Analysis of Virus Spread in Wireless Sensor Networks: An Epidemic Model

Shensheng Tang
Dept. of Engineering Technology
Missouri Western State University
St. Joseph, Missouri

Brian L. Mark
Dept. of Electrical and Computer Eng.
George Mason University
Fairfax, Virginia

***Abstract*—We study the potential threat for virus spread in wireless sensor networks (WSNs). Using epidemic theory, we proposed a new model, called Susceptible-Infective-Recovered with Maintenance (SIR-M), to characterize the dynamics of the virus spread process from a single node to the entire network. By introducing a maintenance mechanism in the sleep mode of WSNs, the SIR-M model can improve the network's anti-virus capability and enable the network to adapt flexibly to different types of viruses, without incurring additional computational or signaling overhead. The proposed model can capture both the spatial and temporal dynamics of the virus spread process. We derive explicit analytical solutions for the model and discuss some practical applications of interest. Extensive numerical results are presented to validate our analysis. The proposed model is applicable to the design and analysis of information propagation mechanisms in communication networks.**

I. Introduction

Wireless sensor networks (WSNs) have received extensive attention due to their great potential in civil and military applications [1]. A typical network configuration consists of sensors working unattended and transmitting their observation values to a processing or control center, the so-called sink node, which serves as a user interface. The sensor nodes have limited power and radio communication capabilities. They can be deployed in inaccessible fields, even extremely hostile environments. Due to the limited transmission range, data generated from sensors that are far away from the sink must be relayed through intermediate nodes; i.e., a source node sends its data to its neighbor nodes, which in turn send the data to their respective neighbors. Due to limited power, modern sensor hardware is usually designed with a low-power sleep mode (cf. [2], [3]). The nodes periodically put themselves into sleep mode for a certain length of time, and then return to the active mode. In this way, significant energy savings can be achieved while maintaining network connectivity.

Because sensor nodes are resource-constrained, they generally have weak defense capabilities and are attractive targets for software attacks (like virus or worm attacks on the Internet), especially when the nodes are deployed in a hostile environment. Actually, malicious codes targeting wireless devices have already started to emerge. For example, the Cabir worm [4] can repeatedly send itself to 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 sensor nodes against software attacks is of great interest to the sensor network community.

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]) can be applied to study the spread of viruses in wireless networks. Some related applications of epidemic models in wireless environments have been discussed in the recent literature [11]–[15]. In [11], a Susceptible-Infective (SI) epidemic model was developed for a simple information diffusion algorithm and the impact of node density on information diffusion was investigated analytically. In [12], a topologically-aware worm propagation model (TWPM), which captures both time and space propagation dynamics, was developed for wireless sensor networks. In [13], an epidemic model for a mobile phone virus was developed, which considered the distribution density, coverage radius, and velocity of the mobile phone. By applying results on the application of random graphs to social networks in [9], epidemic theory was applied in [14] to model the spreading process of compromised nodes and identify key factors determining potential outbreaks in sensor networks. In [15], a general framework based on the principles of epidemic theory 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 simulation of the proposed framework.

In this paper, we study the potential threat for virus spread in wireless sensor networks. Using epidemic theory, we propose a new Susceptible-Infective-Recovered with Maintenance (SIR-M) model to describe the dynamics of the virus spread process with respect to time. The virus starts by infecting a single node, which spreads the virus to its neighbor nodes. The neighbors repeat the process. By introducing a maintenance mechanism in the sleep mode of WSNs, our SIR-M model can improve the network's anti-virus capability and enable the network to adapt flexibly to different types of virus, without any additional computational or signaling overhead. The proposed model can capture both the spatial and temporal dynamics of the virus spread process. We derive explicit analytical solutions and

This work was supported in part by the U.S. National Science Foundation under Grant CNS-0520151.

978-1-4244-5048-0/09/$26.00©2009 IEEE

discuss some practical applications of interest. The proposed model and analysis method are applicable to the design and analysis of information (including virus) propagation protocols for communication networks.

The remainder of the paper is organized as follows. Section II describes the basics of epidemic theory and virus spread in a WSN. Section III presents the SIR-M model, including an analysis of the virus spread behavior and applications of interest. Section IV presents numerical results and further enhances the understanding of the analytical results. Finally, the paper is concluded in Section V.

