J Comb Optim (2010) 20: 47–62
DOI 10.1007/s10878-008-9190-9

EiSIRS: a formal model to analyze the dynamics of worm propagation in wireless sensor networks

Xiaoming Wang · Qiaoliang Li · Yingshu Li

Published online: 10 October 2008

Abstract Based on the epidemic theory, this paper proposes a novel model for analyzing the dynamics of worm propagation in Wireless Sensor Networks (WSNs). The proposed model supports the sleep and work interleaving schedule policy for sensor nodes, and it can also describe the process of multi-worm propagation in WSNs. In addition, a necessary condition for worms to spread in WSNs is derived, which may be useful in designing a secure WSN. Simulation results show that the process of worm propagation in WSNs is sensitive to the energy consumption of nodes and the sleep and work interleaving schedule policy for nodes. Therefore, this paper provides new insights for the dynamics of worm propagation in WSNs.

Keywords WSN · Worm propagation · Epidemic theory · Differential equation · Simulation

X. Wang and Q. Li are supported by NSFC-60773224,10571052, and Key Project of Ministry of Education of China (Grant 107106).

X. Wang (✉)
School of Computer Science, Shaanxi Normal University, Xi'an, Shaanxi 710062, China
e-mail: wangxm@snnu.edu.cn

X. Wang · Q. Li · Y. Li
Department of Computer Science, Georgia State University, Atlanta, GA 30319, USA

Y. Li
e-mail: yli@cs.gsu.edu

Q. Li
School of Computer and Communication, Hunan University, Changsha, Hunan 410081, China
e-mail: qli@cs.gsu.edu

1 Introduction

Wireless sensor networks (WSNs) exhibit promising applications in many fields, such as smart home, biological monitoring, battlefield surveillance, and target tracking. Typically, a WSN consists of a large number of wireless sensors. Each wireless sensor is also called a node. For each node, its wireless communication range, computation capabilities and energy are very limited. Neighboring nodes can directly communicate with each other. A node senses physical parameters in the sensing range of the node. As data packets, a node processes the sensed data, or delivers the sensed data to some neighboring nodes of this node. Some neighbors that receive data packets continue to process or deliver the data packets towards the sink node in multi-hop mode. The sink node is a more sophisticated node with much more energy and communication and computing capabilities where the collected data packets are deeply processed or analyzed, or further delivered to the final destination through a wired network. As the potential applications of WSNs are increasing more and more, worms, as one kind of malicious codes, become one of the main threats to the security of WSNs (Syed and Hayder 2006; Pradip et al. 2007).

To defend against the worms, we need to accurately understand the dynamic characteristics of worm propagation in networks. Formal models of worm propagation are an important theoretical basis for analyzing the dynamic behavior of worm propagation in networks. By formally modeling the process of worm propagation in networks, we can effectively analyze the trace of worm propagation, and precisely predict the trend of worm propagation in the future. In particular, by using a formal model of worm propagation, we may estimate the time point at which worms start to quickly spread in a network in order to take preventing measures. In practice, the process of worm propagation on the Internet is very similar to that of biological virus propagation in the population, so the process of worm propagation on the Internet has been widely studied based on the epidemic theory (Frauenthal 1981; Chen et al. 2003; Dantu et al. 2007; Eugster et al. 2004; Moore et al. 2003; Okamura et al. 2005; Yang et al. 2005; Zou et al. 2007), which effectively models the process of biological virus propagation in the population. However, due to new characteristics of WSNs, such as frequent topology change, high density of nodes, limited energy of nodes, smaller communication range of nodes, and the sleep and work interleaving schedule policy for nodes, the mechanism of worm propagation in WSNs is significantly distinct with that of worm propagation on the Internet. So formal models for analyzing the dynamics of worm propagation on the Internet may not be directly used to analyze the dynamics of worm propagation in WSNs. To the best of our knowledge, little attention has been paid to formal models of worm propagation in WSNs. Facing serious worm threats to the security of WSNs, we need to develop new formal models to precisely describe and analyze the process of worm propagation.

According to our observation, the process of worm propagation in a WSN has three new characteristics, whereas these characteristics do not occur in the process of worm propagation on the Internet. We state the three new characteristics of worm propagation in a WSN as follows:

- A worm residing in a host on the Internet tries to infect other hosts by randomly scanning through the IP addresses of other hosts, whereas a worm residing in a

node in a WSN may just spread to its neighbors, which can directly communicate with this node.

- To prolong the network lifetime, the sleep and work interleaving schedule policy is usually applied to schedule nodes in a large scale WSN. This implies that, when a node is working, a worm residing in this node may spread to the working neighbors of this node, but the sleeping neighbors of the node are not infected. Moreover, when a node is sleeping, any worm residing in this node cannot infect other nodes.
- As the energy of nodes is exhausted, more and more nodes become dead nodes. Any worm residing in other nodes cannot infect these dead nodes. Moreover, when a node dies, it becomes a dead node. All of the worms which ever resided in the dead nodes immediately disappear from the dead nodes. This means that the dead nodes no longer participate in the process of worm propagation in a WSN.

In addition, multi-worm spreading will become a main attack way in large scale WSNs in the future. Therefore, formal models of worm propagation must be able to describe the process of multi-worm propagation in WSNs. However, most of the existing formal models of worm propagation on the Internet cannot describe the process of multi-worm propagation.

