Virus spreading in wireless sensor networks with a medium access control mechanism*

Wang Ya-Qi(王亚奇)† and Yang Xiao-Yuan(杨晓元)

Network and Information Security Key Laboratory of Armed Police Force, Department of Electronics Technology, Engineering University of the Chinese People's Armed Police Force, Xi'an 710086, China

(Received 1 August 2012; revised manuscript received 12 September 2012)

In this paper, an extended version of standard susceptible-infected (SI) model is proposed to consider the influence of a medium access control mechanism on virus spreading in wireless sensor networks. Theoretical analysis shows that the medium access control mechanism obviously reduces the density of infected nodes in the networks, which has been ignored in previous studies. It is also found that by increasing the network node density or node communication radius greatly increases the number of infected nodes. The theoretical results are confirmed by numerical simulations.

Keywords: wireless sensor networks, medium access control, virus spreading, susceptible-infected model

PACS: 02.50.Le, 05.65.+b, 05.70.Np **DOI:** 10.1088/1674-1056/22/4/040206

1. Introduction

In recent years, wireless sensor networks (WSNs) have received a great deal of attention because of their enormous potential applications in civil and military fields.[1] A typical WSN consists of massive sensor nodes working unattendedly and transmitting their collected data to the sink node connected to the Internet.[2] The sensor nodes are generally deployed in inaccessible and hostile environments, and both their power communication capabilities are limited. When the sensor nodes are far away from the sink node, they must transmit their collected data through the intermediate nodes to the sink node, owing to the limited communication range, i.e., the source nodes first send their data to their neighboring nodes, which in turn transmit the data to their respective neighbors. Moreover, the restrained resource often leads to weak defense capabilities of sensor nodes, and thus the sensor nodes are easily attacked by viruses, especially when they are deployed in hostile environments.[3] Therefore, the research of security mechanisms for the WSN has important practical significance.[4]

Using the spreading theory of epidemics to investigate the dynamics of virus spreading in WSN has been widely concerned.[5–7] Motivated by the surfacing viruses that can spread over the air interfaces, De *et al*.[8] used epidemic theory to investigate the potentially devastating threat of node compromise spreading in the WSN, and found that the uniform random deployment was more vulnerable to virus outbreak. Moreover, they presented a susceptible-infected-removed (SIR) model to analyze the propagation rate and the extent of spread of viruses in the WSN over several typical broadcast protocols. The analysis showed that the number of source nodes had a significant influence on the subsequent rate of spread of viruses.[9] Shon and Park[10] presented a novel energy-efficient security architecture to resolve the trade-off issue between security and energy in the WSN, and verified the approach through performance analysis. Nicholas *et al*.[11] proposed a framework to derive the epidemic threshold for any mobility model under the SIS propagation model. Anagnostopoulos *et al*.[12] extended the spreading model SIS to SI^KS, studied the dynamics of multi-epidemical spreading in WSN, and found the relationship among the epidemical thresholds of the transmuted epidemics. Tang[13] gave a modified SI epidemic model to improve the anti-virus capability and flexibly adapt to different viruses of the WSN. Zhang *et al*.[14] introduced an immunization method to enhance the network robustness against viruses. We[15] established a new WSN topology and discussed the virus propagation in it. However, most of the existing studies have not studied the effect of the medium access control (MAC) mechanism on the behavior of virus spreading.

The MAC mechanism is necessary to ensure the normal communication of the WSN, because it can effectively prevent the interference between different speaking nodes using the same channel at the same time.[16–18] When a speaking node is busy, all the other nodes inside its communication range (called the node neighbors) must keep silent. Before sending a package, a node should first check in its transmission range whether any of its neighbors are busy. If a neighbor of the node is speaking, the transmission cannot begin. Thereby, it can be inferred in the way that the MAC mechanism inter-

*Project supported by the National Natural Science Foundation of China (Grant Nos. 61103231 and 61103230), the Natural Science Foundation of Jiangsu Province, China (Grant No. BK2012082), the Innovation Program of Graduate Scientific Research in Institution of Higher Education of Jiangsu Province, China (Grant No. CXZZ11_0401), the Natural Science Basic Research Plan in Shaanxi Province of China (Grant No. 2011JM8012), and the Basic Research Foundation of Engineering University of the Chinese People's Armed Police Force (Grant No. WJY201218).