II. Epidemic Theory and WSN Model

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

A. Epidemic Theory

Epidemic theory aims to study the infection outcomes of a population that possess a susceptibility factor with respect to the infection [16]. 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 the study of influenza, the agent is the individual who has an influenza virus. The virus is spread by direct contact, or by way of a common medium 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 recover from the 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 the Susceptible-Infective-Susceptible (SIS) model (cf. [6]) and the Susceptible-Infective-Recovered (SIR) model (cf. [7], [15]), and applied by epidemiologists, social and behavioral scientists in their respective areas. In the SIS model, a susceptible individual is infected and then after an incubation period, the individual becomes susceptible again. In the SIR model, the susceptible individual is infected, waits for a time period, recovers, and then becomes immune to further infections.

B. WSN Model

We consider a WSN composed of N stationary and identical sensors, uniformly randomly distributed with node density σ over a given geographical area. The sensor nodes are equipped with omnidirectional antennas that have a maximum transmission range of r_0 (see Fig. 1). Information generated from a source node can be transmitted to its neighbor nodes inside its signal transmission range. The neighbor nodes relay this information to their neighbors.

Assume that a given node in a WSN is infected by a virus due to attacks. The virus can be spread together with normal data by the compromised node to its neighbors through broadcast protocols (cf. [17], [18]) and thus threatens the entire network without a whole-scale physical attack. To prevent an outbreak of virus propagation in a WSN, network designers may install appropriate anti-virus software on the sensor nodes before deploying them in the field. The anti-virus software operates online and checks the node periodically. New anti-virus patches may be transmitted to each node by the control center. Moreover, the control center may also recover some nodes with abnormal behavior by simply reloading the nodes' programs.

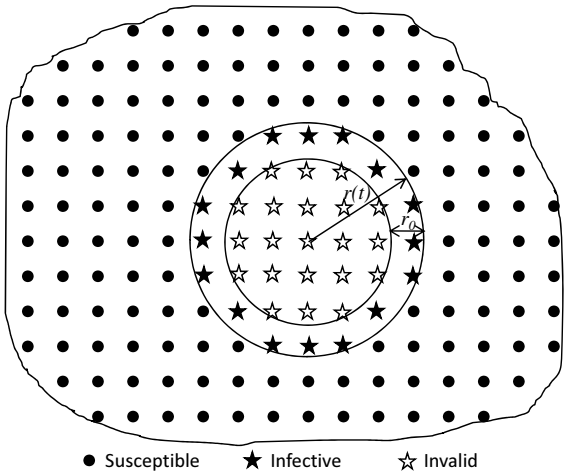

Fig. 1. A Model of Virus Spread in a Wireless Sensor Network.

Sometimes online maintenance may not be enough for a sensor node to combat the infection, since the sensor node is resource-limited and an active node is busy interacting with its neighbors by means of various operations such as "listen", "transmit", "receive", etc. Modern WSNs typically schedule the nodes to sleep during certain periods for power conservation. In sleep mode, a sensor node is inactive with respect to data transmission. We propose to leverage the sleep periods to perform further system maintenance functions, such as in-depth infection check and recovery, or the execution of more powerful anti-virus software which cannot be run in the active mode. The proposed scheme does not incur additional computational burdern, information exchange, or signaling overhead, but can significantly improve the node's anti-virus capability.

Fig. 1 illustrates our 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; such a node is then called an *infective* node. The infective node, through the normal operation of a broadcast protocol, proceeds to spread the virus to its neighboring susceptible nodes, which are located inside its signal transmission range. The neighbor nodes are then infected and spread the virus to their neighbors, and the process continues. From Fig. 1, we observe that when all the neighboring susceptible nodes around an infective node are infected, the infective node can not contribute further to the spread of the infection due to its limited communication

range; thus, the node becomes an *invalid* node. In Fig. 1, all of the nodes inside the inner circle are invalid nodes at time t, i.e., they are not able to spread the virus to the susceptible nodes on the outside.

Next, we study the dynamics of virus spread with time in the network area through quantitative modeling and analysis.

