Chinese Journal of Electronics
Vol.23, No.4, Oct. 2014

A Pulse Immunization Model for Inhibiting Malware Propagation in Mobile Wireless Sensor Networks*

WANG Xiaoming[1], HE Zaobo[1,2] and ZHANG Lichen[1]

(1. *School of Computer Science, Shaanxi Normal University, Xi'an 710062, China*)

(2. *Department of Computer Science, Georgia State University, Atlanta 30303, USA*)

Abstract — Mobile wireless sensor networks (MWSNs) may be under attack due to their large-scale characteristics. One of the main threats is to inject malware into some nodes. To prevent malware from spreading in a large-scale MWSN, an effective measure is to immunize susceptible nodes by disseminating and installing security patches. This work suggests a novel modeling framework and some mathematical models based on the pulse differential equation and the epidemic theory, in which the immunization operations are implemented on susceptible nodes in a pulse way. The maximum immunization period of time is derived to minimine the number of immunization operations while ensuring malware extinct over time in the MWSN. The theoretical results are confirmed by extensive simulations.

Key words — MWSN, Malware propagation, Susceptible-infected-recovered (SIR), Pulse differential equation, Maximum immunization period of time.

I. Introduction

A Mobile wireless sensor network (MWSN) usually consists of many mobile sensor nodes or mobile sink nodes. The nodes communicate with each other through opportunistic contacts caused by the mobility of nodes. MWSNs have been applied in many fields, such as military defense, disaster recovery, vehicular traffic monitoring and industrial automation. Compared with static wireless sensor networks, the advantages of MWSNs involve better energy efficiency, improved coverage, enhanced target tracking and arrangement flexibility due to the mobility of nodes. Thus, MWSNs have gained a lot of attention[1−4].

However, MWSNs are prone to be attacked by self-replicating codes, called the malware propagation. A wireless malware is a piece of malicious software intentionally designed for physically destroying nodes, depleting energy of nodes, blocking regular communications between nodes, or damaging the integrity of regular data packets[5−9]. Thus, it is important to design an effective and efficient mechanism for restraining malware propagation in MWSNs. Currently, one of the popular methods is network immunization, which means that some security patches are disseminated and installed on some susceptible nodes, so that those nodes will not be infected by malware in the future. A key problem is when the immunization operations should be implemented to ensure a piece of malware against becoming a rapid epidemic in the MWSN.

In recent years, many continuous immunization strategies have been proposed to prevent malware from spreading in wired networks and wireless sensor networks [5−10], in which susceptible nodes are continuously immunized every time. Although continuous immunization strategies may effectively eliminate malware from networks, they will consume a large account of network resources, such as communication bandwidth and energy of nodes. In addition, continuous immunization strategies delay regular data transmission, and generate a lot of data transmission collisions. In particular, most of these strategies are designed for static networks without considering the effect of the mobility of nodes on malware propagation, which makes continuous immunization strategies unrealistic to MWSNs. So far, it remains a challenge to design effective and efficient immunization strategies for MWSNs.

Motivated by the Ref.[11], we develop a modeling framework to describe the effect of the mobility of nodes on malware propagation in MWSNs, and then we construct a pulse immunization model for preventing malware from spreading in MWSNs based on the pulse differential equation and the SIR model in the epidemic theory. Finally, we mathematically analyze the existence and stability of a malware-free solution of the proposed model, and derive the maximal immunization period of time, every which the immunization operations are

*Manuscript Received June 2013; Accepted Apr. 2014. This work is supported by the National Natural Science Foundation of China (No.61173094, No.61373083) and the Fundamental Research Funds for the Central Universities of China (No.GK201401002, No.GK201302024).

implemented on susceptible nodes to minimine the number of immunization operations while ensuring malware extinct over time in the MWSN. The simulation results validate the effectiveness and efficiency of our proposed model.