The above characteristics significantly affect the dynamic behavior of worm propagation in a WSN. In Syed and Hayder (2006), Pradip et al. (2007), two formal models of worm propagation in a WSN have been proposed based on the differential equation or the random graph theory. However, these models only improved the existing models of worm propagation on the Internet by limiting the range of worm propagation, without considering the above important characteristics of worm propagation in a WSN. Therefore, these models usually overestimate the speed of worm propagation in a WSN and they can not precisely predict the time point at which the peak of worm propagation occurs. Hence, these models cannot accurately describe the process of worm propagation in a WSN. In Zou et al. (2005), the so-called SIR (Susceptible-Infected-Removed) model is proposed to describe the process of worm propagation on the Internet, and it is widely applied in analyzing the dynamics of worm propagation on the Internet. However, due to different patterns of worm propagation on the Internet and in a WSN, the SIR model may not be directly used to describe the process of worm propagation in a WSN. In Wang and Li (2008), the so-called iSIRS model is proposed based on the new concept of dead state of nodes. The iSIRS model may describe the process of worm propagation with energy consumption of nodes in a WSN. However, the iSIRS model cannot effectively describe the process of worm propagation considering the sleep and work interleaving schedule policy which is generally used to schedule sensor nodes to prolong the lifetime of a WSN, especially a large scale WNS.

To overcome the disadvantage of the iSIRS model, we introduce the working state and sleeping state of nodes to expand the iSIRS model in this paper. we called the expanded model EiSIRS model. The EiSIRS model is based on the epidemic theory and the differential equation, and it can precisely describe the process of worm propagation in a WSN. In addition, we also theoretically derive a necessary condition for worms to spread in a WSN. Simulation results show that the EiSIRS model is valid. Hence, the EiSIRS model is a more practical formal model for analyzing the dynamics of worm propagation in a WSN and it may also be useful in designing a secure WSN.

The remainder of the paper is organized as follows. In Sect. 2, the related work is introduced. In Sect. 3, we propose a novel formal model of worm propagation in a WSN, which consists of differential equations. In addition, we also derive a necessary condition for worms to spread in a WSN. In Sect. 4, simulation results are presented to demonstrate the validity of the proposed model. The conclusion of this paper is in Sect. 5.

2 Related work

The current research on the process of worm propagation in networks is mainly based on the epidemic theory and the state machine. To analyze the dynamics of worm propagation on the Internet, many formal models have been proposed in recent years. Classical models of worm propagation on the Internet are the Susceptible-Infected-Susceptible (SIS) model (Kephart and White 1991), the Susceptible-Infected-Recovered/Susceptible (SIR) model (Zou et al. 2005), the Two-Factor model (Kim et al. 2004) and the Improved Worm Mitigation (IWM) model (Onwubiko et al. 2005). These models consist of differential equations and they can effectively describe the process of worm propagation on the Internet to some extent. However, due to new characteristics of WSNs, formal models of worm propagation on the Internet may not be directly applied to describe the process of worm propagation in WSNs. In Wang and Li (2008), the so-called iSIRS model is proposed to describe the process of worm propagation with energy consumption of nodes in WSNs. In this paper, our objective is to expand the iSIRS model to support the sleep and work interleaving schedule policy for nodes. Therefore, the SIR model and the iSIRS model are briefly introduced as follows.

In the SIR model, a host stays in one of the three states: *susceptible state*, *infectious state* and *removed state*. If a host has been infected by Internet worms, then its current state is called infectious state. If a host has not been infected by any worm, then its current state is called susceptible state. When a host is in infectious state, it will not be infected by the same type of worms residing in this host. Each susceptible host may become an infectious host with the probability β in a unit time. When an infectious host is cleaned of worms with the probability γ in a unit time, the host may become a removed host and the removed host is immune to the same type of worms cleaned from this host. In general, the values of β and γ are distinct. Suppose that the initial number of hosts on the Internet is N. At instant t, the number of infectious hosts is $I(t)$, the number of susceptible hosts is $S(t)$ and the number of removed hosts is $R(t)$. Then the SIR model is formalized as follows:

$$\frac{dI(t)}{dt} = \beta I(t)S(t) - \gamma I(t), \tag{1}$$

$$\frac{dS(t)}{dt} = -\beta I(t)S(t), \tag{2}$$

$$\frac{dR(t)}{dt} = \gamma I(t), \tag{3}$$

$$I(t) + S(t) + R(t) = N. \tag{4}$$

In the SIR model, all the susceptible hosts are assumed to be working forever. However, this assumption does not hold in WSNs due to the limited energy of nodes and the sleep and work interleaving schedule policy used in large scale WSNs. In addition, although a removed node is immune to the same type of worms cleaned from this node before the instant t, this node may be infected by the new worms which occur after the instant t. Hence the SIR model may not be directly used to describe the process of worm propagation in WSNs.

To overcome the shortcoming of the SIR model, the so-called iSIRS model is proposed in Wang and Li (2008). The iSIRS model is an improved SIR model. In the iSIRS model the nodes in a WSN are classified into four sets (states):

- *Susceptible node set S*: the nodes in S have not been infected by any worm in a WSN and these nodes are vulnerable to worms.
- *Infectious node set I*: the nodes in I have been infected by worms in a WSN and they may infect some nodes in S.
- *Recovered node set R*: the nodes in R used to be infected by worms, they are cleaned of worms and are immune to the same type of cleaned worms. However, recovered nodes may be infected by new worms occurring in a WSN in the future.
- *Dead node set D*: the nodes in D never work with their energy exhausted. Thus any worm cannot infect these nodes.