III. Modeling and Analysis

Let $S(t)$, $I(t)$ and $R(t)$ denote the number of susceptible, infective and recovered (or immune) nodes at time t, respectively. Assume that the total population is a constant N, such that $N = S(t) + I(t) + R(t)$ for all t.

Since the nodes are uniformly randomly distributed with density σ, each infected node can contact on the order of $\sigma\pi r_0^2$ neighbor nodes. However, contacting a neighbor does not necessarily lead to a new infective node. Recall that there are three groups of nodes. Only a susceptible neighbor of the infected node can become a new infective node. Contacting an infected neighbor or a recovered neighbor does not change the state of the system, since such a node is either already infected or is immune to infection. Due to the assumption of uniformly distributed node 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. Let γ denote the recovery capacity, which is the probabilistic rate at which an infective node recovers and becomes immune when the infective node is in the active mode. Let λ_a and λ_m denote the rates at which a node transitions from the active mode to the maintenance (sleep) mode, and transitions from maintenance to active mode, respectively. In the maintenance mode, the system maintenance program (including more powerful anti-virus software) is automatically triggered. The susceptible and recovery nodes will quickly pass the check and go to sleep, while the infective nodes will take a longer time for treatment. Depending on the predefined time period of maintenance (or sleep), a fraction of the maintained infective nodes, denoted by p, will be cured and become recovery nodes upon resuming the active mode. The remainder of the nodes will remain in the group of infective nodes. We refer to this modified SIR model as the **SIR-M** model (i.e., SIR with Maintenance).

The basic differential equations that describe the rate of change of susceptible, infective, and recovered nodes are given by

$$\frac{dS(t)}{dt} = -\beta I(t)\frac{\sigma\pi r_0^2}{N}S(t) + \lambda_a S(t) - \lambda_m S(t), \quad (1)$$

$$\frac{dI(t)}{dt} = \beta I(t)\frac{\sigma\pi r_0^2}{N}S(t) + (1-p)\lambda_m I(t) - \lambda_a I(t) - \gamma I(t), \quad (2)$$

$$\frac{dR(t)}{dt} = \gamma I(t) + p\lambda_m I(t) + \lambda_a R(t) - \lambda_m R(t), \quad (3)$$

with the initial conditions

$$S(0) = N-1, I(0) = 1, \text{and } R(0) = 0. \quad (4)$$

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., $\lambda_a = \lambda_m$. Thus, the above equations are simplified as:

$$\frac{dS(t)}{dt} = -\beta I(t)\frac{\sigma\pi r_0^2}{N}S(t), \quad (5)$$

$$\frac{dI(t)}{dt} = \beta I(t)\frac{\sigma\pi r_0^2}{N}S(t) - (p\lambda_a + \gamma)I(t), \quad (6)$$

$$\frac{dR(t)}{dt} = \gamma I(t) + p\lambda_a I(t), \quad (7)$$

where γ and $p\lambda_a$ are refer to active and inactive recovery capacity, respectively.

In Fig. 1, the infection spreads to a radius of $r(t)$ at time t, and the nodes inside the inner circle contribute no further to infection. Thus, the number of susceptible and infective nodes are given, respectively, as

$$S(t) = N - \sigma\pi r(t)^2,$$
$$I(t) = \sigma\pi r(t)^2 - \sigma\pi[r(t) - r_0]^2 - p\lambda_a I(t).$$

From the above equations we obtain

$$I(t) \simeq \frac{2r_0\sqrt{\sigma\pi}}{1+p\lambda_a}\sqrt{N - S(t)} \quad \text{as } r(t) \gg r_0. \quad (8)$$

Applying (8) to (5) and considering the initial condition (4), we have

$$S(t) = N - N\left(\frac{2}{1 + A_0 e^{-A_1 t}} - 1\right)^2, \quad (9)$$

where $A_0 = \frac{\sqrt{N}-1}{\sqrt{N}+1}$, and $A_1 = \frac{2\beta(r_0\sqrt{\sigma\pi})^3}{(1+p\lambda_a)\sqrt{N}}$.

