Int J Wireless Inf Networks (2011) 18:319–326
DOI 10.1007/s10776-011-0147-z

A Modified SI Epidemic Model for Combating Virus Spread in Wireless Sensor Networks

Shensheng Tang

Received: 1 September 2010 / Accepted: 12 April 2011 / Published online: 23 April 2011

Abstract We study the dynamics of virus spread in wireless sensor networks (WSNs). We first analyze the susceptible-infective (SI) epidemic model for WSNs. In the SI model, once a sensor node is attacked by a virus, the infective node then, using normal communications, spreads the virus to its neighboring nodes, which further spread the virus to their neighbors, the process continues until the whole network fails. To combat this drawback, we propose a modified SI model by leveraging the sleep mode of WSNs to perform system maintenance. The modified SI model can improve the network anti-virus capability and flexibly adapt to different types of virus, without causing any additional hardware effort and signaling overhead. We derive the explicit analytical solutions for the modified SI model, which can capture both the spatial and temporal dynamics of the virus spread process. Extensive numerical results are presented to validate our analysis. The proposed model and analysis method are expected to be used for analysis and design of information (including virus) propagation mechanisms in distributed wireless or computer networks.

Keywords Wireless sensor network · SI epidemic model · Virus spread · Infective node

1 Introduction

In the past decade, wireless sensor networks (WSNs) have received more and more interests in academia, industry, and government due to their potential in civil and military applications [1]. A typical WSN consists of sensors working unattended and transmitting their observation values to some processing or control center (i.e., sink node). The sensor nodes are equipped with limited power and radio communication capabilities. They can be deployed in inaccessible fields, even extremely hostile environments. Since the data transmission range is limited, the data generated from sensors that are far away from the sink must be relayed through intermediate nodes. A source node sends its data to its neighbor nodes, the neighbor nodes again send the data to their respective neighbors.

Due to limited power, modern sensor hardware is usually designed with low-power sleep mode (cf. [2, 3]). The nodes periodically put themselves into sleep mode for an scheduled length of time, and then resume back to active mode. In such a way, significant energy savings can be achieved, and at the same time network connectivity is maintained.

Since sensor nodes are resource-restrained and thus low defense capabilities, sensor nodes become attractive targets for software attacks (like the virus or worm attack on Internet), especially when they are deployed in a hostile environment. Actually, malicious code targeting wireless devices have already started to emerge. For example, the Cabir worm [4] can repeatedly sends itself to the Bluetooth-enabled devices inside its host's scanning range. The Mabir worm [5] uses similar scanning techniques to launch proximity attacks. Thus, security mechanisms that can defend against software attacks are of great interest to the researchers in this field. Since there is a basic similarity between the software virus spread among wireless devices and the transmission of epidemic disease in a population, the epidemiological models extensively used by social researchers (cf. [6–10]) could be appropriately applied to virus spread in wireless networks.

S. Tang (✉)
Department of Engineering Technology, Missouri Western State University, 4525 Downs Dr., St. Joseph, MO 64507, USA
e-mail: stang@missouriwestern.edu

There are a few related applications of epidemic models in wireless environments in the literature [11–16]. In [11], an SI epidemic model was developed for a simple information diffusion algorithm. The impact of node density on information diffusion was investigated analytically. In [12], a new framework called probabilistic queuing was introduced to model virus spread in mobile environments. A network was modeled by multiple queues and each queue represents a separate epidemiological population. As nodes shuttle between queues, they bring their infections with them. In [13], a topologically-aware worm propagation model (TWPM) was developed for wireless sensor networks. Both time and space propagation dynamics can be captured based on their proposed framework. In [14], an epidemic model for mobile phone virus was built which considered the distribution density, coverage radius, and moving velocity of mobile phone. In [15], an epidemic framework was proposed for the vulnerability analysis of current broadcast protocols in wireless sensor networks. The spreading rates of the malicious code for three broadcast protocols were studied and applied to their framework for simulation. In [16], an adaptive probabilistic epidemic protocol for WSN in the urban environment was proposed to adapt to the network topology over time. Through simulation studies, the proposed protocol was shown to improve the system performance.