†Corresponding author. E-mail: wjwangyq@126.com

© 2013 Chinese Physical Society and IOP Publishing Ltd

weaves with the node contradiction will affect the spreading dynamics of viruses in the WSN.

Considering the influence of the MAC mechanism,[19,20] we propose a novel SI model to further study virus spreading in the WSN. In this paper, we assume that the sensor nodes each have a maximum transmission radius r_c (the width of the circular strip), and $r(t)$ is the radius of viruses spreading in the WSN at time t (the radius of the outer circle) as shown in Fig. 1. When a sensor node is attacked by viruses, the viruses will propagate together with the normal data to its neighbors. As the spreading process of viruses continues, finally all the nodes of the WSN without any anti-virus mechanism will be compromised. Since the limitation of communication range, the infected nodes inside the inner circle of Fig. 1 cannot spread viruses to susceptible nodes on the outside, i.e., these infected nodes are invalid. In order to exhibit the effect of the MAC mechanism, in our SI model not all the infected nodes inside the circular strip can spread viruses to their neighbors, i.e., some infective nodes will also work as invalid sources. The research shows that the density of the infected nodes with a MAC mechanism is obviously lower than that without it in the networks. Moreover, the increase of the network node density or the node communication radius will greatly increase the number of infected nodes. However, the network size weakens the virus spreading in the WSN.

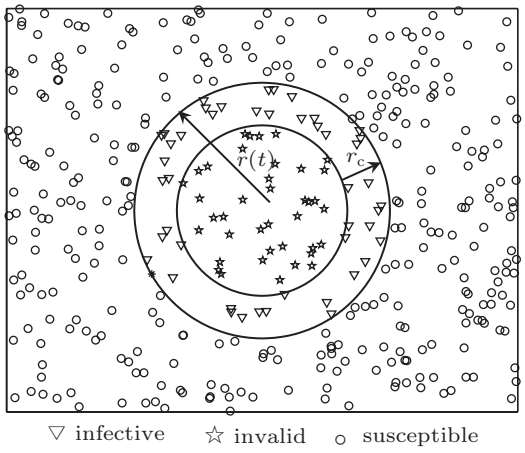


Fig. 1. Spreading phenomenon of viruses in the WSN.

The rest of this paper is organized as follows. In Section 2, a novel SI spreading model with a MAC mechanism is proposed. In Section 3 the theoretical analysis of propagation behaviors of our SI model is presented. Then in Section 4, numerical simulations are given to confirm the predictions achieved in Section 3. Finally, in Section 5 we draw some conclusions from the present study.

2. Novel SI model

In this section, in order to investigate the dynamic behavior of viruses in the WSN with a MAC mechanism, we propose a novel SI model, which is different from the model in the previous related work. The new SI spreading model is defined as follows: each node in the WSN has two different discrete states: susceptible and infected. The susceptible denotes that the nodes are free of viruses but can be infected. Infected means that the nodes carry viruses and can pass the viruses to other susceptible nodes.[21] At the initial moment, we randomly select a node as the infected node. Suppose that the nodes in the WSN are uniformly randomly distributed with density σ, the size of WSN N is constant without considering the node deletion caused by node failure, $S(t)$ and $I(t)$ are the numbers of susceptible and infected nodes at time t, respectively, then we have $N = S(t) + I(t)$.

In our SI model, due to considering the effect of the MAC mechanism, when an infected node gets a chance to transmit a packet by channel contention, all the other infected neighbors inside its transmitting radius r_c cannot speak out at the same moment. The detailed transmission process of viruses is described as follows: at each time step t, when the infected nodes communicate with their susceptible neighbors, these neighbors will be infected with infection probability λ. Here, the probability λ depends not only on the infectivity of the viruses, but also on the communication range of the nodes.[17] According to our SI model, the number of infected nodes will gradually increase with time (t). However, because not all the infected nodes are able to infect other susceptible nodes in the whole spreading process of viruses, the change rate of infected nodes is not directly determined by the total number of infected nodes.