II. Preliminaries

1. Network model

We consider a MWSN with the area of A and N nodes. Each node may roam with a speed v, which results in a final uniform distribution of nodes in the MWSN. The density of nodes is denoted by μ, and defined by $\mu = N/A$. Each node has a limited battery capacity and a wireless transmission range, which is a circle with the radius of r. Without loss of generality, we assume the probability with which each node disappears from the MWSN is b due to its physical component damage or energy depletion. New susceptible nodes are continuously added into the MWSN with the rate of b to keep the total number of all living nodes is a constant at any time.

2. Malware propagation

To model the process of malware propagation, we divide the nodes into four categories: susceptible node, infected node, recovered node and dead node. Each category is also called a state of nodes. At any instant, each node can only be in one of the four states. A node is infected if it is contaminated by malware. An infected node propagates multiple copies of malware to its susceptible neighbors while transmitting data or control messages to them. A node is susceptible if it has no malware and it is prone to be infected by malware in the future. A node is recovered if it is immune to malware in the future, *i.e.*, a recovered node can not be infected by malware. A node is dead if it can not work due to its physical component damage or energy exhaustion. When a susceptible node successfully receives a security patch from one of its neighbors and installs on itself, the susceptible node becomes a recovered node. When an infected node successfully receives a security patch from one of its neighbors and installs on itself, the malware on the infected node is removed, and the infected node becomes a recovered node. In addition, a security patch has no effect on a recovered node. Of course, any dead node is removed from the MWSN due to the loss of its working capability.

For simplicity, we represent the fractions of susceptible nodes, infected nodes, recovered nodes and dead nodes by $S(t)$, $I(t)$, $R(t)$ and $D(t)$ at any instant t, and the states of susceptible nodes, infected nodes, recovered nodes and dead nodes by S, I, R and D, respectively. The transition relationship between two nodal states F and H is denoted by $F \xrightarrow{\zeta} H$, where $F, H \in \{S, I, R\}$, the weight ς means ς nodes in state F enter state H per unit of time. The state transition relationships of nodes are shown in Fig.1.

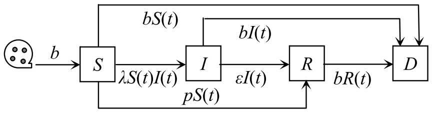


Fig. 1. State transition relationships of nodes

In Fig.1, p is the probability with which a susceptible node becomes a recovered node, ε is the probability with which an infected node becomes a recovered node, b is the dead rate and supplementary rate of nodes, λ is a contact rate between nodes per unit of time. Obviously, we have $0 \le p \le 1$, $0 \le \varepsilon \le 1$, and $0 \le b \le 1$. Because the total number of all living nodes is a constant at any time, we can have

$$S(t) + I(t) + R(t) = 1 \tag{1}$$

The movement process of each node n_j is divided into limited continuous stages, denoted by $t_1, t_2, \ldots, t_K$, where K is a positive integer. We suppose $t_{i+1} - t_i = t_{i+2} - t_{i+1} = t$, where $1 \le i \le K - 2$. In any stage t_i, node n_j moves or stops in an interleaving way. We assume that the time during which node n_j moves is T_1 and that the time during which node n_j stops is T_2, where $T_1 + T_2 = t$. Thus, a larger T_1 implies a smaller T_2, and vice versa. The average speed of node n_j is v, and the movement direction of node n_j is randomly selected from $[0, 2\pi)$. Obviously, the distance that each node can travel at stage t is vT_1, and the area of the communication region of node n_j is $\Phi = 2rvT_1 + \pi r^2$. Thus, the total number of the neighbors of node n_j is $\zeta = \mu\Phi = (2rvT_1 + \pi r^2)N/A$ at each stage. In addition, we suppose that the scanning rate with which a node explores its neighbors is β, and the probability with which an infected node successfully infects its neighbors is α. The capability that an infected node can successfully infect its neighbors is defined by $\eta = \alpha\beta$. Then, the number of the susceptible nodes which an infected node can successfully infect at stage t, is $\delta = \eta\zeta S(t) = \alpha\beta(2rvT_1 + \pi r^2)NS(t)/A$. We let $\lambda = \alpha\beta(2rvT_1 + \pi r^2)N/A$. Obviously, λ is related to some attributes of mobile nodes.

