Model and Dynamic Behavior of Malware Propagation over Wireless Sensor Networks

Yurong Song and Guo-Ping Jiang

Center for Control and Intelligence Technology, Nanjing University of Posts and Telecommunications, Nanjing, 210003, China
{songyr,jianggp}@njupt.edu.cn

Abstract. Based on the inherent characteristics of wireless sensor networks (WSN), the dynamic behavior of malware propagation in flat WSN is analyzed and investigated. A new model is proposed using 2-D cellular automata (CA), which extends the traditional definition of CA and establishes whole transition rules for malware propagation in WSN. Meanwhile, the validations of the model are proved through theoretical analysis and simulations. The theoretical analysis yields closed-form expressions which show good agreement with the simulation results of the proposed model. It is shown that the malware propagation in WSN unfolds neighborhood saturation, which dominates the effects of increasing infectivity and limits the spread of the malware. MAC mechanism of wireless sensor networks greatly slows down the speed of malware propagation and reduces the risk of large-scale malware prevalence in these networks. The proposed model can describe accurately the dynamic behavior of malware propagation over WSN, which can be applied in developing robust and efficient defense system on WSN.

Keywords: wireless sensor networks, malware propagation, model, cellular automata, neighborhood saturation, MAC mechanism, theoretical analysis.

1 Introduction

Wireless sensor networks have been widely used for many interesting and new applications such as environmental monitoring, patient health care monitoring, detection of chemical or biological threats, and military surveillance, tracking and targeting [1]. One key issue is various types of security treats [2, 3] in wireless sensor networks which are highly distributed and resource constrained environments. Attacks against wireless sensor networks could be denial of service, worm, Sybil attack and other malicious codes.

Worm and virus attacks on the Internet have been widely studied [4-8]. Some studies have greatly contributed to our understandings of various security issues and threats to wireless Ad hoc networks. However, wireless sensor networks differ from wireless Ad hoc networks and traditional computer networks in various aspects: First, wireless sensor networks are highly distributed system and consist of a great number of distributed nodes (sensor nodes) with the ability to monitor its surroundings.

J. Zhou (Ed.): Complex 2009, Part I, LNICST 4, pp. 487 – 502, 2009.
© ICST Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2009

Second, sensor nodes are limited in power, computational capacities, and memory[1]. Finally, self-organization is a fundamental feature of wireless sensor networks[9]. Those security mechanisms on Internet or wireless Ad hoc networks could not be applied directly to wireless sensor networks.

Investigation of worms spreading in wireless sensor networks has attracted some researchers [10-12]. Khayam and Radha [10] apply signal processing technique to model space-time propagation dynamics of topologically-aware worms in a sensor network with uniformly distributed nodes. They integrate physical, data link, network and transport protocol characteristics into the proposed model of worm propagation and obtain a closed-form expression of the infected population. De *et al*. [11] model and analyze the node compromise spreading process and identify key factors determining potential outbreaks of such propagations. In particular, they perform their study on random graphs precisely constructed according to the parameters of the network. However, the random graph model is homogeneous, which conflicts with the characteristic that sensor nodes relate closely to the location in WSN. Therefore, the spreading models based on random graph model are not suitable for investigating the propagation over WSN. Afterwards, the authors of Ref.[11], in their another paper [12], point out that the analytical model of [11], based on random graphs, fails to capture the temporal dynamics of the comprise propagation and only succeeds in capturing the outcome of the infection. Furthermore, the authors propose an epidemic theoretic model for evaluating broadcast protocols in wireless sensor networks. However, the model assumes that the number of neighbors that can be infected by any infected node is proportional to all susceptible nodes in the network (see in Eq.(2) and (3) of [12]). The assumption results in an inaccurate evaluation on spreading speed in the process of malware propagation.

Cellular automata (CA) is a mathematical model for complex natural systems [13-16], containing large numbers of simple identical components with local interactions. There is a substantial literature [13, 16-19] on the mathematical model based on cellular automata in epidemiology of theoretical biology. These models based on cellular automata focus on the local characteristics of the disease spreading process influencing the global behavior of the system. However, considering the inherent characteristics of WSN, it is unsuitable that the existing models for epidemiology are applied directly to malware propagation of wireless sensor network.

CA can simulate various uncertain behaviors of complex system, which is difficult for those models based on deterministic equations. Furthermore, CA is easy to realize on computer due to its spatial-temporal discrete property and massively parallel computation. An example of application of cellular automata in wireless sensor networks can be found in [20]. Cunha *et.al*. verify the possibility of using cellular automata to simulate the behavior of a WSN and a simulator has been developed to evaluate an algorithm for a very common problem in sensor networks: the topology control. Particularly, the self–organization and the local interaction are the inherent properties of WSN, which are similar to CA, so CA can be applied to model and simulate the malware propagation in WSN.