In this paper, we study the dynamics of virus spread process with respect to time in wireless sensor networks. The virus starts to infect a single node, which spreads the virus to its neighbor nodes. The neighbors repeat the process. We first analyze the susceptible-infective (SI) epidemic model for WSNs. Almost all sensor networks without any anti-virus mechanism may be described as an SI model. We show that in the SI model, once a sensor node is attacked by a virus, the infective node then, using normal communications, spreads the virus to its neighboring nodes, which further spread the virus to their neighbors, the process continues until the whole network fails. In other words, once a node gets infected by a virus, the whole network will eventually fail due to no anti-virus mechanism. To overcome this drawback, we propose a modified SI model by leveraging the sleep mode of WSNs to perform system maintenance functions. The modified SI model can improve the network anti-virus capability and flexibly adapt to different types of virus, without causing any additional hardware effort and signaling overhead. We derive the explicit analytical solutions for the modified SI model, which can capture both the spatial and temporal dynamics of the virus spread process.

The remainder of the paper is organized as follows. Section 2 describes the basics of epidemic theory and virus spread in a WSN. Section 3 analyzes the SI model for WSNs and proposes a modified SI model. The detailed modeling process of virus spread is presented and the explicit analytical results are derived. Section 4 presents numerical results and further enhances the understanding of the analytical results. Section 5 discusses several applications of interest. Finally, the paper is concluded in Sect. 6.

2 Epidemic Theory and WSN Model

In this section, we briefly introduce the basics of epidemic theory and the dynamics of virus spread in a WSN.

2.1 Epidemic Theory

Epidemic theory aims to study the infection outcomes of a population that possess a susceptibility factor with respect to the infection [17]. Generally, epidemic theory considers three variables: agent, host, and environment. Each of these has many components, however, host–agent interactions vary greatly, and variations in environmental conditions influence the interactions in innumerable ways. For example, in influenza study, the agent is the individual who has an influenza virus. The virus is spread by direct contact, or by way of a common media such as water, food, milk, or contaminated air. When an infectious agent invades a host, the host may get infected and become an agent. The agent may be recovered from infection by vaccination and become immune to further infections. Immunity may be temporary, long-lasting, even permanent. Correspondingly, various models exist in epidemic theory that characterize an infection spread, such as Susceptible-Infective-Susceptible (SIS) model (cf. [6]), Susceptible-Infective-Recovered (SIR) model (cf. [7, 15]), and Susceptible-Infective (SI) model (cf. [11]), and applied by epidemiologists, social and behavioral scientists in their respective areas.

In the SIS model, a susceptible individual gets infection and then after an incubation period, the individual becomes susceptible again. In the SIR model, the susceptible individual gets infection, waits for a time period, and recovers and becomes immune to further infections. The Susceptible-Infected (SI) model assumes no immunity or recovered state. In the SI model, any infected individual can contact and infect any other susceptible individual. Hence, the infection spreads at a particular contact rate, at which an infected individual attempts to contact and infect a susceptible individual. At any given instant during the process of infection, the population of infectives and susceptibles can be distinguished. The infective population is the group of individuals that have been infected and the susceptible population is the group of vulnerable individuals, which have not yet been infected.

2.2 WSN Model

We consider a WSN composed of N stationary and identical sensors which are uniformly randomly distributed with the node density denoted by σ on a given geographic field. The sensor nodes are equipped with omnidirectional antennas which have a maximum transmission range of r_0, as shown in Fig. 1. Information generated from some source node can be transmitted to its neighbor nodes inside its signal transmission range. The neighbors nodes continue to transmit the information to their respective neighbors.

Assume that a given node in a WSN gets infected by a virus due to attacks. The virus can be spread together with normal data by the compromised node to its neighbors through different broadcast protocols, such as [18, 19]. If there is no anti-virus mechanism introduced for the WSN, the virus spread process continues, and the number of compromised nodes increases, until the whole network fails (i.e., the number of inoperative nodes exceeds a certain threshold). In such a way, the enemy can easily threats the whole network without a whole-scale physical attacks.

To prevent an outbreak of virus propagation in a WSN, different anti-virus mechanisms may be introduced into the nodes and/or the network. Recall that modern WSNs are usually scheduled the nodes to sleep mode for power saving. In sleep mode, a sensor node is inactive to data transmission. Thus, we propose to utilize this period to perform anti-virus maintenance. This scheme does not introduce additional hardware effort and signaling overhead, but largely improve the node's anti-virus capability. If a powerful anti-virus software is installed, this maintenance can flexibly adapt to different types of virus. Since sensor nodes are resource-restrained devices, the anti-virus maintenance of nodes are assumed to be performed only in sleep mode.