III. Pulse Immunization Model of Malware Propagation

In the following, considering that the dead nodes have no impact on malware propagation, we suggest a formal model of malware propagation based on the pulse differential equation and the state transition relationships of nodes in Fig.1.

$$\left\{ \begin{array}{ll} \left. \begin{array}{l} \dfrac{dS(t)}{dt} = b - \lambda S(t)I(t) - bS(t) \qquad (2a) \\ \dfrac{dI(t)}{dt} = \lambda S(t)I(t) - \varepsilon I(t) - bI(t) \qquad (2b) \\ \dfrac{dR(t)}{dt} = \varepsilon I(t) - bR(t) \qquad (2c) \end{array} \right\}, & t \neq nT \\ \left. \begin{array}{l} S(nT^+) = (1-p)S(nT) \qquad (2d) \\ I(nT^+) = I(nT) \qquad (2e) \\ R(nT^+) = R(nT) + pS(nT) \qquad (2f) \end{array} \right\}, & t = nT \end{array} \right. \tag{2}$$

where n is a positive integer, $[nT, (n+1)T]$ is time intervals between every two times of immunization operation, and the immunization operations are implemented at times nT and $(n+1)T$, respectively. Obviously, Eq.(2) is a pulse differential system.

In Eq.(2), at any time $t \neq nT$, Eq.($2a$) describes the change rate of the number of susceptible nodes, where b susceptible nodes are added into the MWSN to keep the number of living nodes relatively stable per unit of time, leading to an increase of the number of susceptible nodes; $\lambda S(t)I(t)$ susceptible nodes become infected nodes due to wireless communications between susceptible and infected nodes; $bS(t)$ susceptible nodes become dead nodes due to their physical component damage or energy exhaustion per unit of time, resulting in a decrease of the number of susceptible nodes; Eq.(2b) describes the change rate of the number of infected nodes, where $\lambda S(t)I(t)$ susceptible nodes become infected nodes per unit of time, leading to an increase of the number of infected nodes, εI infected nodes become recovered nodes by taking recovery measures continuously, and $bI(t)$ infected nodes become dead nodes per unit of time, resulting in a decrease of the number of infected nodes; here, λ is used to describe the effect of the mobility of nodes on malware propagation in the MWSN; Eq.(2c) describes the change rate of the number of recovered nodes, where $\varepsilon I(t)$ infected nodes become recovered nodes by installing security patches, leading to an increase of the number of recovered nodes, and $bR(t)$ recovered nodes become dead nodes, leading to a decrease of the number of recovered nodes per unit of time. We use nT^+ to represent the next instant of nT. At any time $t = nT$, Eq.(2d) describes the pulse immunization mechanism; the fraction of susceptible nodes becomes $(1-p)S(nT)$ at the instant nT^+ after an immunization operation is just implemented at the instant nT, leading to a decrease of the number of susceptible nodes; Eq.(2e) describes the fact that a pulse immunization operation does not play any role to all the infected nodes; Eq.(2f) describes the fact that the fraction of recovered nodes increases because a pulse immunization operation has been finished at time nT. At the initial instant $t = 0$, we have $I(0) > 0$, $S(0) > 0$ and $R(0) = 1 - I(0) - S(0)$. Thus we say that Eq.(2) can effectively describe the interactions between a pulse immunization operation and malware propagation in the MWSN.

IV. Model Analysis

1. Existence of a malware-free *T*-period solution

If there exists a malware-free T-period solution of Eq.(2), the malware may die out in the MWSN over time. Otherwise, the malware may persistantly propagate. From Eq.(2), we observe that the first and second equations are independent of the third one. Thus, we can first analyze the first and second equations, and then drive $R(t)$ from Eq.(1) naturally. The result of extracting Eqs.(2a) and (2b) from Eq.(2) can be shown as follows:

$$\begin{cases} \left.\begin{aligned} \frac{dS(t)}{dt} &= b - \lambda S(t)I(t) - bS(t) \\ \frac{dI(t)}{dt} &= \lambda S(t)I(t) - \varepsilon I(t) - bI(t) \end{aligned}\right\}, & t \neq nT \\ \left.\begin{aligned} S(nT^+) &= (1-p)S(nT) \\ I(nT^+) &= I(nT) \end{aligned}\right\}, & t = nT \end{cases} \tag{3}$$