In this paper, we focus on the inherent characteristics of WSN and the dynamic process of malware propagation in WSN is modeled and analyzed using cellular automata. The validations of the model are performed through theoretical analysis and simulations. The theoretical analysis yield closed-form expressions which show good

agreement with the result of the proposed model. The theoretical analysis and simulation results demonstrate that the proposed model characterizes fully the localization and the spatial-temporal correlation and the model is appropriate to simulate malware propagation in WSN. An evolving pattern in the 2-D cellular space is obtained easily under different time using the model. It is shown that the assumption of homogeneous mixing of nodes causes an inaccurate evaluation on spreading speed in the process of worm propagation. Our model and theoretical analysis show that the initial growth of the malware is significantly slower than the exponential growth observed in malware propagation in [11, 12]. Our research shows malware propagation in WSN unfolds neighborhood saturation, which dominates the effects of increasing infectivity and limits the spread of the malware. In addition, MAC mechanism of wireless sensor networks greatly slows down the speed of malware propagation and reduces the risk of large-scale malware prevalence in these networks. The proposed model is able to describe accurately the dynamic behavior of malware propagation on WSN, and can be used for developing robust and efficient defense system on WSN.

The rest of this paper is organized as follows. In Section 2, a few of related analysis and assumption are described. In Section 3, we propose a new model and establish the transition rules for malware propagation in WSN. Neighborhood saturation in process of malware propagation is pointed out in Section 4. In Section 5, a theoretical analysis is presented. In Section 6, the simulations are presented. Finally, the conclusions are given in Section 7.

2 Related Analysis and Assumption

Considering the inherent characteristics of WSN and the spatial-temporal correlation of malware propagation over WSN, some key factors are given and discussed in this section.

2.1 Routing Mechanism

In general, a more robust mechanism for packets routing in wireless sensor networks is by multi-hop broadcasts[1]. Since the transmission power of a wireless radio is attenuated in a squared or even higher order with the distance, multi-hop routing will consume less energy than direct communication. The attackers take advantage of the broadcast mechanism to propagate malicious codes such that malware spreads quickly to the entire network[21]. We assume that infected nodes adopt multi-hop broadcasting strategy to spread malware to their neighbors. Furthermore, the adopted broadcast protocol ensures that each infected node broadcasts the malware to its neighbors only once for the purpose of preventing broadcast storm.

2.2 Infected Rate

The infected rate is related to many factors, such as authentication mechanism for securing data exchanging, attack characteristic of malware and communication pattern. For simplicity, these factors are integrated into a parameter, namely, the infected rate β, with the value being from 0 to 1.

2.3 Death Rate

It is well known that sensor nodes are severely restricted in terms of computation power and communication capability, especially energy. Malware propagation between nodes results in nodes consuming continuously energy and tending to death. So, the death rate of nodes is defined by:

$$\gamma_{ij}(t) = c\varepsilon_{ij}(t), \tag{1}$$

where c is a constant, $\varepsilon_{ij}(t)$ denotes the cumulative consumption of energy of *cell*(*i*,*j*) until the time *t*.

2.4 Media Access Control (MAC)

Malwares over wireless sensor networks will face channel collision, which should reduce the spreading rate of malwares. The MAC protocol specifies a set of rules that enable nearby sensor nodes to coordinate their transmissions in a distributed manner[1]. In our model to be given in the next section, a MAC table is designed to solve the problem of channel collision. If a sensor node is transmitting a packet, the states of its neighbors should be set block (denoted by '1') in MAC table, which means neighbors can not transmit packets at the same time. Each sensor node checks its state in the MAC table before starting a data transmission. The sensor nodes transmit packets when the channels are idle (denoted by '0' in MAC table). Therefore, the transmission is restrained if the channels are busy.

3 Modeling Malware Propagation with Cellular Automata

The proposed models focus on the stochastic properties of malware propagation and the intrinsic characteristic of wireless sensor networks. We utilize an 2-D cellular automata to describe the proposed model.

An 2-D cellular automata is a discrete dynamical system formed by a finite number of $l \times r$ identical objects called cells which are arranged uniformly in a two-dimensional cellular space. Each cell is endowed with a state (from a finite state set Q) that changes at every step of time accordingly to a local transition rule.

In this sense, the state of some cell at time t depends on the states of a set of cells, called its neighborhood, at the previous time step t-1. More precisely, a CA is defined by the 4-uplet (C,Q,V,f), where C denotes the cellular space,

$$C = \{(i, j), 1 \le i \le l, 1 \le j \le r\}, \tag{2}$$

and Q is the finite state set whose elements are all possible states of the cells. The neighborhood of each cell can be described by

$$V_{ij} = \{(i + \Delta i, j + \Delta j)\} \subset Z \times Z \tag{3}$$

where $\Delta i, \Delta j$ denote separately the offset of i, j. The local transition function f can be described by

$$s_{ij}^{t} = f(s_{ij}^{t-1}, \mathbf{s}_{V_{ij}}^{t-1}) \subset Q, \tag{4}$$

where s_{ij}^{t} denotes the state of *cell*(*i,j*) and $\mathbf{s}_{V_{ij}}^{t-1}$ denotes the vector of neighborhood of *cell*(*i,j*) at time *t.*

3.1 Cellular Space

We consider that a flat WSN (as shown in Fig.1) composed of the maximum *N* stationary and identical sensors which are randomly placed on rectangular 2-D grid composed of $L \times L$ *units* is exhibited appropriately by a 2-D cellular space. We assume that each cell is occupied by at most one sensor node. Thus, we can make simulations with fewer nodes than the maximum number of cells. Let ρ denote the relative density of sensor nodes, $\rho = N / L^2$. So, the infrastructure of the flat WSN constructs the cellular space and a sensor node denotes a cell in the space. Each sensor node can establish wireless links with only those nodes within a circle of radius R_c due to the limited power. To simplify analysis, we assume that all sensor nodes are equipped with isotropic antennas that have a maximum transmission range R_c. The horizontal and vertical coordinates of a sensor node are represented by *i* and *j* in the 2-D grid(cellular space). Namely, *node*(*i,j*) denotes a node located in the posotion with the coordinate of (*i,j*).