At any instant t, the number of nodes in S, I, R or D is denoted by $S(t)$, $I(t)$, $R(t)$ or $D(t)$, respectively. In a unit time, a susceptible node becomes an infectious node with the probability α_1; an infectious node is cleaned of worms and becomes a recovered node with the probability α_4; a recovered node becomes a susceptible node with the probability α_5. Due to the energy consumption of nodes, a susceptible node, an infectious node or a recovered node becomes a dead node with the probabilities α_2, α_3, or α_6, respectively. In addition, the average number of worms in an infectious node is k in a unit time, and the above probabilities are mutually independent. Then the iSIRS model is formalized as follows.

$$\frac{dI(t)}{dt} = \frac{r^2}{q^2}\alpha_1 kI(t)S(t) - \alpha_3 I(t) - \alpha_4 I(t), \tag{5}$$

$$\frac{dS(t)}{dt} = \alpha_5 R(t) - \frac{r^2}{q^2}\alpha_1 kI(t)S(t) - \alpha_2 S(t), \tag{6}$$

$$\frac{dR(t)}{dt} = \alpha_4 I(t) - \alpha_5 R(t) - \alpha_6 R(t), \tag{7}$$

$$\frac{dD(t)}{dt} = \alpha_2 S(t) + \alpha_3 I(t) + \alpha_6 R(t), \tag{8}$$

$$I(t) + S(t) + R(t) + D(t) = N. \tag{9}$$

However, the iSIRS model does not support the sleep and work interleaving schedule policy for nodes in WSNs, especially large scale WSNs. Hence, the iSIRS model does not precisely describe the process of worm propagation in WSNs. To overcome the disadvantage of the iSIRS model, we introduce new concepts of working state and sleeping state of nodes to expand the iSIRS model in this paper. We propose a

new formal model of worm propagation to precisely describe the process of worm propagation in WSNs.

3 Model derivation

3.1 Network model and assumption

A WSN consists of n static and identical wireless sensors. Each sensor is called a node. The nodes are uniformly distributed in a circle area with radius q. The nodes are equipped with omni-directional antennas and the wireless communication range of each node is a circle area with radius r. The energy of each node is provided by batteries with limited power, and the batteries may not be recharged. We classify the nodes into the following set (states):

- *Susceptible working node set* S: the nodes in S have not been infected by any worm, they are working and vulnerable to worms. That is, the nodes in S may be infected by worms residing in some working neighbors of these nodes.
- *Susceptible sleeping node set* S': the nodes in S' have not been infected by any worm and they are sleeping. Although these nodes in S' are also vulnerable to worms, worms do not try to infect these nodes. The reason is that these nodes cannot communicate with their working neighbors.
- *Infectious working node set* I: the nodes in I have been infected by worms, and these nodes are working. For any node in I, a worm residing in this node may infect some susceptible working neighbors of this node and a worm residing in a working neighbor of this node may also infect this node.
- *Infectious sleeping node set* I': the nodes in I' have been infected by worms and these nodes are sleeping. So worms residing in these nodes do not try to infect other nodes and worms residing in other nodes cannot infect the nodes in I'. It is because the nodes in I' cannot communicate with their working neighbors.
- *Recovered working node set* R: the nodes in R used to be infected by some worms, but they are now cleaned of worms. So the nodes in R are immune to such a type of cleaned worms. Moreover, the nodes in R are currently working and they may be infected by new worms residing in some working neighbors of this nodes.
- *Recovered sleeping node set* R': the nodes in R' used to be infected by worms, but they are cleaned of worms. Hence the nodes in R' are immune to the same type of cleaned worms. Moreover, the nodes in R' are currently sleeping. So the worms does not try to infect the nodes in R'.
- *Dead node set* D: the nodes in D are dead with their energy exhausted. Hence any worm does not try to infect the nodes in D. Usually, the set D includes the nodes which cannot work from now on. For example, the nodes which have exhausted their energy or which are physically destroyed or which are logically removed from the network, and so forth.

At any instant t, the cardinalities of S, S', I, I', R, R' and D are denoted by $S(t)$, $S'(t)$, $I(t)$, $I'(t)$, $R(t)$, $R'(t)$ and $D(t)$, respectively. In this paper, we make the following assumptions:

- All of worms only reside in some nodes in I or I'.
- At the initial instant $t = 0$, the values of $I'(0)$, $R(0)$, $R'(0)$, $S'(0)$ and $D(0)$ are 0, and the values of $S(0)$ and $I(0)$ are greater than zero.
- In a unit time the state of each node is one of the seven states. A node transits from its current state to another with the susceptible-infectious-recovery-susceptible (SIRS) mechanism of worm propagation and the sleep and work interleaving schedule policy for nodes.
- The probabilities with which a node in S becomes a node in I, D or S' are α_1, α_2 or α_{12}; the probabilities with which a node in I becomes a node in D, R or I' are α_3, α_4 or α_8; the probabilities with which a node in R becomes a node in S, D or R' are α_5, α_6 or α_{10}; the probability with which a node in S' becomes a node in S is α_{11}; the probability with which a node in I' becomes a node in I is α_7; the probability with which a node in R' becomes a node in R is α_9.

According to our observation, the above probabilities are related to practical applications and mutually independent of each other.