When the malware dies out in the MWSN, there must exist a time t', such that $I(t) = 0$ when $t > t'$; moreover, there exists a positive integer n', such that $I(nT) = 0$ when $n > n'$. At this time, from Eq.(3) we have

$$\begin{cases} \dfrac{dS(t)}{dt} = b - bS(t), & t \neq nT \\ S(nT^+) = (1-p)S(nT), & t = nT \end{cases} \tag{4}$$

In the time interval $[nT, (n+1)T]$, the solution of Eq.(4) is $S(t) = 1 + (S(nT^+) - 1)e^{-b(t-nT)}$. From Eq.(4), we can derive

$$S((n+1)T^+) = (1-p)S((n+1)T) \tag{5}$$

We represent $S(nT^+)$ by S_n. Combining the solution of Eq.(4), from Eq.(5) we can derive

$$S_{n+1} = (1-p)(1 + (S_n - 1)e^{-bT}) \tag{6}$$

From Eq.(6), it is easy to deduce a map f, such that $S_{n+1} = f(S_n)$. When Eq.(6) reaches its equilibrium states, we have $S_{n+1} = S_n$. Thus, we can derive the only equilibrium state of Eq.(6) as follows

$$S^* = \frac{(1-p)(e^{bT} - 1)}{e^{bT} + p - 1} \tag{7}$$

With the equilibrium state S^* as the initial value of Eq.(6), we have

$$\left|\frac{df(S_n)}{dS}\right|_{S=S^*} = (1-p)e^{-bT} \tag{8}$$

Obviously, from Eq.(8) we have $\left|\dfrac{df(S_n)}{dS}\right|_{S=S^*} < 1$. Thus, the equilibrium state S^* of Eq.(6) is locally stable according to the stability criterion of differential systems[12]. Moreover, the local stability implies the global stability of S^*. This means that the pulse immunization operations generate the sequence S_n which converges to the equilibrium state S^*. As such, we can derive a T-period solution of Eq.(4) as follows

$$S^T(t) = (1 + (S^* - 1)e^{-b(t-nT)}) \tag{9}$$

where $t \in [nT, (n+1)T]$. Thus, $(S^T(t), 0)$ is the malware-free T-period solution of Eq.(3).

2. Stability of a malware-free *T*-period solution

To discuss the stability of a malware-free T-period solution of Eq.(3), we make the following transformation

$$\begin{cases} S(t) = S^T(t) + s(t) \\ I(t) = i(t) \end{cases} \tag{10}$$

where $s(t)$ and $i(t)$ are small perturbations on the malware-free T-period solution $(S^T(t), 0)$ of Eq.(3). Substituting Eq.(10) into Eq.(3) and expanding by the Taylor Series while neglecting high order terms, we can obtain a linear pulse differential system of Eq.(3) as follows.

$$\begin{cases} \left.\begin{aligned} \frac{ds(t)}{dt} &= -bs(t) - \lambda s(t)i(t) \\ \frac{di(t)}{dt} &= (\lambda(s(t) + \lambda s^T(t) - \varepsilon - b)i(t) \end{aligned}\right\}, & t \neq nT \\ \left.\begin{aligned} s(nT^+) &= (1-p)s(nT) \\ i(nT^+) &= i(nT) \end{aligned}\right\}, & t = nT \end{cases} \tag{11}$$