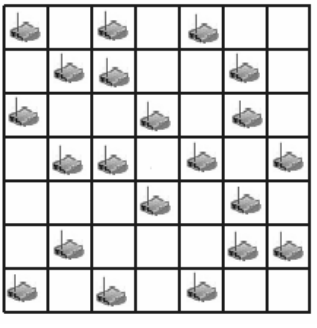


Fig. 1. Distribution of sensor nodes in a flat WSN with L^2 areas and *N* nodes

3.2 Neighborhood

According to the corresponding transmission range R_c, the neighborhood of each sensor is defined as shown in Fig. 2. Without loss of generality, let the length of a cell of grid be 1 *unit*, if R_c =1 *unit*, each node/cell can have no more than 4 nodes as its neighbors, namely the Von Neumann neighborhood, and if R_c =1.5 *units*, each node/cell can have no more than 8 nodes as neighbors, namely the Moore neighborhood. It is obvious that a node should have more neighbors with the value of R_c increasing, such that the neighborhood of *node*(*i,j*) is defined by

$$V_{ij} = \{(x, y) : \sqrt{(x-i)^2 + (y-j)^2} \le R_c, (x, y) \subset C\}. \tag{5}$$

Let $N(V_{ij})$ denote the number of neighborhood of *node*(*i,j*).

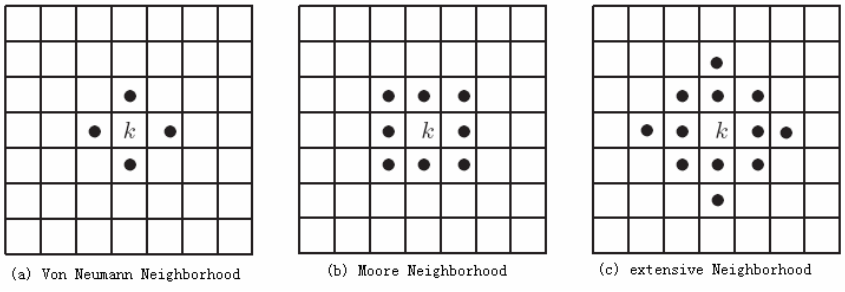


Fig. 2. Cell *k* and its possible neighborhoods in a 2-D cellular automata

3.3 State Set

At a particular time *t*, each cell of the cellular space is in a specific state, which depends on a specific application. Considering the MAC mechanism of WSN, we extend the definition of a state variable to that of a state vector. The vector includes two participants that denote epidemic state set Q_1 and channel state set Q_2 separately.

Borrowing the concept of epidemiology, the epidemic state of a sensor node or a cell can be one of following these states: susceptible, infected, recovery or death. Let $Q_1 = \{-1, 0, 1, 2\}$ and denote $s_{ij}(t) \in Q_1$ the epidemic state variable of *cell*(*i*,*j*) and $\mathbf{s}_{V_{ij}}(t) \in Q_1$ the state vector of neighborhood of *cell*(*i*,*j*) at time *t* , we define

$$s_{ij}(t) = \begin{cases} 0, & cell(i,j) \quad is \text{ susceptible } at\ time\ t \\ 1, & cell(i,j) \quad is \text{ infected } at\ time\ t \\ 2, & cell(i,j) \quad is \text{ recovered } at\ time\ t \\ -1, & cell(i,j) \quad is \text{ dead } at\ time\ t \end{cases}. \tag{6}$$

The channel state of a sensor node can be idle or busy. Let $Q_2 = \{0,1\}$ and denote $m_{ij}(t) \in Q_2$ the channel state variable of *cell*(*i*,*j*) and $m_{V_{ij}}(t) \in Q_2$ the state vector of neighborhood of *cell*(*i*,*j*) at time *t* , we define

$$m_{ij}(t) = \begin{cases} 0, & \text{the channel of } cell(i,j) \quad is \text{ idle } at\ time\ t \\ 1, & \text{the channel of } cell(i,j) \quad is \text{ busy } at\ time\ t \end{cases}. \tag{7}$$

3.4 Transition Function

The transition function can be constructed by

$$s_{ij}(t) = f(s_{ij}(t-1), \mathbf{s}_{V_{ij}}(t-1)). \tag{8}$$

The detailed rules of (8) are described below and the transition process of states is shown in Fig. 3.

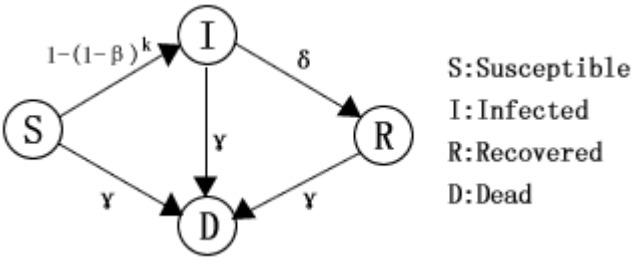


Fig. 3. Process of states transforming of sensor nodes

Susceptible to Infected/Dead. If $s_{ij}(t-1)=0$, then $s_{ij}(t)=1$ with probability $1-(1-\beta)^k$, or $s_{ij}(t)=-1$ with probability γ , where β and γ are defined below.