From (5) and (6), we obtain

$$\frac{dI}{dS} = -1 + \frac{(p\lambda_a + \gamma)\cdot N}{\beta\cdot\sigma\pi r_0^2}\frac{1}{S}. \quad (10)$$

Using the initial condition, we derive

$$I(t) = N - S(t) - \frac{\rho N}{\beta\sigma\pi r_0^2}\ln\left(\frac{N-1}{S(t)}\right), \quad (11)$$

where $\rho \triangleq \gamma + p\lambda_a$ is called the total recovery capacity. Substituting (9) into (11), we obtain the expression of $I(t)$ with respect to time t. Finally, $R(t)$ is obtained directly as

$$R(t) = \frac{\rho N}{\beta\sigma\pi r_0^2}\ln\left(\frac{N-1}{S(t)}\right). \quad (12)$$

We have obtained the dynamics of $I(t)$, $S(t)$, and $R(t)$ with respect to time t. Next, we use the analytic results to discuss some practical applications of interest.

A. Maximum number of infective nodes

When a node gets infected, it spreads the infection through regular communication protocols. Consequently, the number of infective nodes will gradually increase. At the same time, the active and inactive recovery mechanisms in the SIR-M model will contribute to a decrease in the number of infective nodes. Thus, there should be a point in time when a maximum value, I_m, of $I(t)$ is achieved.

Setting $\frac{dI}{dS} = 0$ in(10), we obtain

$$S(t) = \frac{\rho N}{\beta\sigma\pi r_0^2}. \tag{13}$$

Since $\frac{d^2I}{dS^2} = -\frac{\rho N}{\beta\sigma\pi r_0^2}\frac{1}{S^2} < 0$, $I(t)$ achieves a maximum value when $S(t) = \frac{\rho N}{\beta\sigma\pi r_0^2}$. Combining (9) and (13), we have

$$t = \frac{1}{A_1}\ln\left(\frac{A_0}{A_2 - 1}\right), \tag{14}$$

where $A_2 \triangleq \frac{2}{1+\sqrt{1-\rho/(\beta\sigma\pi r_0^2)}}$. Thus, (14) determines the time at which $I(t)$ achieves the maximum value I_m.

B. Avoiding network failure due to virus spread

In general, a large-scale dense WSN has relatively high network survivability. Such a WSN usually has the capability to fulfill its mission in the presence of some degree of even serious threats such as attacks, failures, or accidents. However, when many nodes become infected, the network may cease to operate normally, resulting in a condition known as *network failure*. Here, we define the network to be in a 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, the following condition must be satisfied:

$$I_m \leq I_F. \tag{15}$$

From (11) and (13), we obtain

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

The above inequality (16) is called the network operation condition. Given the values of a certain set of network parameters, this condition can be satisfied by adjusting the values of the other parameters, thus avoiding network failure. For example, if N, I_F, β are given, we can adjust ρ (either λ_a, p, or γ, or all of them), σ, and/or r_0 to satisfy the condition.

For illustration purposes, let us fix σ and r_0, and study how the recovery capacity ρ can be adjusted to adapt to the different types of viruses (corresponding to different values of β). The exact solution for ρ can be determined numerically by solving a nonlinear equation based on (16). Here, we derive an explicit approximate solution. Rewrite (16) as

$$\rho\left[1 - \ln\left(\frac{\rho}{\beta\sigma\pi r_0^2}\right) - \ln\left(\frac{N}{N-1}\right)\right] \geq \left(1 - \frac{I_F}{N}\right)\sigma\pi r_0^2. \tag{17}$$

Since $0 < \frac{\rho}{\beta\sigma\pi r_0^2} < 1$ (note that $\sigma\pi r_0^2$ is the number of neighbors of an infected node), we can apply a Taylor series expansion [19] about $\frac{1}{2}$ to obtain the following approximation

$$\ln\left(\frac{\rho}{\beta\sigma\pi r_0^2}\right) \backsimeq \ln\left(\frac{1}{2}\right) + \frac{2\rho}{\beta\sigma\pi r_0^2} - 1. \tag{18}$$

Substituting (18) into (17), we derive a principle for selecting ρ as a function of β:

$$\rho \geq \frac{1}{2}\beta\sigma\pi r_0^2[C_0 - \sqrt{C_0^2 - 2(1 - \frac{I_F}{N})}, \tag{19}$$

where the constant $C_0 \triangleq 1 + \frac{1}{2}\ln(\frac{2(N-1)}{N})$, and it is required that $\frac{I_F}{N} \geq 1 - \frac{1}{2}C_0^2$ (e.g., $\frac{I_F}{N} \geq 0.163$ as $N = 10$, $\frac{I_F}{N} \geq 0.1$ as $N = 100$, $\frac{I_F}{N} \geq 0.094$ as $N = 1000$), which is easily satisfied in practice.