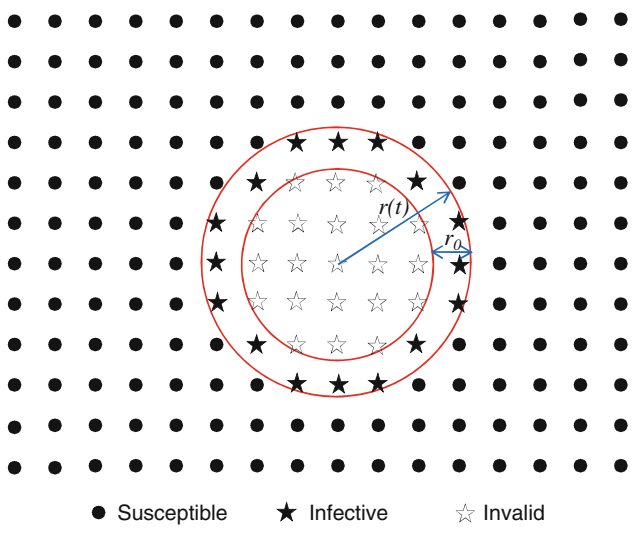

Fig. 1 A model of virus spread in a wireless sensor network

Figure 1 illustrates the proposed virus spread model in a WSN. Initially, all nodes are referred to as *susceptible* nodes until a node (e.g., the center of the circle) is infected by a virus. That node becomes an *infective* node. The infective node, using the normal operation of a broadcast protocol, spreads the virus to its neighboring susceptible nodes, which are located within its signal transmission range. The neighbor susceptible nodes are then infected and spread the virus to their respective neighbors, and the process continues. From Fig. 1, we observe that when all the neighboring susceptible nodes around an infective node get infected, the infective node can not contribute further to the infection spread due to its limited communication range, and thus becomes an *invalid* node. In Fig. 1, all the nodes inside the internal circle are invalid nodes at time t, they are not able to spread virus to the outside susceptible nodes.

3 Modeling and Analysis

Let $S(t)$ and $I(t)$ denote the number of susceptible and infective at time t, respectively. Assume that the total population in the network is constant and denoted by N, then we have $N = S(t) + I(t)$ for any t.

Since the nodes are uniformly randomly distributed with density σ, each infected node can contact $\sigma\pi r_0^2$ nodes every time, which are its neighbors. However, not all of the neighbors lead to new infective nodes. Recall that there are two groups of nodes. Only a susceptible neighbor of the infected node can become a new infective; an infected neighbor leads to nothing changes, since it has already been infected. Due to uniformly distributed deployment, the fraction of the infected node's neighbors that can possibly get infected at time t can be approximated as $S(t)/N$. Let β denote the infection capacity, which represents the probabilistic rate of getting infected in a contact between an infective and a susceptible node. Clearly, β depends on the infectivity of a virus and the communication rate of a protocol, since the virus spreads itself by piggybacking on normal data through regular communications.

3.1 SI Model—Without Anti-Virus Mechanism

In this case, once a node gets infected by a virus, it will remain in infected state due to no anti-virus mechanism. Thus, the number of infected nodes gradually increases with respect to time t. However, the rate of change of infective nodes does not directly depend on the total number of infected node so far. As mentioned above, not all the infected nodes have the capability to infect others.

For example, in Fig. 1, the nodes inside the internal circle at time t are not able to spread virus to the outside susceptible nodes. Only the infective nodes in the circular strip area can infect others. The number of these infective nodes at time t can be calculated as

$$\sigma\pi r(t)^2 - \sigma\pi[r(t) - r_0]^2 \simeq 2\sigma\pi r_0 r(t) \quad \text{as } r(t) \gg r_0,$$

where $r(t)$ is the radius of infection spread at time t. Note that $\sigma\pi r(t)^2 = I(t)$. Recall that each of these infective nodes has $\sigma\pi r_0^2$ neighbors due to limited signal transmission range, among which the susceptible nodes approximately occupies the fraction of $S(t)/N$ at time t. Thus, the basic differential equations that describe the rate of change of susceptible and infective nodes are determined as:

$$\frac{dS(t)}{dt} = -\beta 2(\sqrt{\sigma\pi} r_0)^3 \sqrt{I(t)} \frac{N - I(t)}{N}, \tag{1}$$

$$\frac{dI(t)}{dt} = \beta 2(\sqrt{\sigma\pi} r_0)^3 \sqrt{I(t)} \frac{N - I(t)}{N}, \tag{2}$$

where the initial condition is (Assume only one node gets infected initially):

$$S(0) = S_0 = N - 1 \quad \text{and} \quad I(0) = I_0 = 1. \tag{3}$$

By applying the boundary condition $I(0) = 1$, we solve $I(t)$ as

$$I(t) = N \left(\frac{2}{1 + \frac{\sqrt{N}-1}{\sqrt{N}+1} e^{-\frac{2\beta(\sqrt{\sigma\pi} r_0)^3 t}{\sqrt{N}}}} - 1 \right)^2. \tag{4}$$

The $S(t)$ can be easily obtained by $S(t) = N - I(t)$.