As such, the stability problem of the malware-free T-period solution of Eq.(3) is transformed into the stability problem of the zero solution of Eq.(11). Since Eq.(11) is a T-period linear system, we just need to discuss the Floquet multipliers of the basic solution matrix of Eq.(11) in the time interval $[0, T]$ according to the Floquet theorem[12]. Suppose $C(t)$ is a basic solution matrix of Eq.(11). Then we say $C(t+T)$ is also a basic solution matrix of Eq.(11), and we have

$$C(t+T) = C(t)M \tag{12}$$

where M is a value-single matrix corresponding to $C(t)$. The characteristic values of M, denoted by ω_1 and ω_2, are called the Floquet multipliers of Eq.(11). We construct the following system

$$\begin{cases} \dfrac{dA(t)}{dt} = \alpha A(t), \quad t \neq nT \\ A(nT^+) = \eta A(nT), \quad t = nT \end{cases} \tag{13}$$

where $A(t+nT) = A(t)$, and α and μ are constants. Suppose ω_j $(j = 1, 2, \ldots)$ are all the Floquet multipliers of Eq.(13). According to the pulse differential equation theory[9], for each ω_j, if $|\omega_j \mid \leq 1$, the solutions of Eq.(13) are stable. Otherwise, these solutions are unstable. We let $\boldsymbol{A}(t)$ be a basic solution matrix of Eq.(11) when $t \neq nT$. Then we have

$$\frac{d\boldsymbol{A}(t)}{dt} = \begin{pmatrix} -b & -\lambda S^T(t) \\ 0 & (\lambda S^T(t) - \varepsilon - b) \end{pmatrix} \boldsymbol{A}(t) \tag{14}$$

where $\boldsymbol{A}(0)$ is an unit matrix when $t = 0$. From Eq.(14), we obtain

$$\boldsymbol{A}(T) = \begin{bmatrix} s_1(T) & s_2(T) \\ i_1(T) & i_2(T) \end{bmatrix} \tag{15}$$

where $s_1(T) = e^{-bT}$, $i_1(T) = 0$, and $i_2(T) = e^{\int_0^T (\lambda S^T(t) - \varepsilon - b)dt}$. Note that there is no need to calculate the exact form of $s_2(T)$ as it is not required in the following analysis. When $t = nT$, from Eq.(13) we have

$$\begin{pmatrix} s(nT^+) \\ i(nT^+) \end{pmatrix} = \begin{pmatrix} 1-p & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} s(nT) \\ i(nT) \end{pmatrix} \tag{16}$$

Therefore, we can derive a value-single matrix $\boldsymbol{M}$ for Eq.(13) as follows.

$$\begin{aligned} \boldsymbol{M} &= \begin{pmatrix} 1-p & 0 \\ 0 & 1 \end{pmatrix} \boldsymbol{A}(T) \\ &= \begin{pmatrix} (1-p)e^{-bT} & (1-p)s_2(T) \\ 0 & i_2(T) \end{pmatrix} \end{aligned} \tag{17}$$

We can derive the Floquet multipliers of Eq.(11) as follows

$$\begin{cases} \omega_1 = (1-p)e^{-bt} \\ \omega_2 = e^{\int_0^T (\lambda S^T(t) - \varepsilon - b)dt} \end{cases} \tag{18}$$

From the Floquet theorem, we know that the equilibrium state of Eq.(3) is locally stable if $|\omega_i| < 1$, where $i = 1, 2$. Obviously, we have $0 < \omega_1 < 1$. Thus the stability of the malware-free T-period solution of Eq.(3) depends on ω_2. We let

$$\int_0^T (\lambda S^T(t) - \varepsilon - b)dt \leq 0 \tag{19}$$

From Eq.(19), we have the following equation

$$\frac{1}{T}\int_0^T S^T(t)dt \leq (\varepsilon + b)/\lambda \tag{20}$$

Suppose κ is a sufficiently small real variable and $\kappa > 0$. We add κ on $S^T(t)$, then Eq.(20) still holds. Thus, we have

$$\frac{1}{T}\int_0^T (S^T(t) + \kappa)dt \leq (\varepsilon + b)/\lambda \tag{21}$$

Considering all the solutions of Eq.(3) are non-negtive, from Eq.(3) we have

$$\begin{cases} \dfrac{dS(t)}{dt} \leq b - bS(t), \quad t \neq nT \\ S(nT^+) = (1-p)S(nT), \quad t = nT \end{cases} \tag{22}$$