3.2 Transition relationship between node states

Based on the assumptions and the epidemic theory (Frauenthal 1981), we use a labeled directed graph $G(V, E, L)$ to describe the transition relationships between node states, as shown in Fig. 1. Here, V is the set of vertex, and $V = \{S, S', I, I', R, R', D\}$; E is the set of edges, L is the set of edge labels, and $E \subset V \times V \times L$.

In Fig. 1, for $X, Y \in V$, and $Z \in L$, if there is a directed edge $(X, Y, Z) \in E$ from X to Y, then (X, Y, Z) means that Z nodes in X change their states to Y in a unit time. For example, the edge $(I, R, \alpha_4 I(t))$ implies that $\alpha_4 I(t)$ nodes in I change their states to R in a unit time. As for the edge $(S, I, \alpha_1 k S''(t))$, k is the average number of worms in each node in I in a unit time and $S''(t)$ is the number of the susceptible working neighbors of a node in I in a unit time. Clearly, $S''(t)$ is usually much less than $S(t)$ due to the limited communication range of nodes and the sleep and work interleaving schedule policy applied in a large-scale WSN. This is very different from the mechanism of worm propagation on the Internet. To the best of our knowledge, this difference is neglected in the models proposed in Syed and Hayder (2006) and Pradip et al. (2007). Additionally, their models do not describe the process of multi-worm propagation, whereas multi-worm propagation will become a main attack way in a large scale WSN. In our model, the above issues are addressed.

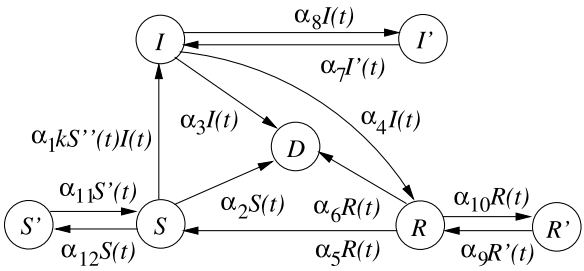

Fig. 1 State transition relationships of nodes in a WSN

3.3 Model formalization

Let $[t, t+\Delta t]$ be a time interval. Here, Δt is a segment of time starting from t. $\Delta t \geq 0$ and it is small enough. According to the epidemic theory and the state transition relationship of nodes (see Fig. 1), the fluctuating number of nodes in I from t to $t+\Delta t$ is calculated by (10).

$$I(t+\Delta t) - I(t) = (\alpha_1 k S''(t) I(t) + \alpha_7 I'(t) - \alpha_3 I(t) - \alpha_4 I(t) - \alpha_8 I(t))\Delta t. \quad (10)$$

Let the communication area of each node in a WSN be S_r, and the density of nodes in S be $p(t)$ at instant t. The wireless communication radius of each node is r. Then the communication area S_r may be calculated by (11).

$$S_r = \pi r^2. \quad (11)$$

The node density $p(t)$ is calculated by (12) at instant t.

$$p(t) = \frac{S(t)}{\pi q^2}. \quad (12)$$

The number of susceptible working neighbors of each node is calculated by (13) at instant t.

$$S''(t) = S_r p(t). \quad (13)$$

From (11)–(13), we have the following equation:

$$S''(t) = \frac{r^2}{q^2} S(t). \quad (14)$$

From (10) and (14), the fluctuating number of nodes in I from t to $t+\Delta t$ is calculated by (15).

$$I(t+\Delta t) - I(t) = \left(\frac{r^2}{q^2}\alpha_1 k S(t) I(t) + \alpha_7 I'(t) - \alpha_3 I(t) - \alpha_4 I(t) - \alpha_8 I(t)\right)\Delta t. \quad (15)$$

Similar to the derivation of (15), we can derive (16), which calculates the fluctuating number of nodes in S from t to $t+\Delta t$.

$$S(t+\Delta t) - S(t) = \left(\alpha_5 R(t) + \alpha_{11} S'(t) - \frac{r^2}{q^2}\alpha_1 k S(t) I(t) - \alpha_2 S(t) - \alpha_{12} S(t)\right)\Delta t. \quad (16)$$

The fluctuating number of nodes in R from t to $t+\Delta t$ is calculated by (17).

$$R(t+\Delta t) - R(t) = (\alpha_4 I(t) + \alpha_9 R'(t) - \alpha_5 R(t) - \alpha_6 R(t) - \alpha_{10} R(t))\Delta t. \quad (17)$$

The fluctuating number of nodes in D from t to $t+\Delta t$ is calculated by (18).

$$D(t+\Delta t) - D(t) = (\alpha_2 S(t) + \alpha_3 I(t) + \alpha_6 R(t))\Delta t. \quad (18)$$

The fluctuating number of nodes in I' from t to $t+\Delta t$ is calculated by (19).

$$I'(t+\Delta t)-I'(t)=(\alpha_8 I(t)-\alpha_7 I'(t))\Delta t. \tag{19}$$

The fluctuating number of nodes in S' from t to $t+\Delta t$ is calculated by (20).

$$S'(t+\Delta t)-S'(t)=(\alpha_{12} S(t)-\alpha_{11} S'(t))\Delta t. \tag{20}$$

The fluctuating number of nodes in R' from t to $t+\Delta t$ is calculated by (21).

$$R'(t+\Delta t)-R'(t)=(\alpha_{10} R(t)-\alpha_9 R'(t))\Delta t. \tag{21}$$

Generally speaking, the total number of nodes in a large scale WSN could be very large. Hence we may believe that the number of nodes in different states continually changes within Δt. Further, we derive the following differential equations (22)–(28) from (15)–(21), respectively.