Infected nodes try to spread malware to their neighbors at each time step. A susceptible sensor's node becomes infected with the probability β when the node receives a packet containing a copy of the malware. However, during each time interval, the susceptible node can receive malware from its k neighbors($k \le N(V_{ij})$), so a susceptible node becomes infected node with the probability $1-(1-\beta)^k$. Note that k is the number of neighbors with infected state ($s_{xy}(t-1)=1,\ (x,y)\subset V_{ij}$) and idle state of channel ($m_{xy}(t-1)=0,\ (x,y)\subset V_{ij}$) at the time interval between t-1 and t, so,

$$k=\sum_{(x,y)\subset V_{ij}}(s_{xy}(t-1)=1 \text{ and } m_{xy}(t-1)=0). \tag{9}$$

Considering the limited power of sensors, some sensor nodes can become dead at the rate γ .

Infected to Recovered/Dead. If $s_{ij}(t-1)=1$, then $s_{ij}(t)=2$ with probability δ , or $s_{ij}(t)=-1$ with probability γ ;

In particular, infected sensors can get a patch and recover from the infected state with the probability δ .

Recovered to Dead. If $s_{ij}(t)=2$, then $s_{ij}(t)=-1$ with probability γ .

Let S(t), I(t), R(t) and D(t) denote the population of susceptible, infected, recovered and dead nodes, respectively, the we have

$$\begin{cases} S(t)=\sum_{i,j}(s_{ij}(t)=0), \\ I(t)=\sum_{i,j}(s_{ij}(t)=1), \\ R(t)=\sum_{i,j}(s_{ij}(t)=2), \\ D(t)=\sum_{i,j}(s_{ij}(t)=-1), \\ N=S(t)+I(t)+R(t)+D(t) \end{cases} . \tag{10}$$

4 Neighborhood Saturation

In [19], the phenomena of neighborhood saturation in native cellular automata has been pointed out, where the cell layers adopted Moore neighborhood model, shown in Fig. 4.

The neighborhood saturation is also the inherent characteristic of WSN. In the following, the phenomena of neighborhood saturation will be described in the process of malware propagation over WSN. Fig. 5 depicts the cell layers with respect to a central cell in layer1. Layer1 has L_1 neighboring cells in its outer-line layer2. The outer-line neighborhood of $layer_i$ is $layer_{i+1}$ and the inner-line neighborhood is $layer_{i-1}$. L_i is the number of cells in $layer_i$ and is defined in equation (11). It can be visualized as the area enclosed by layer L_{i-1} subtracted from the area enclosed by layer L_i.

$$L_i = \begin{cases} 1 & i = 1 \\ [\rho\pi(R_c i)^2 - \rho\pi R_c^{\,2}(i-1)^2] & i > 1 \end{cases}, \tag{11}$$

where [x] is the nearest integer to x. Furthermore, it is easy to deduce that

$$\frac{L_{i+1}}{L_i} = \frac{2i+1}{2i-1} \to 1, \quad \text{when } i \to \infty . \tag{12}$$

Equation (12) means that at higher layer, each cell at $layer_i$ is able to infect effectively only one outer-line cell at $layer_{i+1}$. This resulting neighborhood saturation slows effectively down the speed of malware propagation in WSN. The similar result that geographical localization effects on the propagation has also been observed in SARS transmission [22, 23].

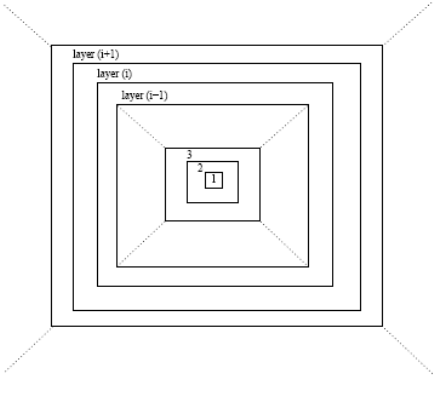


Fig. 4. Cell layers in [19]

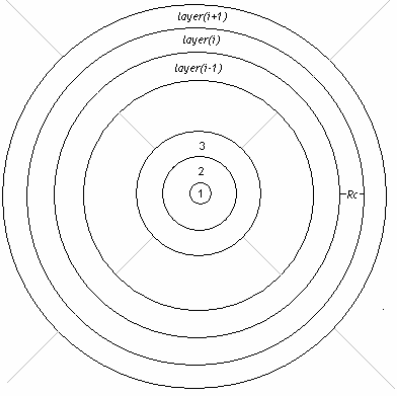


Fig. 5. Cell layers in WSN

5 Theoretical Analysis

Based on SI epidemic theory, a theoretical analysis is presented for analyzing the propagation of worms over wireless sensor networks. The theoretical analysis focuses on capturing the impact of the spatial deployment of sensor nodes to malware propagation. In particular, the sensor nodes have limited communication range R_c. For simplification, we assume that one node located in center of the grid is infected in initial time.

An important characteristic of spreading dynamic in WSN is that there is a circular region of infected nodes centered at the source node which grows outwards. That is the nodes in the infected circular region try to infect their susceptible neighboring nodes lying outside this circle, as shown in Fig. 6.