According to the comparison theorem of the differential equation, for any sufficiently large time t, we have

$$S(t) \leq S^T(t) + \kappa \tag{23}$$

Combining Eq.(23) with the second equation of Eq.(3), we have

$$\frac{dI(t)}{dt} \leq I(t)[\lambda(S^T(t) + \kappa) - \varepsilon - b] \tag{24}$$

By integrating Eq.(24) in the time interval $[0, T]$, we have

$$\begin{aligned} I(t) &\leq I_0 \exp\left[\int_0^T (\beta(S^T(t) + \kappa) - \varepsilon - b)ds\right] \\ &= I_0\left[\left(\int_0^T + \cdots + \int_{\kappa T}^{(\kappa+1)T} + \int_{(\kappa+1)T}^t\right)\right. \\ &\quad \left. \cdot\, (\beta(S^T(t)) - \varepsilon - b)ds\right] \end{aligned} \tag{25}$$

For Eq.(25), we have that κ converges to zero when t converges to zero. Combining Eqs.(24) and (25), we have

$$\lim_{t \to \infty} I(t) = 0 \tag{26}$$

This means the malware-free T-period solution of Eq.(3) is globally stable.

3. The maximum immunization period of time

Substituting Eq.(10) into Eq.(24), we have

$$1 + \frac{p^2}{Tb(p - 1 + e^{Tb})} - \frac{p}{Tb} < (\varepsilon + b)/\lambda \tag{27}$$

We let $S_c = (\varepsilon + b)/\lambda$. From Eq.(27), we can get the maximum immunization period of time, denoted by $T_{\max 1}$, in which the stability of the malware-free T-period solution is ensured. Because there is no analytical solution for Eq.(27) when the equality holds, we will give the numerical solution of $T_{\max 1}$ in simulations. Note that $T < T_{\max 1}$ means the frequency of immunization operations is high, leading to the malware-free T-period solution is stable, whereas $T > T_{\max 1}$ means the malware-free T-period solution will be unstable.

Another method to ensure the fraction of infected nodes monotonically decreases to zero is to keep $dI/dt < 0$ at any time. At this time, for Eq.(2) we have

$$S(t) < (\varepsilon + b)/\lambda = S_c \tag{28}$$

Eq.(28) implies that the immunization operation should be implemented once the fraction of susceptible nodes is closed to the threshold S_c. If the immunization period of time T is less than a critical value $T_{\max 2}$, we say that $S(t)$ must be below S_c.

From the T-period solution $S^T(t)$ of Eq.(10), we have $dS^T(t)/dt \geq 0$. Thus, in any pulse immunization period of time, the fraction of susceptible nodes reaches the minimum value once the pulse immunization operation is implemented on susceptible nodes, whereas gradually reaches the maximum value of $S^*/(1-p)$ before the pulse immunization operation is implemented on susceptible nodes. Hence, the following condition must hold to ensure $S(t) < S_c$.

$$\frac{S^*}{1-p} < (\varepsilon + b)/\lambda \tag{29}$$

Substituting Eq.(9) into Eq.(29), we can derive $T_{\max 2}$ as follows

$$T_{\max 2} = \frac{1}{b} \ln \left(1 + \frac{pS_c}{1-S_c}\right) \tag{30}$$

where $\ln(x)$ is a logarithmic function.

V. Simulation Results

For comparison, we give a continuous immunization model of malware propagation, which is based on the ordinary differential equation.

$$\begin{cases} \dfrac{dS(t)}{dt} = b - \lambda S(t)I(t) - bS(t) - qS(t) \\ \dfrac{dI(t)}{dt} = \lambda S(t)I(t) - \varepsilon I(t) - bI(t) \\ \dfrac{dR(t)}{dt} = \varepsilon I(t) - bR(t) + qS(t) \end{cases} \tag{31}$$

where q is a continuous immunization rate of susceptible nodes, and ε, b and λ are the same ones as of Eq.(2).

The main parameters used in our simulations are as follows: $A = 2000 * 2000$, $N = 1000$, $v = [2, 5]$, $T1 = [0, 200]$, $T2 = [0, 100]$, $r = 10$, $b = 0.05$, $\alpha = 0.5$, $\varepsilon = 0.2$, $p = 0.5$, $q = 0.5$, and $\beta = 0.63$. With the above parameters, we can calculate $T_{\max 1} = 5.3495$ from Eq.(27) and $T_{\max 2} = 3.7061$ from Eq.(30). We verify the following situations by simulations.