3. Analysis of the SI model

Let $s(t)$ and $i(t)$ denote the densities of the infected and susceptible nodes at time t, respectively. Obviously, the two variables satisfy $s(t) = S(t)/N$ and $i(t) = I(t)/N$. In our SI model, since not all the infected nodes can spread viruses, we denote the number of infected nodes that work as valid sources at time t, with $I_e(t)$, and represent the density with $i_e(t)$ that satisfies $i_e(t) = I_e(t)/N$. For the case of node uniform random deployment, each node can contact the order of $\sigma\pi r_c^2$ neighbors. Using the mean-field theory,[22] the reaction equations of $s(t)$ and $i(t)$ with time t are respectively given by

$$\frac{\mathrm{d}i(t)}{\mathrm{d}t} = \lambda\sigma\pi r_c^2 i_e(t)s(t), \tag{1}$$

$$\frac{\mathrm{d}s(t)}{\mathrm{d}t} = -\lambda\sigma\pi r_c^2 i_e(t)s(t). \tag{2}$$

From Fig. 1, we know that the infected nodes inside the internal circle do not have the ability to spread viruses to the outside susceptible nodes. Only those that are in the circular strip area are able to infect other susceptible nodes. Combining the MAC mechanism,[13,17] the number of infected nodes

working as valid sources $I_e(t)$ at time t can be calculated as

$$I_e(t) = \frac{\sigma\pi r(t)^2 - \sigma\pi[r(t)-r_c]^2}{\sigma\pi r_c^2} = \frac{2r(t)}{r_c} - 1, \quad (3)$$

when $r(t) \gg r_c$, we have

$$I_e(t) \approx 2r(t)/r_c, \quad (4)$$

meanwhile, we can easily obtain

$$\sigma\pi r(t)^2 = I(t). \quad (5)$$

Substituting Eq. (5) into Eq. (4), we derive

$$I_e(t) = \frac{2\sqrt{I(t)}}{r_c\sqrt{\sigma\pi}}, \quad (6)$$

then we have

$$i_e(t) = \frac{2\sqrt{i(t)}}{r_c\sqrt{\sigma\pi N}}. \quad (7)$$

Combining Eq. (1) and Eq. (7), one can obtain

$$\frac{di(t)}{dt} = \lambda\sigma\pi r_c^2 \frac{2\sqrt{i(t)}}{r_c\sqrt{\sigma\pi N}}[1-i(t)] = \frac{2\lambda r_c\sqrt{\sigma\pi}}{\sqrt{N}}\sqrt{i(t)}[1-i(t)]. \quad (8)$$

By applying the initial condition $i(t=0) = i_0 = 1/N$,[23] we solve $i(t)$ as

$$i(t) = \left(1 - \frac{2(\sqrt{N}-1)}{(\sqrt{N}+1)\exp\left(\frac{2\lambda r_c\sqrt{\sigma\pi}}{\sqrt{N}}t\right) + (\sqrt{N}-1)}\right)^2. \quad (9)$$

Equation (9) shows that in the proposed SI model, for a given network size N, the density of infected nodes is related to the node communication radius r_c, node density σ, and infection probability λ. When $t \to \infty$, then $i(t) \to 1$, which reveals that once a node in the WSN is attacked by viruses, all the nodes will be eventually infected. From this, we can reduce the virus spreading in the networks by properly reducing the node density.

From Eq. (9), we can obtain

$$i'(t) \sim e^{-Ct}, \quad (10)$$

where the constant $C = 2\lambda r_c\sqrt{\sigma\pi}/\sqrt{N}$ and $i'(t) = 1 - \sqrt{i(t)}$.

4. Numerical simulations

In this section, in order to compare with the above analytical predictions, numerical experiments on the proposed SI model are performed. Assume that the nodes in the WSN follow uniform random distribution. In the simulation process, the parameters are chosen as follows: the size of network $N = 2000$, 3000, 4000, the communication radius $r_c = 0.7$, 1, 1.2, 1.4, the node density $\sigma = 1$, 2, 4 and the infection probability $\lambda = 0.1$, 0.3, 0.5, respectively. All the chosen parameters are dimensionless. The dynamic process starts with randomly selecting a node as the infected node, and all the following simulation results are obtained by averaging at least 20 independent runs of the network model.