We observe that when $t \to \infty$, $I(t) \to N$, i.e., asymptotically all the nodes eventually get infected. This indicates that the WSN without an anti-virus mechanism is very easy to be attacked and once attacked by only one virus, the whole network will be eventually subject to failure. Next, we propose a modified SI model, which can combat the virus spread.

3.2 Modified SI Model—With Anti-Virus Mechanism

Since modern WSNs are usually scheduled the nodes to sleep mode for power saving, we propose to leverage the sleep periods to perform anti-virus maintenance functions. Let λ_a and λ_s denote the rate that a node goes from the active mode to the sleep mode, and resume from sleep to active mode, respectively. In the sleep mode, the system anti-virus program is automatically triggered. The susceptible nodes will quickly pass the check and go to sleep, while the infective nodes will take longer time for treatment. Depending on the predefined time period of maintenance, a fraction of the maintained infective nodes, denoted by ρ, will be cured and become susceptible nodes when resuming, and the rest will be still go to the infective group. Thus, the basic differential equations can be determined as:

$$\frac{dS}{dt} = -\beta 2(\sqrt{\sigma\pi} r_0)^3 \sqrt{I} \frac{N-I}{N} - \lambda_a S + \lambda_s S + \rho\lambda_s I, \tag{5}$$

$$\frac{dI}{dt} = \beta 2(\sqrt{\sigma\pi} r_0)^3 \sqrt{I} \frac{N-I}{N} - \lambda_a I + (1-\rho)\lambda_s I, \tag{6}$$

where the initial condition is still the same:

$$S(0) = S_0 = N - 1 \quad \text{and} \quad I(0) = I_0 = 1. \tag{7}$$

To keep the total number of nodes stable, we assume that a balance is maintained between the rate going into the maintenance mode and the rate resuming from the maintenance mode, i.e., $\lambda_a = \lambda_s = \lambda$. Thus, the above equations are simplified as:

$$\frac{dS}{dt} = -\beta 2(\sqrt{\sigma\pi} r_0)^3 \sqrt{I} \frac{N-I}{N} + \rho\lambda I, \tag{8}$$

$$\frac{dI}{dt} = \beta 2(\sqrt{\sigma\pi} r_0)^3 \sqrt{I} \frac{N-I}{N} - \rho\lambda I, \tag{9}$$

where $\rho\lambda$ indicates the anti-virus capability, and ρ is related to the performance of the anti-virus program. The larger the value of ρ or λ, the stronger anti-virus capability the system has.

By applying the boundary condition $I(0) = 1$, we solve $I(t)$ as

$$I(t) = \begin{cases} \left(\frac{B+C}{1 + \frac{C-1}{B+1} e^{-\frac{1}{2}A(B+C)t}} - B \right)^2, & I(t) \le C^2, \\ \left(\frac{B+C}{1 - \frac{C-1}{B+1} e^{-\frac{1}{2}A(B+C)t}} - B \right)^2, & I(t) \ge C^2, \end{cases} \tag{10}$$

where $A = \frac{2\beta}{N}(\sqrt{\sigma\pi} r_0)^3$, $B = \sqrt{\left(\frac{\rho\lambda}{2A}\right)^2 + N} + \frac{\rho\lambda}{2A}$, and $C = \sqrt{\left(\frac{\rho\lambda}{2A}\right)^2 + N} - \frac{\rho\lambda}{2A}$.

When $t \to \infty, I(t) \to C^2$, i.e.,

$$I(\infty) = \left(\sqrt{\left(\frac{\rho\lambda}{2A}\right)^2 + N} - \frac{\rho\lambda}{2A} \right)^2.$$

In practice, the first equation in (10) is used to describe the dynamics of virus spread (We will show this in Sect. 5). Once $I(t)$ is obtained, $S(t)$ can be determined by $S(t) = N - I(t)$.

4 Numerical Results

In this section, we do more detailed quantitative analysis for the modified SI model by presenting numerical results in terms of the analytical results obtained. The network is assumed to have $N = 1000$ sensor nodes. The other

parameters β, ρ, λ, r_0, and σ are shown separately with variable values in each figure. As a comparison, the performance of the pure SI model is also displayed in some figures. Note also that all parameters are given in dimensionless units, which can be mapped to specific units of measurement.