Case 1: When $T < T_{max2}$, the fraction of infected nodes will monotonically decrease to zero over time.

Case 2: When $T_{max2} < T < T_{max1}$, the fraction of infected nodes will finally decrease to zero, but the drop is not monotonic over time.

Case 3: When $T_{max1} < T$, the fraction of infected nodes will not decrease to zero over time, *i.e.*, the malware will persistantly propagate over time.

Obviously, Case 1 and Case 2 will show the existence and stability of a malware-free T-period solution of Eq.(2), and Case 3 will show the persistence of malware propagation in the MWSN. Firstly, we let $T = 3$, *i.e.*, Case 1. The simulation results are shown in Fig.2(a). Obviously, the simulation results verify Case 1. The simulation results of Eq.(31) are shown in Fig.2(b). From Fig.2(a) and (b), we notice that the time at which $I(t)$ converges to zero with pulse immunization operations is longer than that with traditional continuous immunization operations. This is because the number of pulse immunization operations is less than that of continuous immunization operations. Secondly, we respectively let $T = 3, 4, 4.5$ and 5, *i.e.*, Case 2. The simulation results are shown in Fig.2(c). Clearly, the simulation results is aggreement with Case 2. In addition, we notice that a larger T means a longer convergence time. The reason is similar to that of Case 1. Finally, we let $T = 8$, *i.e.*, Case 3. The simulation results are shown in Fig.2(d). Obviously, the simulation results are consistent with Case 3.

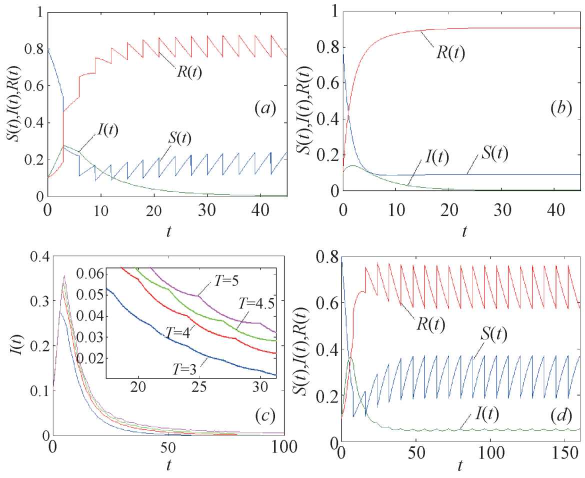


Fig. 2. The verification of Case 1, Case 2, and Case 3

In addition, we observe the impact of the communication radius and mobile speed of nodes on $T_{\max 1}$ and $T_{\max 2}$. With a different mobile speed v and communication radius r of nodes, the values of $T_{\max 1}$ and $T_{\max 2}$ are shown in Fig.3(a) and Fig.3(b), respectively. From Fig.3(a) and Fig.3(b), we notice that a larger v or r means smaller $T_{\max 1}$ and $T_{\max 2}$, respectively. This is because an infected node with a larger r or v can communicate with more susceptible neighbors per unit of time, leading to more susceptible neighbors being infected.

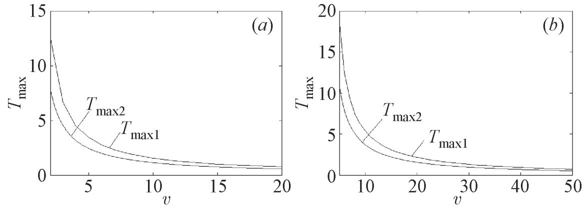


Fig. 3. Impact of r and v on $T_{\max 1}$ and $T_{\max 2}$

VI. Conclusion

Based on the pulse differential equation and the SIR model, a pulse immunization model is proposed for preventing malware from spreading in MWSNs. By analyzing the existence and stability of a malware-free T-period solution of the proposed model, the maximal immunization period of time is derived, every which the immunization operations are implemented on susceptible nodes to minimine the number of immunization operations while ensuring malware extinct over time in the MWSN. The simulation results validate our theoretical analysis.

