following:

- The larger the communication radius of nodes is, the earlier the spreading beginning time of worms in the network is.
- The value of *h* affects the maximal number of infectious nodes. That is, the bigger the value of *h* is, the larger the maximal number of infectious nodes is.

The reason is that there are more susceptible nodes in the communication range of infectious nodes in a given unit time. As a result, there may be more susceptible nodes to be infected by worms residing in infectious nodes.

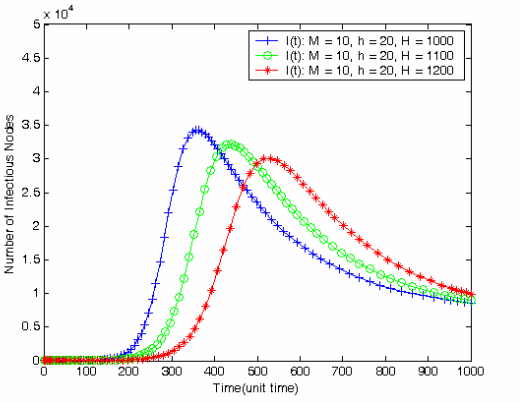

Figure 4. The number of infectious nodes in different *H*.

Fig. 4 shows the number of infectious nodes on sensitivity of worm propagation for different *H*. The general wireless ad hoc network is configured as <50000, 1, 0, 0, 20, *, 10, 0.00065, 0.004, 0.001, 0.0001, 0.0005, 0.0008>. From this figure, we observe the following:

- The smaller the communication area (i.e., *H*) of the network is, the earlier the spreading beginning time of worms in the network is, and the faster the worm spreads.

- The value of H affects the maximal number of infectious nodes. That is, the bigger the H is, the smaller the maximal number of infectious nodes is.

The reason is that a bigger value of H decreases the density of nodes in the network, further decreases the number of susceptible nodes in the communication ranges of infectious nodes. As a result, there may not be more susceptible nodes to be infected by worms residing in infectious nodes.

At last, we analyze the number of infectious nodes on sensitivity of worm propagation in the wireless ad hoc network for different $S(0)$. For simplicity, using the parameter initial values in Fig. 2, we calculate a threshold θ = 5509 by (9). Let $S(0)$ be 5509, 6700 and 7000, respectively.

Taking into account the energy consumption of nodes in a wireless ad hoc network, some new nodes are regularly deployed in some ad hoc network applications, for example, the ambient temperature monitoring. On the other hand, no new node is deployed into the existing wireless network later, e.g., a specific and quick war. So two cases $M = 0$ and $M > 0$ will be discussed under the different $S(0)$, respectively.

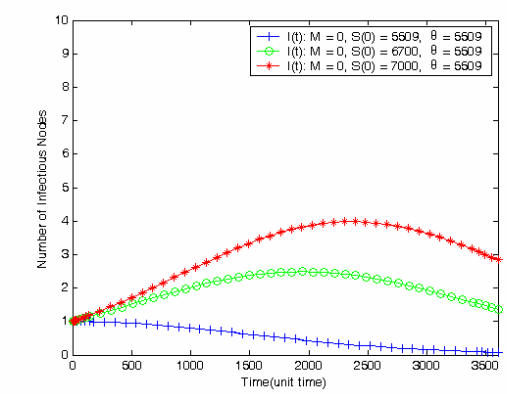

Figure 5. The number of infectious nodes in different $S(0)$ and $M = 0$.

Fig. 5 shows the number of infectious nodes for different $S(0)$ and M = 0. The general wireless ad hoc network is configured as <*, 1, 0, 0, 20, 1000, 0, 0.00065, 0.004, 0.001, 0.0001, 0.0005, 0.0008>. From this figure, we have made the following observations:

- When the number of initial susceptible nodes equals the threshold of worm propagation in a specific wireless ad hoc network, i.e., $S(0)$ = 5509, a worm may not spread in the network.
- When the number of initial susceptible nodes is greater than the threshold of worm propagation, a worm may spread in the network. Moreover, the larger the value of $S(0)$ is, the faster the worm spreads. The numerical simulation results are consistent with Theorem I in Section III.