Figure 2 shows the number of infective nodes $I(t)$ with respect to the change of parameters β and ρ. As expected, when β is fixed and ρ is increased, the $I(t)$ of the modified SI model decreases. When ρ is fixed and β is increased, $I(t)$ increases. Thus, an increase of ρ or decrease of β will cumber the spread of virus. It is also observed that, as time goes, $I(t)$ in the SI model gradually increases and eventually reaches the maximum number N (definitely at this point the network fails); while $I(t)$ in the modified SI model gradually increases but stops at a certain level depending on the given parameters β and ρ.

Figure 3 shows the response curves of the number of susceptible nodes $S(t)$. As time goes, $S(t)$ in the SI model gradually decreases from $N-1$ until to zero; while $S(t)$ in the modified SI model gradually decreases but remains at a certain level depending on the given parameters β and ρ. This level is kept at a higher point as ρ is increased or β is decreased.

Figure 4 shows the response of the number of infective nodes $I(t)$ with respect to the change of λ and ρ. When λ or ρ is increased, (i.e., increasing the rate of going to sleep mode for maintenance or enhancing the power of anti-virus programs), $I(t)$ decreases quickly. If both λ and ρ are increased, $I(t)$ decreases more quickly. Figure 5 shows the response of the number of susceptible nodes $S(t)$. We observe that an increase of λ or ρ will cumber the spread of virus and thus remain $S(t)$ at a higher level.

Figure 6 shows the response of the number of infective nodes $I(t)$ with respect to different values of the density σ

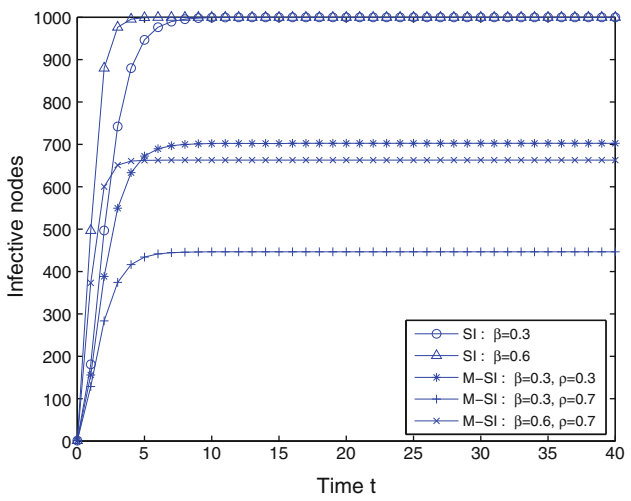

Fig. 2 The response of $I(t)$ w.r.t the change of β and ρ ($\lambda = 1$, $r_0 = 2$, $\sigma = 1$)

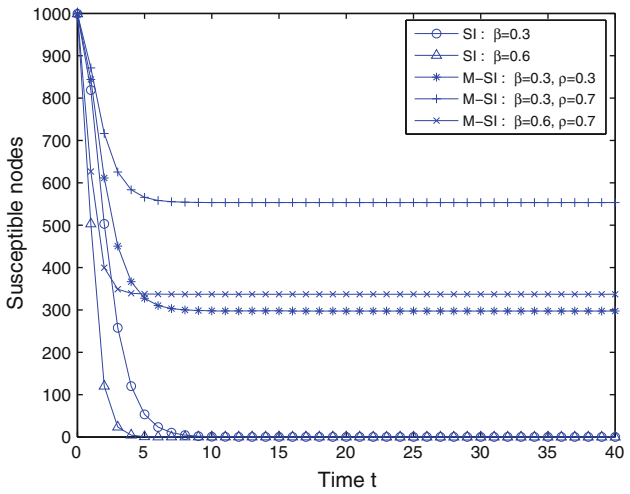

Fig. 3 The response of $S(t)$ w.r.t the change of β and ρ ($\lambda = 1$, $r_0 = 2$, $\sigma = 1$)

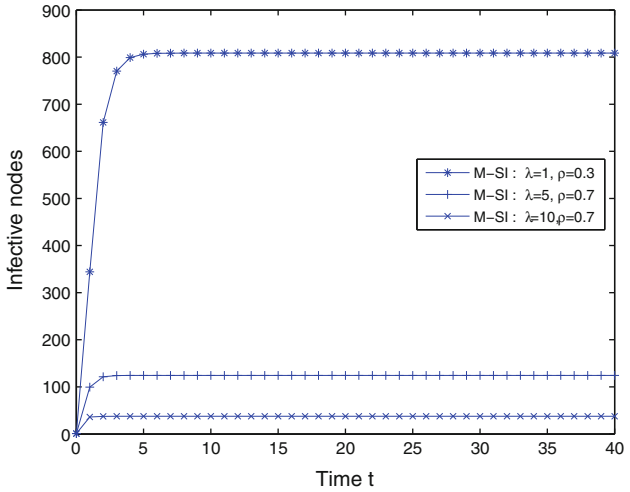

Fig. 4 The response of $I(t)$ w.r.t the change of λ and ρ ($\beta = 0.5$, $r_0 = 2$, $\sigma = 1$)