Figure 2 shows the corresponding relationship between the density of infected nodes $i(t)$ and time t with the MAC mechanism, where $\lambda = 0.1$ and $N = 2000$. From Fig. 2, we can observe that when different values of σ and r_c are selected, the results of the numerical simulation are basically consistent with the theoretical analysis from Eq. (9), which proves the correctness of the theoretical analysis. It is also noted that due to taking a reasonable approximation in the process of theoretical analysis, the results obtained from the theoretical analysis are a little larger than the numerical simulations. Figure 3 exhibits the change of $i'(t)$ with the time t for different values of C with the MAC mechanism. As shown in Fig. 3, all the plots decay exponentially, $i'(t) \sim \exp(-Ct)$, which are also in better agreement with the theoretical predictions from Eq. (10).

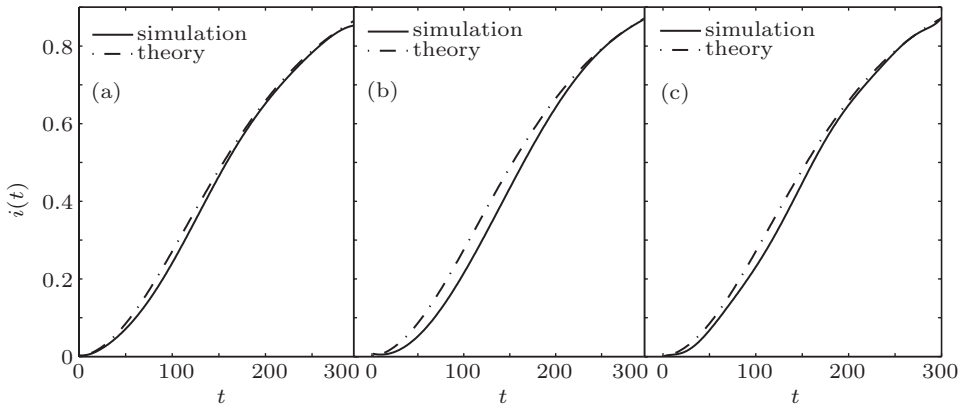


Fig. 2. Plots of density of infected nodes $i(t)$ versus the time t with the MAC mechanism: (a) $\sigma = 1$, $r_c = 1.4$; (b) $\sigma = 2$, $r_c = 1$; (c) $\sigma = 4$, $r_c = 0.7$.

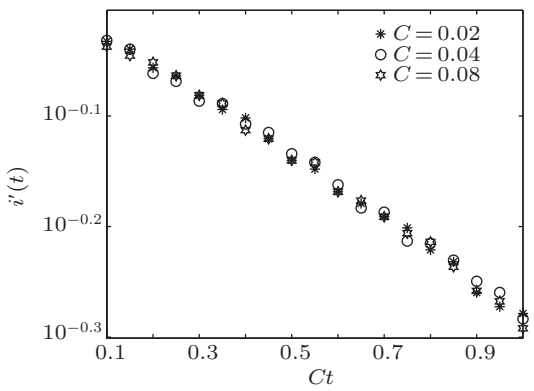


Fig. 3. Plots of $i'(t)$ versus Ct for different values of C with the MAC mechanism.

Figure 4 represents the variations of density of the infected nodes $i(t)$ with time t for different values of communication radius r_c, with and without the MAC mechanism, respectively, where $\lambda = 0.1$, $\sigma = 1$, and $N = 2000$. From Fig. 4, we can observe that the communication radius affects the virus spreading in the WSN for both those with and without a MAC mechanism. Given the communication radius r_c, $i(t)$ with the MAC mechanism is obviously less than that without it in the WSN, which implies that the MAC mechanism can effectively inhibit the transmission of viruses. Figure 4 also shows that $i(t)$ increases with communication radius r_c increasing, for which the reason is that the infected nodes with large r_c can infect more susceptible nodes at the same time.