$$\frac{dI(t)}{dt}=\frac{r^2}{q^2}\alpha_1 kS(t)I(t)+\alpha_7 I'(t)-\alpha_3 I(t)-\alpha_4 I(t)-\alpha_8 I(t), \tag{22}$$

$$\frac{dS(t)}{dt}=\alpha_5 R(t)+\alpha_{11} S'(t)-\frac{r^2}{q^2}\alpha_1 kS(t)I(t)-\alpha_2 S(t)-\alpha_{12} S(t), \tag{23}$$

$$\frac{dR(t)}{dt}=\alpha_4 I(t)+\alpha_9 R'(t)-\alpha_5 R(t)-\alpha_6 R(t)-\alpha_{10} R(t), \tag{24}$$

$$\frac{dD(t)}{dt}=\alpha_2 S(t)+\alpha_3 I(t)+\alpha_6 R(t), \tag{25}$$

$$\frac{dI'(t)}{dt}=\alpha_8 I(t)-\alpha_7 I'(t), \tag{26}$$

$$\frac{dS'(t)}{dt}=\alpha_{12} S(t)-\alpha_{11} S'(t), \tag{27}$$

$$\frac{dR'(t)}{dt}=\alpha_{10} R(t)-\alpha_9 R'(t). \tag{28}$$

Let the initial number of nodes in a WSN be N. At any instant t, the following equation holds.

$$I(t)+S(t)+R(t)+D(t)+I'(t)+S'(t)+R'(t)=N. \tag{29}$$

The EiSIRS model consists of (22)–(29) and it is a dynamic feedback differential system.

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

Theorem 1 *For a given WSN, the number of nodes is N, and these nodes are uniformly deployed in a circle area with radius q, and the communication range of each node is a circle area with radius r. At the initial instant $t=0$, the average number*

of worms in every infectious working node is k, the number of susceptible working nodes is $S(0)$. k worms in an infectious working node may spread in the WSN, only if the condition $S(0) > \frac{(\alpha_3+\alpha_4+\alpha_8)q^2}{\alpha_1 kr^2}$ is satisfied. Otherwise, k worms cannot spread in the WSN. Here, $\alpha_1, \alpha_3, \alpha_4$ and α_8 are the same as ones of Sect. 3.1, respectively.

Proof For k worms in an infectious working node in a WSN, if k worms can successfully spread in the WSN at the initial instant $t = 0$, then the following condition must be satisfied.

$$\left.\frac{dI(t)}{dt}\right|_{t=0} > 0. \tag{30}$$

That is, the spread rate of worms must be greater than zero. From (22), the following condition must be satisfied.

$$\frac{r^2}{q^2}\alpha_1 kS(0)I(0) + \alpha_7 I'(0) - \alpha_3 I(0) - \alpha_4 I(0) - \alpha_8 I(0) > 0. \tag{31}$$

From (31) and the assumptions of Section 3.1: $I(0) > 0$ and $I'(0) = 0$, the following condition is derived.

$$S(0) > \frac{(\alpha_3 + \alpha_4 + \alpha_8)q^2}{\alpha_1 kr^2}. \tag{32}$$

Therefore, Theorem 1 is correct. □

We represents the right of (32) by λ as follows.

$$\lambda = \frac{(\alpha_3 + \alpha_4 + \alpha_8)q^2}{\alpha_1 kr^2}. \tag{33}$$

Theorem 1 implies when the number of the initial susceptible working nodes is not greater than λ, k worms may not spread in the WSN. Hence, we consider λ as the threshold for k worms to spread in the WSN. In practical applications, we may set the values of $\alpha_7, \alpha_8, \alpha_9, \alpha_{10}, \alpha_{11}$ and α_{12} to 0 in order to prohibit using the sleep and work interleaving schedule policy for nodes. At that time, the EiSIRS model proposed in this paper becomes the iSIRS model. Therefore, the iSIRS model is a special case of the EiSIRS model.

4 Simulation results and analysis

Our simulations focus on how the parameters q, r and k affect the number of infectious working nodes in a WSN. Based on the proposed model, we conduct the simulations with the assistance of Vinsim 5.0, which can effectively simulate non-linear dynamic feedback differential systems. For simplicity, we set the probabilities α_1, α_2, α_3, α_4, α_5, α_6 and α_7 to 0.1, 0.0008, 0.005, 0.21, 0.4, 0.008, 0.009, and set the probabilities α_8, α_9, α_{10}, α_{11} and α_{12} to 0.006, respectively. Let $R(0)$, $D(0)$, $I'(0)$, $S'(0)$ and R'(0) be 0, and let $S(0)$, $I(0)$, q, r and k be 10000, 1, 600, 20 and 6, respectively.