and the transmission range r_0. The $I(t)$ will become larger as the node density σ is increased or the node's signal transmission range becomes larger. It can also be seen that the maximum point of $I(t)$ is achieved earlier as σ or r_0 is increased. An increase of node density will lead to the increase of infected nodes each time. A stronger signal transmission capability will achieve the same result. This can also be seen in Fig. 7 from another direction. In Fig. 7, the response of the number of susceptible nodes $S(t)$ is illustrated with respect to the change of different σ and r_0. As the node density σ or transmission range r_0 is increased, $S(t)$ will decrease more quickly.

Therefore, by properly designing the parameters ρ, λ, σ, or r_0, the virus spread can be effectively controlled by the modified SI model.

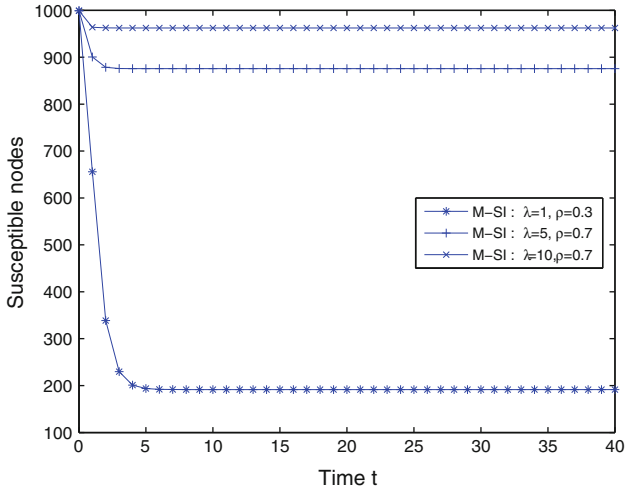

Fig. 5 The response of $S(t)$ w.r.t the change of λ and ρ ($\beta = 0.5$, $r_0 = 2$, $\sigma = 1$)

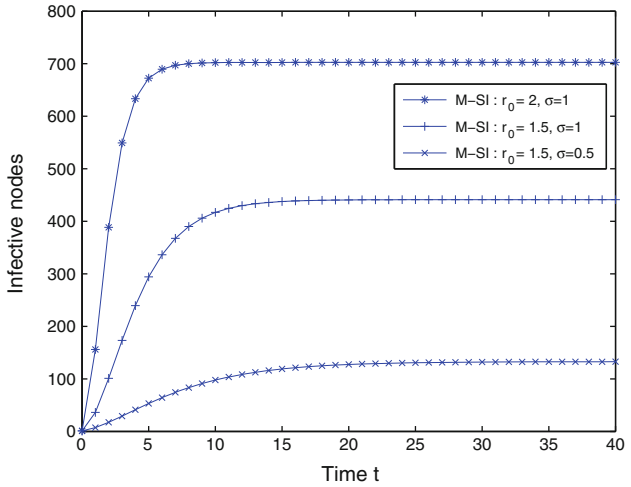

Fig. 6 The response of $I(t)$ w.r.t the change of r_0 and σ ($\beta = 0.3$, $\rho = 0.3$, $\lambda = 1$)

5 Discussion

In this section, we use the analytic results of the modified SI model to discuss several applications of interest.

5.1 What Is the Maximum Number of the Infective Nodes?

When a node gets infected, it will spread to its neighbor nodes, which spread to their respective neighbors. The number of infective nodes will be gradually increased. Due to the anti-virus maintenance mechanism in the modified SI model, the number of infective nodes will be controlled to a certain value and cannot be increased anymore. This value is called the maximum number of the infective nodes, denoted by I_{max}.