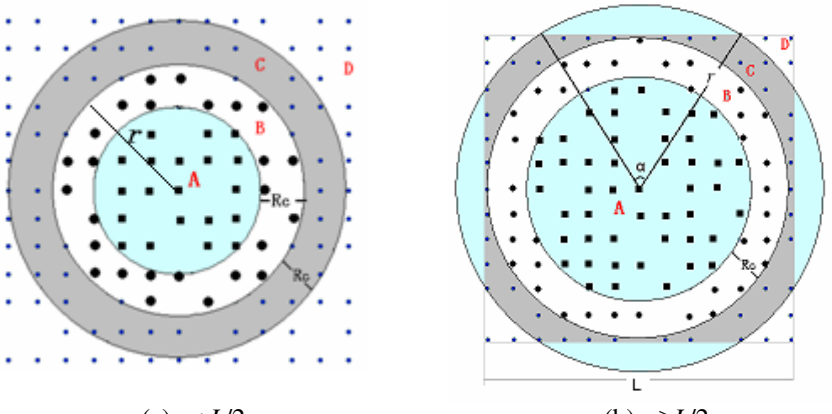
As shown in Fig. 6, the nodes in region A and B are infected nodes.The difference between region A and B is that the nodes in region A cannot infect any susceptible node because all the susceptible nodes are out of their communication area. The nodes in region B can infect the nodes in region C. The nodes in region D cannot be infected by the nodes in region B due to the limitation of communication distance. We define the width of region B or C to be R_c , the radius of the infected region to be r and the increment of r to be Δr in each time step of malware propagation. $\Delta r \le R_c$ due to the effect of MAC, density of sensor node, infected rate and security mechanism.

When r<L/2, the area of the potential region C increases with time evolution as shown in Fig. 6(a) and when r>=L/2, the area decreases as shown in Fig. 6(b).

Through above analysis, a function of the infected population is established for considering the two stages separately.

First Stage: *r<L/2*

Under the boundary condition $\rho = 1, \beta = 1$ and without MAC mechanism, we have $\Delta r = R_c$. Namely, in the above ideal case, the radius of the infected region



(a) $r< L/2$ (b) $r \ge L/2$

Fig. 6. Spreading characteristic in flat WSN: (a) first stage: $r< L/2$; (b) second stage: $r \ge L/2$

extends outside by the increment $\Delta r = R_c$ for each time. After t times, the area $I_{area}(t)$ of infected region should be

$$I_{area}(t) = \pi r^2 = \pi(\Delta r t)^2 = \pi(R_c t)^2 . \tag{13}$$

Note that t is a discrete time.

Considering the real situation, it is necessary that $\Delta r < R_c$, without generality, let $\Delta r = bR_c$, $0 \le b \le 1$. So, the number of infected nodes should be

$$I(t) = \rho\pi r^2 = \rho\pi(bR_c t)^2 . \tag{14}$$

When $bR_c t = L/2$, the first stage ends and $t_{\max} = L/2bR_c$.

Second stage: $r \ge L/2$

When $r \ge L/2$, the potential region C will decrease with the time evolution, as shown in Fig. 6 $r \ge L/2$ (b), the population of infected nodes can be expressed by

$$I(t) = \rho\pi r^2 - 4\rho S_{arc} = \rho\pi(bR_c t)^2 - 2\rho(bR_c t)^2(\alpha_t - \sin\alpha_t)) , \tag{15}$$

where S_{arc} denotes the area of a camber region and α_t the corner of the camber with the center

$$\sin\alpha_t = \frac{L\sqrt{(bR_c t)^2 - (L/2)^2}}{(bR_c t)^2} . \tag{16}$$

Apparently, b is an important factor affecting the spreading speed. We know that the spreading speed is in proportion to the infected rate and density of nodes. Furthermore, the MAC mechanism constrains the malware propagation. So, we have

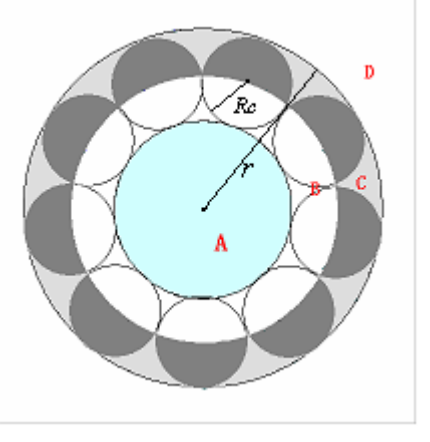


Fig. 7. Maximum coverage area shown in the shadow of region *C* due to avoiding channel collision for each time step

$b = f(\beta, \rho, p)$, where p is the coverage rate due to MAC mechanism, describing new infected region in the region C. First, the maximum coverage rate $\mathrm{cov}_{\max}$ is shown in Fig. 7, when $t \to \infty, R_c \ll r$. The infected nodes in region B can spread to the maximum region, i.e., the black area in region C. The closed result of $\mathrm{cov}_{\max}$ is $\mathrm{cov}_{\max} \approx \pi / 4$. It is obvious that $p < \mathrm{cov}_{\max}$.

6 Simulations

We simulate the malware propagation in a wireless sensor network consisting of N sensors distributing uniformly and randomly in a cellular space with $L^2 = 200 \times 200\ unit^2$ cells. $\rho = N / L^2$ denotes the sensor density. The communication range of each sensor is defined by R_c. Each simulation starts by infecting a sensor node located in the center of the WSN. Our goal is to investigate the spreading dynamics of malware in a wireless sensor network and to compare the result of simulations with theoretical analysis and those models in [11,12].