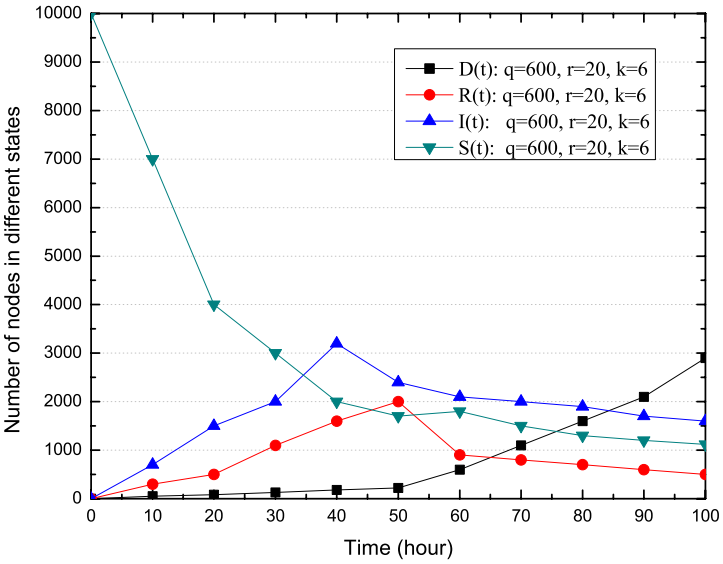

Fig. 2 The curves that the number of nodes in infectious, susceptible or recovered working state and dead state changes with time

In practice, we can apply random functions to define these probabilities, so that the randomization of state transition of nodes in a WSN can be well described.

The trends that the number of nodes in different working states changes with time are shown in Fig. 2. Here, the x-axis represents the progression of time, and the y-axis represents the number of nodes in different states. As Fig. 2 shows, the number of infectious working nodes rapidly increases at the initial spreading phase of worm propagation in a WSN then quickly decreases, and then changes at a relatively stable level. From Fig. 2, it is also noticed that the number of dead nodes slowly increases, and finally changes at a stable level. In contrast, the number of susceptible working nodes quickly decreases, then changes at a relatively stable level. These dynamic characteristics of worm propagation in a WSN are very similar to ones of worm propagation on the Internet. This similarity may be explained as follows. The initial number of susceptible working nodes is relatively large, which results in a fast increase of infectious working nodes. When the total number of nodes in a WSN does not change, the fast increase of infectious working nodes must lead to a fast decrease of susceptible working nodes. In addition, for a recovered working node, when a new worm starts to propagate in a WSN, the node may become a susceptible working node, then the node might be infected by the new worm. However, most of models of worm propagation in the literature do not support this case. On the other hand, due to the energy consumption of nodes, the number of dead nodes rises and finally becomes the initial number of nodes in a WSN. As a result, the number of nodes in other states finally becomes zero. This dynamic phenomenon is unique to the process of worm propagation in a WSN.

The trends that the number of nodes in different sleeping states changes with time are shown in Fig. 3. Figure 3 reveals that the number of nodes in different sleeping

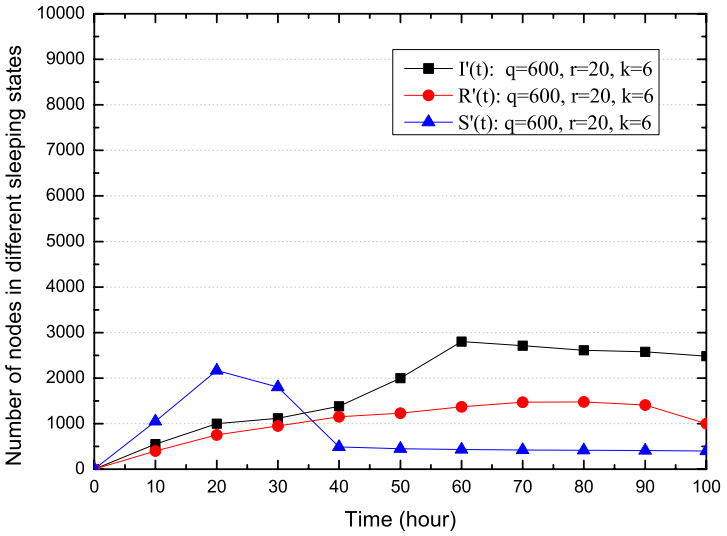

Fig. 3 The curves that the number of nodes in different sleeping states changes with time

states quickly increases for a relatively short period of time. After reaching the maximal value, the number of nodes in different sleeping states rapidly decreases for a relatively short period of time then slowly reduces and finally becomes zero. This dynamic characteristic is also unique to the process of worm propagation in a WSN, and the main reasons are that each node has a limited energy and nodes are scheduled by the sleep and work interleaving schedule policy. Note that the number of nodes in different sleeping states is related to the parameters α_{1-12} and the number of nodes in different working states. The parameters α_{1-12} and the number of nodes in different working states are related to the sleep and work interleaving schedule policy used in a certain practical application. Hence the process of worm propagation in a large scale WSN becomes very complex.

To observe how the threshold λ affects the number of nodes in I, when $\alpha_1 = 0.1, \alpha_3 = 0.005, \alpha_4 = 0.21, \alpha_8 = 0.006, q = 600, r = 20$, and $k = 6$, we calculate a threshold $\lambda = 714$ by (33). Let $S(0)$ be 714, 760 and 800, respectively. The simulation results are shown in Fig. 4. From Fig. 4 it is noted when the number of initial susceptible working nodes is equal to the threshold of worm propagation in a specific WSN, that is, $S(0) = 714$, k worms may not spread in the WSN. When the number of initial susceptible working nodes is greater than the threshold of worm propagation, k worms may spread in the WSN. Moreover, the larger the value of $S(0)$ is, the faster the k worms spread, as shown in the cases $S(0) = 760$, and $S(0) = 800$. The results are consistent with Theorem 1.

To observe how the parameters q, r and k influence the number of nodes in I, we conduct three groups of simulations. In each group, we conduct the simulation three times by different values of q, r and k.