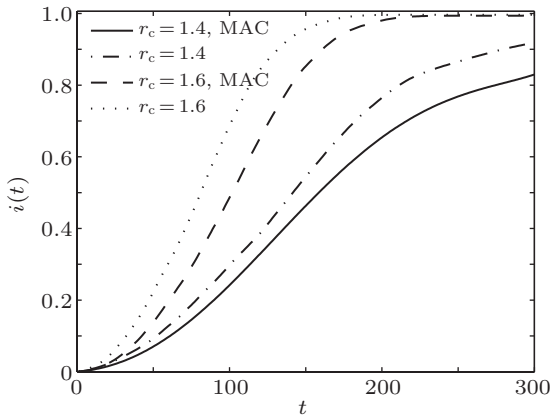


Fig. 4. Curves of $i(t)$ versus time t for different values of r_c with and without MAC mechanism, respectively.

Figure 5 depicts the evolution relationship between the density of infected nodes $i(t)$ and time t for different values of σ, with and without a MAC mechanism, respectively, where $\lambda = 0.1$, $r_c = 1.2$, and $N = 2000$. From Fig. 5, we find that for the same value of σ, the existence of the MAC mechanism reduces the number of infected nodes. Moreover, increasing σ can greatly accelerate the virus spreading in the networks. This is because inside the communication range r_c of an infected node, the larger the value of σ, the more susceptible nodes can be infected.

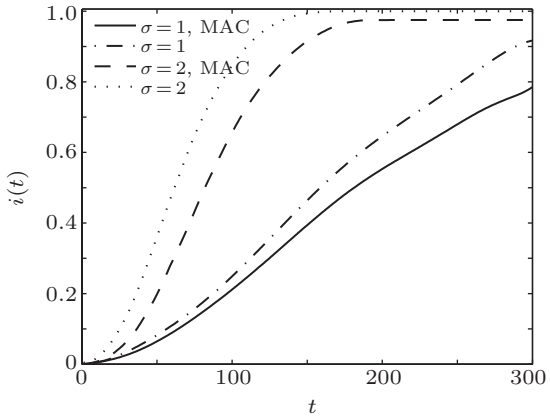


Fig. 5. Curves of $i(t)$ versus time t for different values of σ with and without a MAC mechanism, respectively.

Figure 6 exhibits the changes of the density of infected nodes $i(t)$ with time t for different values of λ with a MAC mechanism, where $\sigma = 1$, $r_c = 1.4$, and $N = 2000$. As shown in Fig. 6, the density of infected nodes $i(t)$ obviously increases as λ increases, which is mainly because the large λ raises the probability that the susceptible nodes are infected, thus accelerating the network virus spreading. As a result, more and more nodes in the networks are infected.

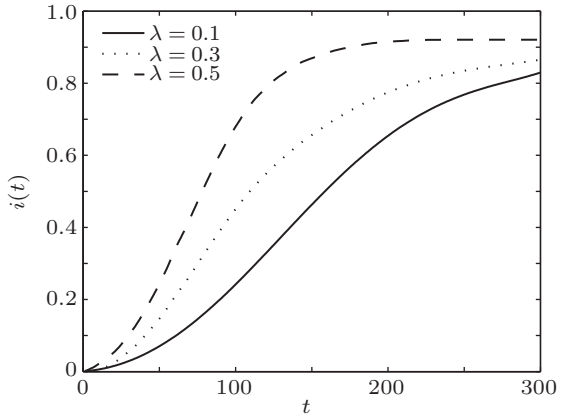


Fig. 6. Plots of density of infected nodes $i(t)$ versus time t for different values of λ with a MAC mechanism.

Figure 7 illustrates the dependence of density of infected nodes $i(t)$ on time t for different values of N with MAC mechanism, where $\sigma = 1$, $r_c = 1.4$, and $\lambda = 0.1$. As shown in Fig. 7, $i(t)$ decreases as network size increases. From this it follows that there obviously exists a finite-size effect in our SI model, which is consistent with that of the SI model without a MAC mechanism and strongly supports the above theoretical analysis. Furthermore, we can draw a conclusion that in order to reduce the spreading velocity of viruses in WSN, a larger N should be chosen, which is exactly contrary to the conclusions obtained by the previous studies on the transmission behaviors of viruses in WSN.