6.1 Simulations for the Proposed Model vs. the Theoretical Analysis

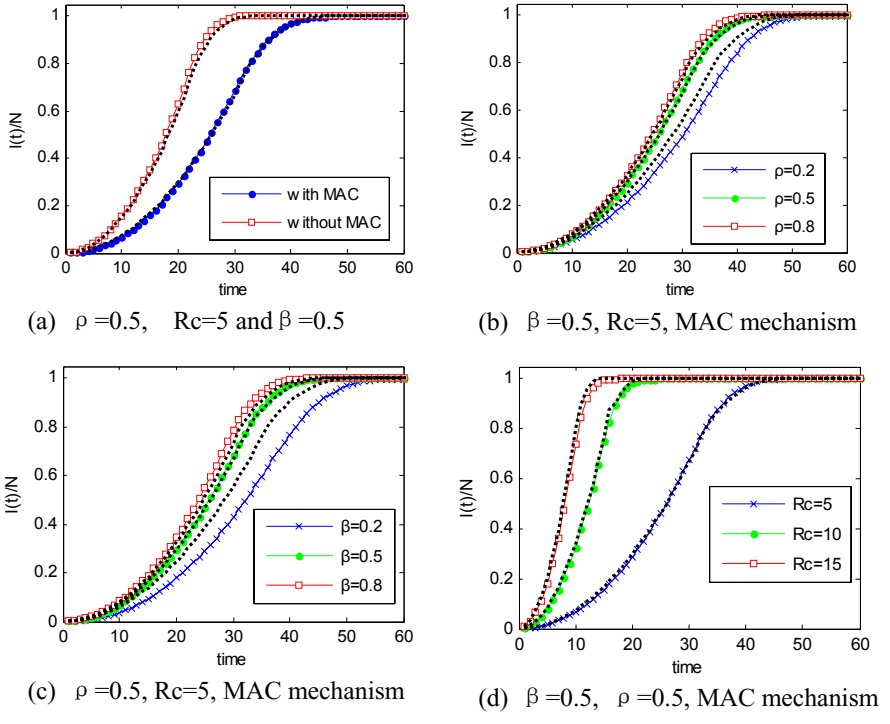
In the simulations, we set $\delta = 0, \gamma = 0$ for the comparison between the proposed model and the theoretical analysis. The other cases can be found in our another paper [24].

There is one initially infected node that locates in the center of the wireless sensor network. We pay more attention to 4 factors impacting on the malware propagation, which include MAC mechanism, node's relative density ρ, infected rate β and the communication range R_c. The time evolutions of the total fraction of infected nodes, $I(t)/N$, under the impact of the 4 factors are exhibited in Fig. 8.(a),(b),(c) and (d) respectively. Solid-line is for our proposed CA model, and Dashed-line denotes the theoretical analysis.

From Fig. 8, we can see that, the time evolution of the proposed CA model agrees perfectly with the theoretical analysis. The malwares show an exponentially increasing transmission from the initial time until reaching approximately 80% infected population, then show a slow transmission until the malwares spread to the whole network. Also we can find that, the MAC mechanism results in a competition between adjacent sensor nodes to access to the shared wireless channel, so MAC mechanism greatly slows down the speed of malware propagation and reduces the risk of large-scale malware prevalence in these networks.

6.2 Simulation for the Proposed Model vs. the Model in [12]

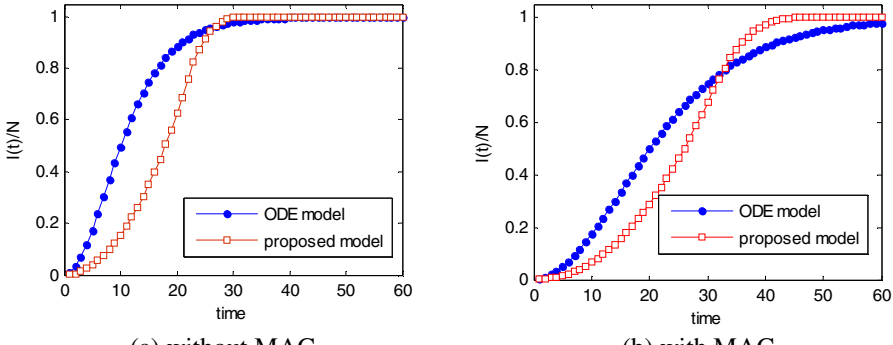
In [12], an ODE model and expression with respect to *I(t)* has been established. However, the model of the paper does NOT considered the impact of MAC mechanism. For comparison, we add a parameter p concerning MAC mechanism to revise the value of η in the Equation of [12], and let p=1 when the network has no



(a) ρ =0.5, Rc=5 and β =0.5 (b) β =0.5, Rc=5, MAC mechanism

(c) ρ =0.5, Rc=5, MAC mechanism (d) β =0.5, ρ =0.5, MAC mechanism

Fig. 8. Time evolution of the fraction of infected nodes on the proposed model(*solid-line*) vs. the theoretical analysis(*dashed-line*): (a) effect of MAC mechanism, (b) effect of relative densityρ, (c) effect of infected rateβand (d) effect of communication range R_c



(a) without MAC (b) with MAC

Fig. 9. Time evolution of the fraction of infected nodes on the proposed model vs. the model in Ref.[12] (a) ρ=0.5,β=0.5, Rc=5, the absence of MAC mechanism (b) ρ=0.5,β=0.5, Rc=5, the presence of MAC mechanism

the MAC mechanism and p=0.5 when the MAC mechanism takes action. The revised equation can be described by

$$I(t) = N\left(2/(1+(\frac{\sqrt{N}-1}{\sqrt{N}+1})e^{-\frac{\beta c\eta p}{\sqrt{N}}t})-1\right)^2, \tag{17}$$

where η is the average number of neighbors of a node, $\eta = \rho\pi R_c^2$, and $c = 2\sqrt{\rho\pi}R_c$ is a proportional constant. More details can be seen in [12].