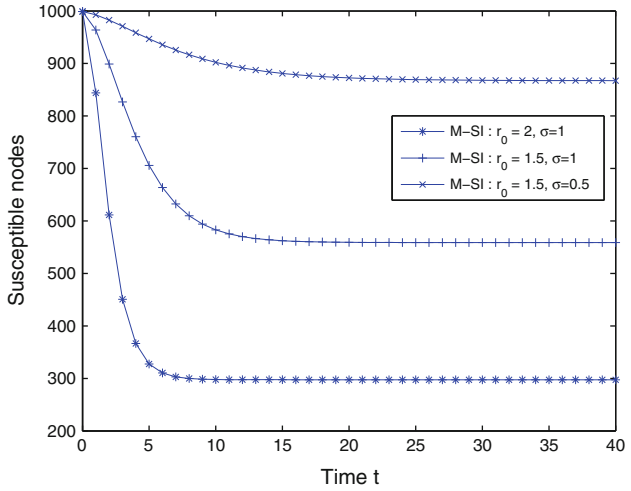

Fig. 7 The response of $S(t)$ w.r.t the change of r_0 and σ ($\beta = 0.3$, $\rho = 0.3$, $\lambda = 1$)

From (9), let $\sqrt{I} = x$, we obtain the following differential equation

$$\frac{dx}{dt} = -\frac{A}{2}(x + B)(x - C), \tag{11}$$

where constants A, B, and C are the same as that given in Sect. 3. Take the derivative of (11), we have

$$\frac{d^2x}{dt^2} = -\frac{A}{2}(2x + B - C). \tag{12}$$

Since $B > C$, x has a maximum value at $\frac{dx}{dt} = 0$, i.e., $x_{max} = C$. Thus, I_{max} is obtained as

$$I_{max} = C^2 = \left(\sqrt{\left(\frac{\rho\lambda}{2A}\right)^2 + N} - \frac{\rho\lambda}{2A}\right)^2, \tag{13}$$

where A is re-written as $A = \frac{2\beta}{N}(\sqrt{\sigma\pi}r_0)^3$. The above result also implies that only the first equation in (10) can be used to describe the dynamics of virus spread in the modified SI model.

5.2 Can a Virus Be Eventually Removed?

In (13), we observe that the virus spread can be controlled to a limited range by appropriately adjusting some or all of the design parameters ρ, λ, σ, and r_0. Particularly, when $\left(\frac{\rho\lambda}{2A}\right)^2 \gg N$, alternatively,

$$\frac{\rho\lambda}{\beta} \gg \frac{4}{\sqrt{N}}(\sqrt{\sigma\pi}r_0)^3, \tag{14}$$

we have $I(t) \to 0$, i.e., the virus is possible to be eliminated eventually. Moreover, if the virus in few compromised nodes cannot be eliminated, the control center can recover

these nodes of abnormal behavior by simply reloading the nodes' programs.

5.3 How to Avoid the Network Failure due to Virus Spread?

The network survivability is very large for a large-scale dense WSN. It usually has the capability to fulfill its mission in the presence of some degree of threats such as attacks, failures, or accidents. However, when a large number of nodes are subject to failures, the network may not be operated normally, which is referred to as the *network failure*.

We define that the network is in failure state when the number of infected nodes is greater than a threshold, say I_F, $0 < I_F \leq N$, i.e., $I(t) > I_F$. In other words, to avoid the network failure, we must satisfy the following condition:

$$I_{max} \leq I_F. \tag{15}$$

Substituting (13) into (15), we have

$$\rho\lambda \geq \frac{2\beta(\sqrt{\sigma\pi}r_0)^3}{\sqrt{I_F}}\left(1-\frac{I_F}{N}\right). \tag{16}$$

The above inequality (16) is called the *network operation condition*. Given some input parameters, one can adjust other parameters to satisfy this condition and thus to avoid network failure. For example, if N, I_F, β are given, we can adjust ρ, λ, σ, and r_0 to satisfy the condition. For the simplest case, we can fix σ, r_0 and ρ, and only adjust λ (i.e., the rate that a node goes from the active mode to the sleep mode), to adapt to the different types of virus (corresponding to different values of β).

6 Conclusion

We have studied the dynamics of virus spread in wireless sensor networks. We first analyze the SI epidemic model for WSNs. In the SI model, once a sensor node is attacked by a virus, the infective node then spreads the virus to its neighboring nodes, which further spread the virus to their neighbors, the process continues until the whole network fails. The SI model does not provide any anti-virus protection for WSNs. To overcome this drawback, we proposed a modified SI model by leveraging the sleep mode of WSNs to perform system maintenance, such as virus check and processing. The modified SI model can improve the network anti-virus capability and flexibly adapt to different types of virus, without causing any additional hardware effort and signaling overhead. We derive the explicit analytical solutions for the modified SI model, which can capture both the spatial and temporal dynamics of the virus spread process. Extensive numerical results are presented to validate the analysis.

It is worthy to note that, although we focused on modeling the virus spread process over a wireless sensor network, the proposed model is applicable to more generic scenarios such as modeling either data dissemination or malware attacks over different types of networks, including wireless networks, computer networks (e.g., the Internet), medical networks, and social networks.