Case 1 Let $q = 600$ and $k = 6$. Keep q and k as a constant, respectively. Further, assign 14, 17 and 20 to r, respectively. The simulations are conducted by different

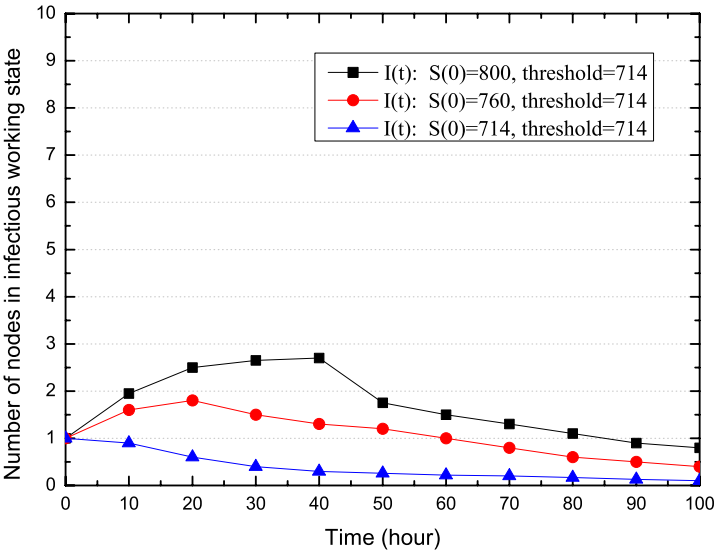

Fig. 4 The curves that the number of nodes in infectious working state changes with time when the spreading threshold $\lambda = 714$

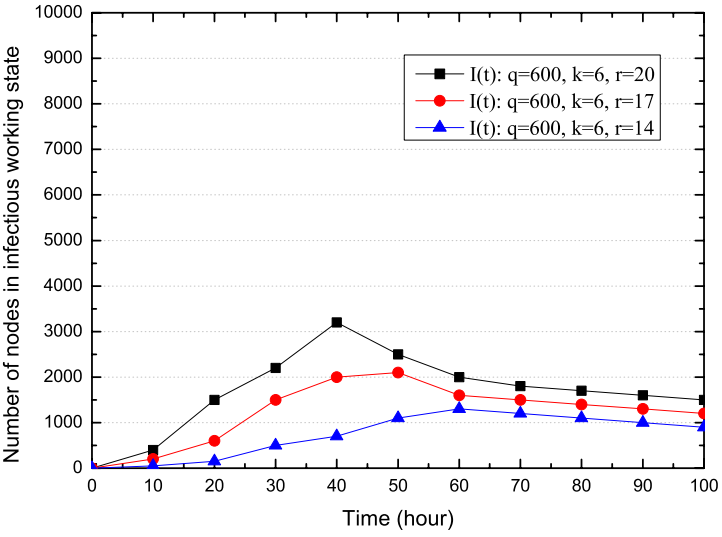

Fig. 5 The curves that the number of nodes in infectious working state changes with time when the communication radius of nodes is different

values of r and the results are shown in Fig. 5. Figure 5 shows that the larger the communication radius of nodes is, the earlier the spreading beginning time of worms in the WSN is. Figure 5 also shows that the value of r affects the maximal number of infectious working nodes. That is, the bigger the value of r is, the larger the maximal

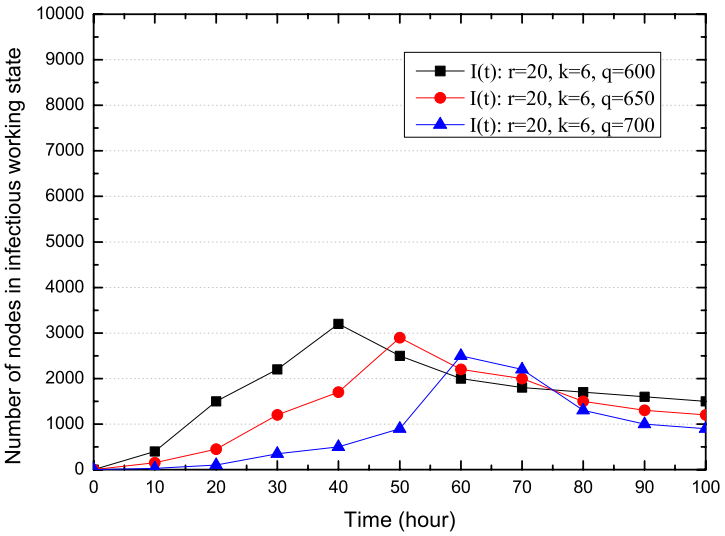

Fig. 6 The curves that the number of nodes in infectious working state changes with time when the communication radius of the WSN is different

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

Case 2 Let $r = 20$ and $k = 6$. Keep r and k as a constant, respectively. Further, assign 600, 650 and 700 to q, respectively. The simulations are conducted by different values of q, and the results are shown in Fig. 6. Figure 6 shows that the smaller the communication radius of a WSN is, the earlier the spreading beginning time of worms in the WSN is, and the faster the k worms spread. Figure 6 also shows that the value of q affects the maximal number of infectious working nodes. That is, the bigger the value of q is, the smaller the maximal number of infectious working nodes is. The reason is that a bigger value of q decreases the density of nodes in the WSN, further decreases the number of susceptible working nodes in the communication ranges of infectious working nodes. As a result, there may not be more susceptible working nodes to be infected by worms residing in infectious working nodes.