IV. Numerical Results

We present numerical results in terms of the analytical results obtained in Section III. The network is assumed to have $N = 5000$ sensor nodes. The other parameters are set as follows, unless otherwise indicated in the figures: $p = 0.5$; $\lambda_a = 0.5$; $r_0 = 2$; $\sigma = 0.5$ (all parameters are given in dimensionless units). The values of the parameters β and γ are shown in the figures.

Fig. 2 shows the transient response of the number of infective nodes $I(t)$ as a function of various parameters. As expected, over time, $I(t)$ first increases gradually, reaches the maximum point, and then decreases gradually. We also observe that as the recovery capacity γ increases, the outbreak of an infection becomes smaller, and the outbreak point is achieved earlier. As the infection capacity β increases, the results change in an inverse way. An increase in the value of γ or a decrease in β will slow down the spread of the virus.

Fig. 3 shows the transient response of the number of susceptible nodes $S(t)$. As time passes, $S(t)$ decreases gradually to zero. Note that $S(t) = 0$ does not imply a network failure, since an infection process often accompanies a recovery process. We also observe that as γ is changed, $S(t)$ does not change, which can be seen from (9) in Section III. As β increases, $S(t)$ decreases more quickly, since more susceptible nodes will be infected.

Fig. 4 shows the transient response of the number of infective nodes $I(t)$ with respect to different values of the density σ and the transmission range r_0. The maximum value of $I(t)$ increases as the node density σ increases or the node's transmission range becomes larger. It can also be seen that the outbreak point is achieved earlier when σ or r_0 is increased. An increase in the node density leads to an increase in the number of infected nodes. A stronger signal transmission capability achieves the same result, as can be seen from Fig. 5. In Fig. 5, the transient response of the number of susceptible nodes $S(t)$ is illustrated with respect to the changes in the parameters σ and r_0. As the node density σ or transmission range r_0 increases, $S(t)$ decreases more quickly.

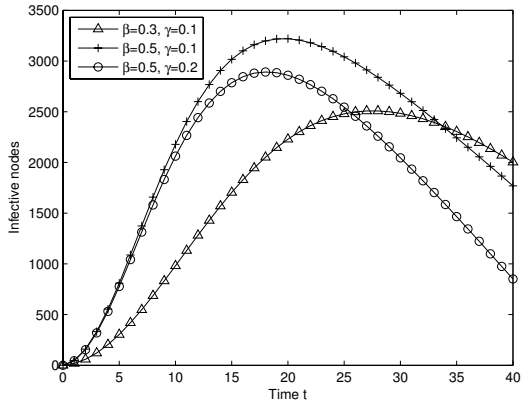

Fig. 2. Transient response of $I(t)$ w.r.t. β and γ.

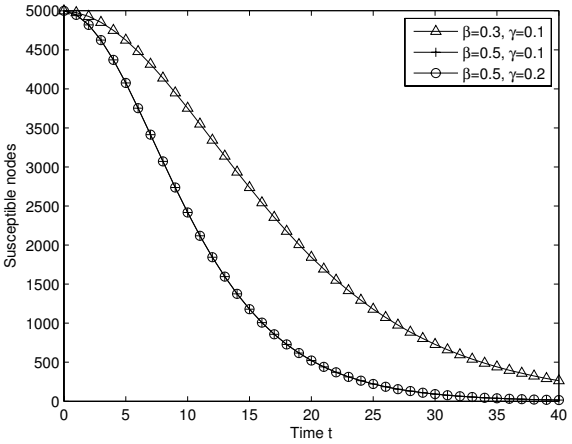

Fig. 3. Transient response of $S(t)$ w.r.t. β and γ.