By normalizing the time in simulation of Eq.(17), the time evolutions of malware propagation for the two models is shown in Fig. 9.

From Fig. 9, we find the initial speed of propagation is quicker in ODE model than that in our proposed model, but slower in the last stage of propagation. A reasonable explanation is that, ODE model assumes that the number of infected neighbors is in proportion to the fraction of all susceptible nodes in the network, which results in an inaccurate evaluation on spreading speed in the process of malware propagation. In fact, the malware propagation in WSN has the chacteristic of local spatial interaction. And the presence of neighborhood saturation dominates the effects of increasing infectivity and limits the spread of the malware.

6.3 Simulation for Evolution Pattern

Fig. 10 and Fig. 11 show the wireless sensor network evolving patterns in the 2-D cellular space under different time *t*. The key difference between Fig. 10 and Fig. 11 is that the former neglects the impact of MAC mechanism, whereas the latter is more concerned to the impact of MAC mechanism.

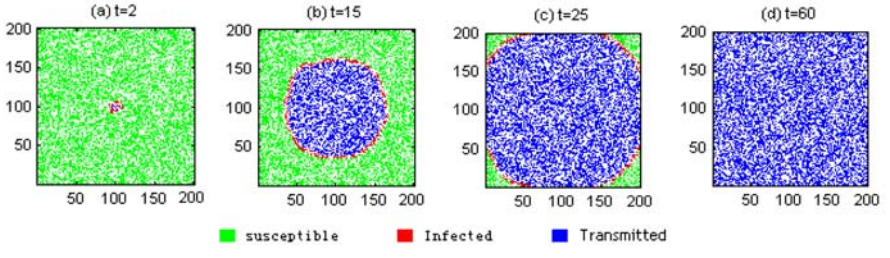


Fig. 10. Evolution pattern without MAC mechanism in the 2-D space withρ=0.5,β=0.5,Rc=5

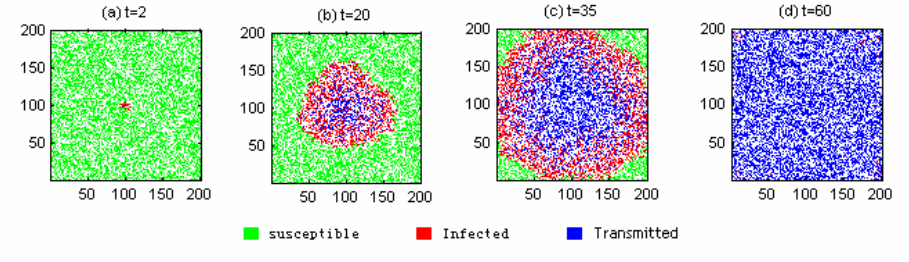


Fig. 11. Evolution pattern with MAC mechanism in the 2-D space withρ=0.5,β=0.5,R_c=5

From the evolution snapshots (Fig. 10 (a)-(d) and Fig. 11(a)-(d)), one can see that the epidemic diffuses continuously from infected source toward outside and the propagation goes along a circular front which is spatially bounded. Specially, in our model, the adopted broadcast protocol ensures that each infected node broadcasts the malware to its neighbors only once for the purpose of preventing broadcast storm. So, those infected nodes that have transmitted packets of malware can not send malware propagation any more. In fact, an infected node inside of the circular has also no chance to infect other susceptible nodes that lie outside of the circular for the reason that interactions among nodes are distance-dependent.

Considering MAC mechanism, Fig. 11 has two key differences with the Fig. 10. First, the diffused speed of malware propagation in Fig. 11 is slower than that in Fig. 10 because the MAC mechanism chokes the malware propagation.

Second, the border between the nodes that have transmitted packet and the nodes that haven't transmitted packets becomes unclear. Due to the constraint of MAC mechanism, only partial nodes win channels to transmit packets in each time step and other nodes must wait for channels to transmit packets, which leads to the wide region occupied by those infected nodes that haven't transmitted packets. In addition, most nodes in the region can never send malware for the limitation of communication range.

The characteristic of propagation with the local spatial interaction between nodes is greatly different from the propagation over Internet and results in slowing the speed of propagation.

7 Conclusions and Future Work

A model based on cellular automata has been proposed to investigate and analyze the dynamic behaviors of malware propagation over wireless sensor networks. The model successfully captures the inherent characteristics of wireless sensor networks, such as limited energy, channel contention and multi-hop broadcast protocols, and reflects the self-organization, neighborhood saturation and spatio-temporal correlation of process of malware propagation. The validations of the model have been performed through theoretical analysis and various simulations. In addition, a comparative analysis between the proposed model and the model in [12] has been done, which further demonstrates the local spatial interaction of malware propagation in WSN, and the presence of neighborhood saturation slows down the spread of the malware. The MAC mechanism of wireless sensor networks greatly slows down the speed of malware propagation and reduces the risk of large-scale malware prevalence in the networks. The proposed model can describe accurately the dynamic behavior of malware propagation on WSN, which can be used for developing robust and efficient defense system on WSN.