References

[1] S. Ehsan, K. Bradford, M. Brugger and B. Hamdaoui, “Design and analysis of delay-tolerant sensor networks for monitoring and tracking free-roaming animals”, *IEEE Transactions on Wireless Communications*, Vol.11, No.3, pp.1220–1227, 2012.

[2] J.J. Guo, C. Cho, Y. Wang and K.M. Lee, “Wireless mobile sensor network for the system identification of a space frame bridge”, *IEEE/ASME Transactions on Mechatronics*, Vol.17, No.3, pp.499–507, 2012.

[3] D.R. Zhu, J.H. Han, J. Ou and J. Min, "Single beacon cruise positioning algorithm in wireless sensor networks", *Chinese Journal of Electronics*, Vol.22, No.3, pp.559–562, 2013.

[4] S.L. Xu and S.S. Lee, "Route optimization algorithm for vehicle to vehicle communication using location information", *Chinese Journal of Electronics*, Vol.21, No.4, pp.583–588, 2012.

[5] M.Y. Ko and N. Gautam, "Epidemic-based information dissemination in wireless mobile sensor networks", *IEEE/ACM Transactions on Networking*, Vol.18, No.6, pp.1738–1751, 2010.

[6] P. Li and R.C. Wang, "Research of malicious code attack effect based on synthetic entropy method", *Chinese Journal of Electronics*, Vol.22, No.3, pp.449–454, 2013.

[7] S. Zanero, "Wireless malware propagation: A reality check", *IEEE Security* & *Privacy*, Vol.7, No.5, pp.70–74, 2009.

[8] M.H.R. Khouzani and S. Sarkar, "Maximum damage battery deletion attack in mobile sensor networks", *IEEE Transactions on Automatic Control*, Vol.56, No.10, pp.2358–2368, 2011.

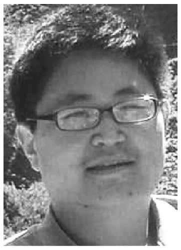
[9] X.M. Wang, Z.B. He, X.Q. Zhao, C. Lin, Y. Pan and Z.P. Cai, "Reaction-diffusion modeling of the malware propagation in mobile wireless sensor networks", *Science China Information Sciences*, Vol.56, No.9, pp.092303:1–092303:18, 2013.

[10] J. Zong, A. Li and L.S. Wen, "SHIS model of e-mail virus propagation", *Chinese Journal of Electronics*, Vol.21, No.4, pp.619–622, 2012.

[11] Y. Yao, L. Guo, H. Guo, G. Yu, F. Gao and X. Tong, "Pulse quarantine strategy of Internet worm propagation: Modeling and analysis", *Computers and Electrical Engineering*, Vol.38, pp.1047–1061, 2012.

[12] F. Verbust, *Nonlinear Differential Equations and Dynamical Systems*, Springer-Verlag, Berlin, Germany, 2000.

WANG Xiaoming was born in 1964. He received the Ph.D. degree in computer science from Northwest University, Xi'an, China, in 2005. He is currently a professor and Ph.D. supervisor in Shaanxi Normal University, Xi'an, China. His main research interests include wireless sensor networks, opportunistic networks. (Email: wangxm@snnu.edu.cn)



HE Zaobo was born in 1988. He received the M.S. degree in computer science from Shaanxi Normal University, Xi'an, China, in 2014. He is a Ph.D. candidate in computer science in Georgia State University, USA. His main research interests include wireless sensor network and social networks. (Email: hezaobo@126.com)

ZHANG Lichen (corresponding author) was born in 1979. He received the M.S. degree and Ph.D. degree in computer science from Shanxi Normal University, Xi'an, China, in 2005 and 2012, respectively. He works as a visiting scholar in Georgia State University, USA, from October 2008 to October 2009. His main research interests include wireless sensor network and opportunistic networks. (Email: zhanglichen@snnu.edu.cn)