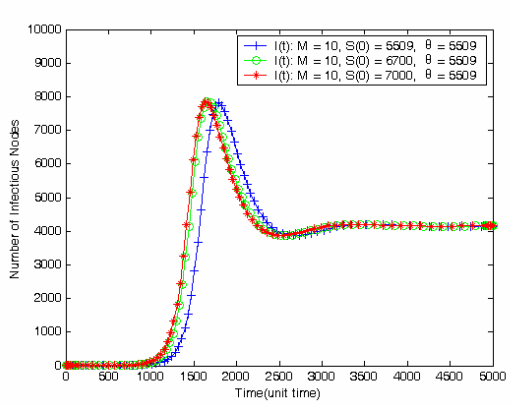

Figure 6. The number of infectious nodes in different $S(0)$ and $M > 0$.

Fig. 6 shows the number of infectious nodes for different $S(0)$ and M > 0. The general wireless ad hoc network is configured as <*, 1, 0, 0, 20, 1000, 10, 0.00065, 0.004, 0.001, 0.0001, 0.0005, 0.0008>. From this figure, this phenomenon is similar to the worm propagation scenario on the Internet, the number of infectious hosts fluctuates firstly in a certain range, and then changes at a relatively stable level, for more information, the readers can refer to our another paper [12].

From the above simulation results and analysis, the dynamic characteristics of worm propagation are mainly related to the network topology and the energy consumption of nodes in a wireless ad hoc network.

V. CONCLUSION

In this paper, we propose a general model for the propagation of a new class of worms which specifically target wireless computing nodes. According to this model, a necessary condition for such worms to spread in wireless ad hoc networks is theoretically derived. Our numerical analysis results are provided to demonstrate the validity of the model. Based on the proposed model, how to automatically adjust the communication range of nodes to control the process of worm propagation will be an interesting direction. As future work, we plan to consider more other factors on the impact of the spread of worms in these networks, such as the limited bandwidth and wireless translation delay.

ACKNOWLEDGMENT

This paper is partially supported by Beijing key discipline program.

REFERENCES

[1] Kleinberg, Jon, “Computing: The wireless epidemic,” Nature, vol.449, Sep 2007, pp. 287-288, doi:10.1007/978-3-540-92191-2.

[2] Dagon, D.; Martin, T.; Starner, T, “Mobile phones as computing devices: the viruses are coming!” Pervasive Computing, IEEE Press, vol.3, pp.11-15, doi: 10.1109/MPRV.2004.21.

[3] Hypponen M. “Malware goes mobile,” Scientific American, vol.295, no5, Nov 2006, pp.70-77.

[4] A.G. McKendrick, “Applications of Mathematics to Medical Problems,” Proceedings of the Edinburgh Mathematical Society, vol.44, 1925, pp.94-130, doi:10.1017/S0013091500034428.

[5] Kephart, J.O. White, S.R, "Directed-graph epidemiological models of computer viruses," Research in Security and Privacy, 1991. Proceedings., 1991 IEEE Computer Society Symposium on, Oakland, CA, USA, May 1991, pp. 343-359, doi: 10.1109/RISP.1991.130801.

[6] C.C. Zou, W. Gong, and D. Towsley, "Code red worm propagation modeling and analysis," Proceedings of the 9th ACM conference on Computer and communications security, Washington, DC, USA, Nov 2002, pp.138-147, doi: 10.1145/586110.586130.

[7] G. Yan and S. Eidenbenz, "Modeling Propagation Dynamics of Bluetooth Worms," IEEE ICDCS'07, IEEE Press, Canada, June 2007, pp.353-368, doi: 10.1109/TMC.2007.129.

[8] Maziar Nekovee, "Epidemic Spreading of Computer Worms in Fixed Wireless Networks," Computing & Communication, Springer-Verlag, vol.5151, Nov 2008, pp.105-115, doi:10.1007/978-3-540-92191-2.

[9] Xiaoming Wang, Qiaoliang Li and Yingshu Li, "EiSIRS: a formal model to analyze the dynamics of worm propagation in wireless sensor networks," Combinatorial Optimization, Springer Netherlands, vol.10, Oct 2008, pp.1-16, doi:10.1007/s10878-008-9190-9.

[10] Wang X, Li Y, "A improved SIR model for worm propagation in wireless sensor networks," Chin J Electron. J. vol. 18, pp.28-32, 2008.

[11] Frauenthal JC. Mathematical modeling in epidemiology, Springer-verlag, New York Inc, Nov. 1980, pp.12-24.

[12] Chen Junhua, Wei Shengjun. "Modeling and Analyzing the Spread of Worms with Bilinear Incidence Rate," unpublished.