References

1. S. Tang and W. Li, Qos supporting and optimal energy allocation for a cluster-based wireless sensor network, *Elsevier Computer Communications*, Vol. 29, pp. 2569–2577, 2006.
2. D. Yupho and J. Kabara, The effect of physical topology on wireless sensor network lifetime, *Journal of Networks*, Vol. 2, pp. 14–23, 2007.
3. N. A. Pantazisa, D. J. Vergadosb, D. D. Vergadosa, and C. Douligeris, Energy efficiency in wireless sensor networks using sleep mode TDMA scheduling, *Ad Hoc Networks*, Vol. 7, pp. 322–343, 2009.
4. P. Ferrie, P. Szor, R. Stanev, and R. Mouritzen, *Security responses: Symbos.cabir*, tech. rep., Symantec Corporation, 2004.
5. E. Chien, *Security response: Symbos.mabir*, tech. rep., Symantec Corporation, 2005.
6. J.-L. Sanders, Quantitative guidelines for communicable disease control programs, *Biometrics*, Vol. 27, pp. 883–893, 1971.
7. H. W. Hethcote, An immunization model for a heterogeneous population, *Theoretical Population Biology*, Vol. 14, pp. 338–349, 1978.
8. R. Pastor-Satorras and A. Vespignani, Epidemic spreading in scale-free networks, *Physical Review Letters*, Vol. 86, pp. 3200–3203, 2001.
9. M. E. J. Newman, Spread of epidemic disease on networks, *Physical Review E*, Vol. 66, pp. 1–11, 2002.
10. Y. Moreno, M. Nekovee, and A. Vespignani, EfficiLency and reliability of epidemic data dissemination in complex networks, *Physical Review E*, Vol. 69, pp. 1–4, 2004.
11. A. Khelil, C. Becker, J. Tian, and K. Rothermel, Directed-graph epidemiological models of computer viruses. In *Proc. 5th ACM Int'l Workshop on Modeling Analysis and Simulation of Wireless and Mobile Systems*, pp. 54–60, 2002.
12. J. W. Mickens and B. D. Noble, Modeling epidemic spreading in mobile environments. In *Proc. 4th ACM Workshop on Wireless Security (WiSe'05)*, Cologne, Germany, pp. 77–86, 2005.
13. S. A. Khayam and H. Radha, A topologically-aware worm propagation model for wireless sensor networks. In *Proc. 2nd Int'l Workshop on Security in Distributed Computing Systems*, pp. 210–216, 2005.
14. H. Zheng, D. Li, and Z. Gao, An epidemic model of mobile phone virus. In *1st Int'l Symposium on Pervasive Computing and Applications*, pp. 1–5, Aug. 2006.
15. P. De, Y. Liu, and S. K. Das, An epidemic theoretic framework for evaluating broadcast protocols in wireless sensor networks. In *Proc. IEEE Int'l Conf. on Mobile Adhoc and Sensor Systems (MASS), Pisa, Italy*, Oct. 2007.
16. S. K. Tan and A. Munro, Adaptive probabilistic epidemic protocol for wireless sensor networks in an urban environment. In *Proc. 16th International Conference on Computer Communications and Networks (ICCCN 2007)*, pp. 1105–1110, Aug. 2007.
17. R. M. Anderson and R. M. May, *Infectious Diseases of Human: Dynamics and Control*. Oxford University Press, Oxford, 1991.

18. J. W. Hui and D. Culler, The dynamic behavior of a data dissemination protocol for network programming at scale. In *Proc. 2nd International Conference on Embedded Networked Sensor Systems*, Baltimore, MD, pp. 81–94, Nov. 2004.
19. S. Boyd, A. Ghosh, B. Prabhakar, and D. Shah, Gossip algorithms: design, analysis and applications. In *Proc. IEEE INFOCOM'05*, Miami, FL, Mar. 2005.

Author Biography

Shensheng Tang is an assistant professor of Electrical Engineering at Missouri Western State University. He received his B.S. degree from Tianjin University, Tianjin, China, M.S. degree from China Academy of Telecommunications Technology, Beijing, China, and Ph.D. from University of Toledo, Ohio, USA, all in Electrical Engineering. He has 8 years of industrial experience for product development and commercialization in electronics and telecommunications fields, as hardware engineer, system engineer, and manager, respectively. He is a senior member of IEEE and has produced over 40 refereed papers in the areas of communications and networking. His research interests lie in Communication Systems and Networking, Statistical Signal Processing, Modeling and Performance Evaluation.