In our near future work, we will be further evaluating the influence of the consumption of energy on system behaviors during the process of malware propagation, and developing robust and efficient strategies against the malware propagation to improve the network security.

Acknowledgements

This work was supported in part by the Program for New Century Excellent Talents in University of China under the Contract NCET-06-0510, by the National Natural Science Foundation of China under the Contract 60874091 and by Scientific Innovation Program for University Research Students in Jiangsu Province, China, under the Contract CX08B_081Z.

References

1. Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., Cayirci, E.: Wireless sensor networks: a survey. Computer Networks 38, 393–422 (2002)
2. Pathan, A.S.K., Lee, H.W., Hong, C.S.: Security in Wireless Sensor Networks: Issues and Challenges. Proc. of the 8th IEEE ICACT 2, 1043–1048 (2006)
3. Perrig, A., Stankovic, J., Wagner, D.: Security in wireless sensor networks. Communications of the ACM 47, 53–57 (2004)
4. Staniford, S., Paxson, V., Weaver, N.: How to Own the Internet in Your Spare Time. Usenix Security (2002)
5. Zou, C.C., Towsley, D., Gong, W.B.: Modeling and simulation study of the propagation and defense of internet e-mail worms. IEEE Transactions on Dependable and Secure Computing 4, 105–118 (2007)
6. Zou, C.C., Gong, W., Towsley, D.: Code red worm propagation modeling and analysis. In: Proceedings of the 9th ACM Conference on Computer and Communications Security, p. 10 (2002)
7. Pastor-Satorras, R., Vespignani, A.: Epidemic spreading in scale-free networks. Physical Review Letters 86, 3200–3203 (2001)
8. Newman, M.E.J., Forrest, S., Balthrop, J.: Email networks and the spread of computer viruses. Physical Review E 66, 35101 (2002)
9. Mills, K.L.: A Brief Survey of Self-Organization in Wireless Sensor Networks. Wireless Communications and Mobile Computing 7, 823–834 (2007)
10. Khayam, S.A., Radha, H.: Using signal processing techniques to model worm propagation over wireless sensor networks. Signal Processing Magazine 23, 164–169 (2006)
11. De, P., Liu, Y., Das, S.K.: Modeling Node Compromise Spread in Wireless Sensor Networks Using Epidemic Theory. In: Proceedings of the 2006 International Symposium on on World of Wireless, Mobile and Multimedia Networks, pp. 237–243 (2006)
12. De, P., Liu, Y., Das, S.K.: An Epidemic Theoretic Framework for Evaluating Broadcast Protocols in Wireless Sensor Networks. In: IEEE Internatonal Conference on Mobile Adhoc and Sensor Systems, MASS, Pisa, Italy, pp. 1–9 (2007)
13. White, S.H., Rey, A.M.d., Sanchez, G.R.: Modeling epidemics using cellular automata. Applied Mathematics and Computation 186, 193–202 (2007)
14. Georgoudas, I.G., Sirakoulis, G.C., Andreadis, I.: Modelling earthquake activity features using cellular automata. Mathematical and Computer Modelling 46, 124–137 (2007)
15. Encinas, L.H., Hoya White, S., Del Rey, A.M., Rodriguez Sanchez, G.: Modelling forest fire spread using hexagonal cellular automata. Applied mathematical modelling 31, 1213–1227 (2007)
16. Ahmed, E., Elgazzar, A.S.: Onsome applications of cellular automata. Physica A 296, 529–538 (2001)

17. Liu, Q.-X., Jin, Z.: Cellular automata modelling of SEIRS. Chinese Physics 14, 1370–1377 (2005)
18. Fuentes, M.A., Kuperman, M.N.: Cellular automata and epidemiological models with spatial dependence. Physica A 267, 471–486 (1999)
19. Mikler, A.R., Venkatachalam, S., Abbas, K.: Modeling Infectious Diseases using Global Stochastic Cellular Automata. Journal of Biological Systems 13, 421–439 (2005)
20. Cunha, R.O., Silva, A.P., Loreiro, A.A.F., Ruiz, L.B.: Simulating large wireless sensor networks using cellular automata. In: Proceedings of the 38th annual Symposium on Simulation, pp. 323–330 (2005)
21. Akkaya, K., Younis, M.: A survey on routing protocols for wireless sensor networks. Ad Hoc Networks 3, 325–349 (2005)
22. Small, M., Tse, C.K.: Clustering model for transmission of the SARS virus: application to epidemic control and risk assessment. Physica A: Statistical Mechanics and its Applications 351, 499–511 (2005)
23. Small, M., Tse, C.K., Walker, D.M.: Super-spreaders and the rate of transmission of the SARS virus. Physica D: Nonlinear Phenomena 215, 146–158 (2006)
24. Song, Y., Jiang, G.-P.: Modeling malware propagation in wireless sensor networks using cellular automata. In: IEEE ICNNSP 2008, Zhenjiang, China, pp. 623–627 (2008)