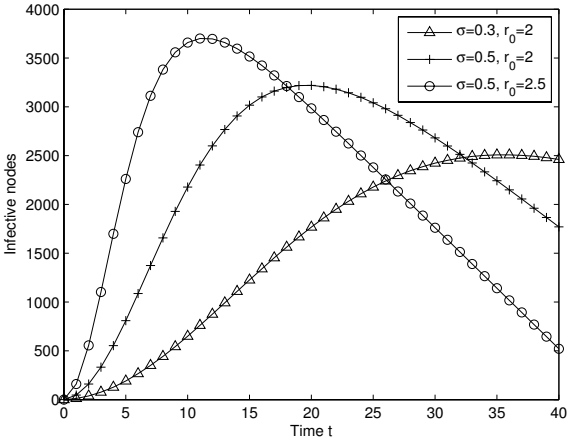

Fig. 4. Transient response of $I(t)$ w.r.t. σ and r_0.

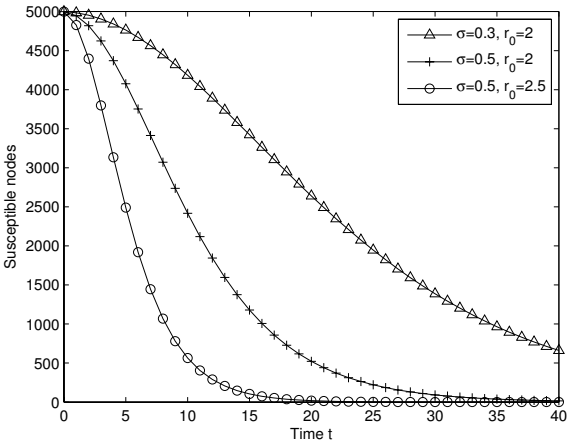

Fig. 5. Transient response of $S(t)$ w.r.t. σ and r_0.

Fig. 6 shows the relationship between $I(t)$ and $S(t)$ under different settings of β and γ. Initially, the number of susceptible nodes is close to $N-1$ while the number of infective nodes is 1. As time passes, $S(t)$ decreases gradually, while $I(t)$ increases gradually. After $I(t)$ achieves the outbreak point, its value decreases gradually. We also observe that as the recovery capacity γ increases, or the infection capacity β decreases, the outbreak point of $I(t)$ becomes smaller. The reason is the same as that in Fig. 2. Fig. 7 shows the relationship between $I(t)$ and $S(t)$ for different values of p, the fraction of infected nodes who are treated in the maintenance mode and then become recovered nodes. As can be observed, the larger the value of p, the more infected nodes will be cured. As seen in Fig. 7, when p is increased, $I(t)$ becomes smaller. When $p = 0$, the maintenance mode fails and the SIR-M model reduces to an SIR model; in this case, the maximum value of the outbreak point is achieved.

Fig. 8 shows the total recovery capacity ρ with respect to the infection capacity β under different network failure thresholds. To check the accuracy of our approximate solution, we compare it with the exact solution obtained, numerically. Both results are closely matched. As seen in Fig. 8, the recovery capacity ρ can be adjusted for different types of viruses (with different values of β). Note that ρ is a linear function of β with different slopes under different thresholds.

V. Conclusion

In this paper, we studied the potential threat of virus spread in wireless sensor networks. Using epidemic theory, we proposed a new SIR-M model to describe the dynamics of the virus spread process from a single node to the entire network. By introducing a maintenance mechanism in the sleep mode of WSNs, our SIR-M model can improve the network's anti-virus capability and enable the network to adapt to different types of viruses without additional computational or signaling overhead. The proposed model captures both the spatial (e.g., node density, transmission range) and the temporal (e.g., transient responses of $S(t)$, $I(t)$, and $R(t)$) dynamics of the virus spread process.