Case 3 Let $q = 600$ and $r = 20$. Keep q and r as a constant, respectively. Further, assign 4, 5 and 6 to k, respectively. The simulations are conducted by different values of k and the results are shown in Fig. 7. Figure 7 shows that the bigger the value of k is, the earlier the spreading beginning time of worms in a WSN is, and the faster the k worms spread in the WSN. Figure 7 also shows that the value of k affects the maximal number of infectious working nodes. That is, the bigger the value of k is, the larger the maximal number of infectious working nodes is. It is because a bigger value of k enhances the possibility with which an infectious working node spread more worms to more susceptible working neighbors of this infectious working node in a unit time.

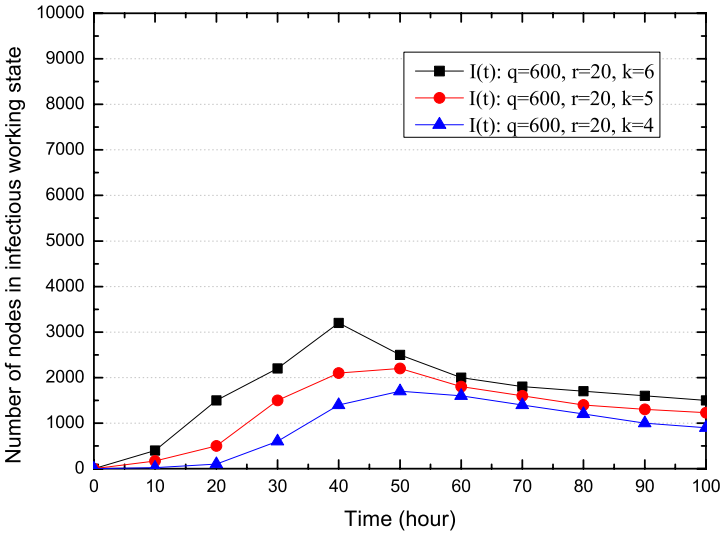

Fig. 7 The curves that the number of nodes in infectious working state changes with time when the average number of worms residing in a node is different

As a result, there may be more susceptible working nodes to be infected by worms residing in infectious working nodes.

From the above simulation results, we believe that the dynamic characteristics of worm propagation is related to the network topology, the energy consumption of nodes and the sleep and work interleaving schedule policy used in large scale WSNs. This provides new insights for the dynamics of worm propagation in WSNs, especially large scale WSNs.

5 Conclusion

In this paper, we propose a novel formal model to analyze the dynamics of worm propagation in WSNs. The proposed model is called EiSIRS model. The EiSIRS model is based on the epidemic theory and it consists of differential equations. According to the proposed model, a necessary condition for worms to spread in a large scale WSN is theoretically derived. In addition, the proposed model supports the sleep and work interleaving schedule policy used in a large scale WSN, and it also takes into account the multi-worm propagation issue. Simulation results are provided to demonstrate the validity of the proposed model. Based on the proposed model, how to automatically adjust the communication range of nodes to control the process of worm propagation will be an interesting direction.

References

Chen ZS, Gao LX, Kwiat K (2003) Modeling the spread of active worms. In: Proceedings of IEEE INFOCOM, pp 1890–1900

Dantu R, Cangussu JW, Patwardhan S (2007) Fast worm containment using feedback control. IEEE Trans Dependable Secure Comput 4(2):119–136

Eugster PT, Guerraoui R, Kermarrec AM, Massoulie L (2004) Epidemic information dissemination in distributed systems. Mathematical modeling in epidemiology. IEEE Comput 37(5):60–67

Frauenthal JC (1981) Mathematical modeling in epidemiology. Springer, New York. ISBN-10:0387103287

Kephart OJ, White RS (1991) Directed-graph epidemiological models of computer viruses. In: Proceedings of IEEE symposium on security and privacy, pp 22–35

Kim J, Radhakrishnan S, Dhall SK (2004) Measurement and analysis of worm propagation on Internet network topology. In: Proceedings of IEEE international conference on computer communications and networks, pp 495–500

Moore D, Paxson V, Savage S, Shannon C, Stanoford S, Weaver N (2003) Inside the slammer worm. IEEE Secur Priv 1(4):33–39

Okamura H, Kobayashi H, Dohi T (2005) Markovian modeling and analysis of Internet worm propagation. In: Proceedings of the 16th IEEE international symposium on soft reliability engineering, pp 149–158

Onwubiko C, Lenaghan AP, Hebbes L (2005) An improved worm mitigation model for evaluating the spread of aggressive network worms. In: Proceedings of IEEE international conference on computer as tool, pp 1710–1713

Pradip D, Liu Y, Sajalk D (2007) Modeling node comprise spread in wireless sensor networks using epidemic theory. In: Proceedings of IEEE international symposium on a world of wireless, mobile and multimedia networks, pp 237–243

Syed KA, Hayder R (2006) Using signal processing techniques to model worm propagation over wireless sensor networks. IEEE Signal Process Mag 23(2):164–169

Wang X, Li Y (2008) A improved SIR model for worm propagation in wireless sensor networks. Chin J Electron 18(1):28–32

Yang F, Duan HX, Li X (2005) Modeling and analyzing of the interaction between worms and antiworms during network worm propagation. Sci China Ser E Inf Sci 34(8):841–856

Zou CC, Gong G, Towsley D (2005) The monitoring and early warning for Internet worms. IEEE Trans Netw 13(6):961–974

Zou CC, Towsley D, Gong W (2007) Modeling and simulation study of the propagation and defense of Internet e-mail worms. IEEE Trans Dependable Secure Comput 4(2):105–118