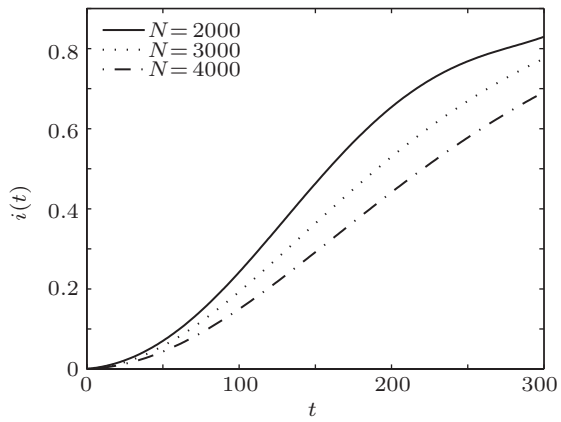


Fig. 7. Curves of density of infected nodes $i(t)$ as a function of time t for different values of N with the MAC mechanism.

5. Conclusions

Considering the influence of the MAC mechanism, in this paper we propose a new SI model to study the spreading behavior of viruses in the WSN by using the transmission dynamics of epidemics. The characteristic feature of our SI model is that in the process of virus spreading, when an infected node is transmitting a packet, all the other infected nodes inside its transmission range must keep silent. Firstly, it is found that the MAC mechanism can obviously reduce the number of infected nodes in the networks, which has been ignored in previous studies. Secondly, we also find that the increase of the network node density or node communication radius will apparently increase the density of infected nodes. Finally, we can effectively inhibit virus propagation by increasing the network size. In order to improve the security features of the WSN, it is necessary to use the epidemic propagation theory to deeply investigate the virus spreading dynamics in the WSN. In this paper only the effect of the MAC mechanism is considered, however, there are various communication protocols in the WSN. Combining multiple protocols to discuss the spread of network viruses is the problem that should be studied in the future.

References

[1] Yang Z, Meratnia N and Havinga P 2010 *IEEE Commun. Surv. Tut.* **12** 159
[2] Buratti C, Conti A, Dardari D and Verdonen R 2009 *Sensors* **9** 6869
[3] Madan R 2006 *IEEE T. Wirel. Commun.* **5** 748
[4] Sun B, Yan G H, Xiao Y and Yang T A 2009 *Ad Hoc Netw.* **7** 1489
[5] Dong J, Curtmola R and Nita-Rotaru C 2009 *Comput. Commun.* **32** 1790
[6] Mills K L 2007 *Wirel. Commun. Mob. Com.* **7** 823
[7] Dong J, Curtmola R and Nita-Rotaru C 2011 *IEEE T. Mobile Comput.* **10** 653
[8] De P, Liu Y H and Das S K 2009 *IEEE T. Sensor Network* **5** 1
[9] De P, Liu Y H and Das S K 2009 *IEEE T. Mobile Comput.* **8** 413
[10] Shon T and Park Y 2009 *Ksii T. Internet Inf.* **3** 597
[11] Nicholas C, Aditya Prakash B, Tong H H and Faloutsos M 2011 *Lect. Notes Comput. Sci.* **6640** 266
[12] Anagnostopoulos C, Hadjiefthymiades S and Zervas E 2011 *J. Parallel Distr. Com.* **71** 87
[13] Tang S S 2011 *International Journal of Wirel.* **18** 319
[14] Zhang S K, Gong S R, Cui Z M and Liu Q 2009 *Journal of Networks* **4** 170
[15] Wang Y Q and Yang X Y 2012 *Acta Phys. Sin.* **61** 090202 (in Chinese)
[16] Nekovee M 2007 *New J. Phys.* **9** 189
[17] Zhu C P, Wang L, Liu X Y and Yan Z J 2012 *Chin. Phys. Lett.* **29** 010504
[18] Saxena N, Roy A and Shin J 2008 *Comput. Netw.* **52** 2532
[19] Zhang H F, Small M, Fu X C and Wang B H 2009 *Chin. Phys. B* **18** 3639
[20] Barthélemy M, Barrat A, Pastor-Satorras R and Vespignani A 2004 *Phys. Rev. Lett.* **92** 178701
[21] Gong Y W, Song Y R and Jiang G P 2012 *Chin. Phys. B* **21** 010205
[22] Pastor-Satorras R and Vespignani A 2001 *Phys. Rev. Lett.* **86** 3200
[23] Roshani F and Naimi Y 2012 *Phys. Rev. E* **85** 036109