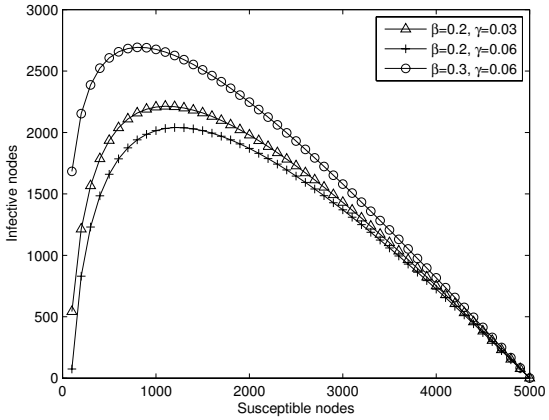

Fig. 6. $I(t)$ vs. $S(t)$ w.r.t. β and γ.

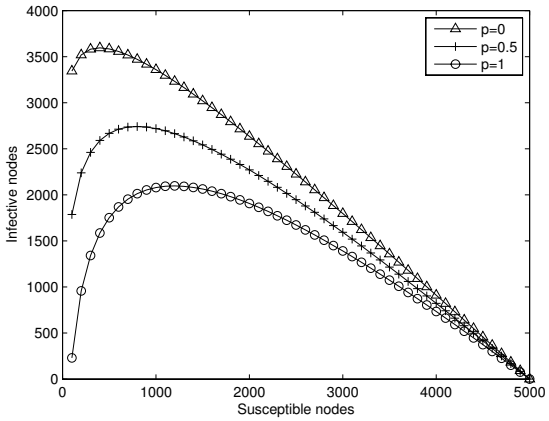

Fig. 7. $I(t)$ vs. $S(t)$ w.r.t. p.

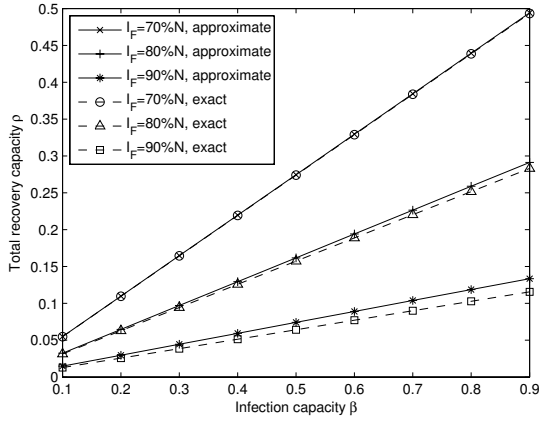

Fig. 8. Total recovery capacity ρ w.r.t. infection capacity β under different network failure thresholds I_F.

We derived explicit solutions for the number of nodes in different groups with respect to time and discussed some practical applications of interest. Extensive numerical results were presented to validate our analysis. It is worthwhile to note that although we focused on modeling the virus spread process in a wireless sensor network, the proposed model is applicable to more general scenarios, such as modeling either (useful) data dissemination or a malware attack 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, Aug. 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, Sep. 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, Mar. 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, Dec. 1971.

[7] H. W. Hethcote, "An immunization model for a heterogeneous population," *Theoretical population biology*, vol. 14, pp. 338–349, Dec. 1978.

[8] R. Pastor-Satorras and A. Vespignani, "Epidemic spreading in scale-free networks," *Physical Review Letters*, vol. 86, pp. 3200–3203, Apr. 2001.

[9] M. E. J. Newman, "Spread of epidemic disease on networks," *Physical Review E*, vol. 66, pp. 1–11, July 2002.

[10] Y. Moreno, M. Nekovee, and A. Vespignani, "Efficiency and reliability of epidemic data dissemination in complex networks," *Physical Review E*, vol. 69, pp. 1–4, May 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] 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.

[13] 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.

[14] P. De, Y. Liu, and S. K. Das, "Modeling node compromise spreading in wireless sensor networks using epidemic theory," in *Proc. IEEE WoWMoM 2006*, (Niagara-Falls, NY), June 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] R. M. Anderson and R. M. May, *Infectious Diseases of Human: Dynamics and Control*. Oxford: Oxford Univ. Press, 1991.

[17] 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.

[18] S. Boyd, A. Ghosh, B. Prabhakar, and D. Shah, "Gossip algorithms: Design, analysis and applications," in *Proc. IEEE INFOCOM'05*, (Miami, FL), Mar. 2005.

[19] M. Abramowitz, *Handbook of Mathematical Functions: with Formulas, Graphs, and Mathematical Tables*. Government Printing Office, 10th ed., June 1984.