Virus Propagation Model for Wireless Sensor Networks Based on IPv6

https://doi.org/10.3991/ijoe.v14i10.9309

Zhinan Zhou(✉), Wendi Wang
Modern Education and Technology Centre, Hebei Agricultural University, Baoding, China
zhinanzh@hebau.edu.cn

Yuxia Li
Jiangsu Maritime Technical Institute, Nanjing, China

Abstract—This paper aims to disclose the features of virus propagation in wireless sensor networks (WSNs). To this end, the author analysed the data transmission mode of WSNs which follow IPv6 protocol. Then, the virus propagation in such networks was simulated and discussed under different scenarios. Based on the simulation results and the traditional virus propagation model, a new model was put forward to describe the virus transmission in IPv6 WSNs. The proposed model lays a theoretical basis for relevant studies and the guarantee of WSN security.

Keywords—wireless sensor networks (WSNs), virus propagation model, IPv6, information security

1 Introduction

With the dawn of the big data era, wireless sensor networks (WSNs) have evolved from independent closed networks for data collection, processing and utilization to a stub network that provide the collected data to the other data communication networks (DCNs). In the latest WSNs, each sensor node serves as a data collector and command execution, while the remote high-performance computers or even supercomputer is responsible for analysis and processing of advanced and complicated data. In this way, the sensed data can be fully exploited at a low energy consumption.

As shown in Figure 1, WSNs are usually connected with other DCNs via gateways, forming heterogeneous WSNs. By this connection method, all communication traffics between WSNs and DCNs are converted through the gateway. Despite solving the lack of IP address space, this approach may increase the chance of single-point failure and threaten the network reliability. What is worse, the gateway connection only supports uplink data propagation, failing to accurately control WSN nodes by upstream terminals. In this case, it is impossible to implement applications with bidirectional data propagation requirements on WSNs.

The emergence of IPv6 WSNs has offered a good solution to the above problems. This type of WSNs not only provide a massive amount of address resources, but also

facilitate the inter-network connection of heterogeneous WSNs [1]. IPv6 WSNs can be connected with other DCNs without the gateway. The communication traffics are no longer converted at the gateway. Instead, the sensor nodes can achieve direct communication with other DCNs. In general, IPv6 WSNs suppress the chance of single-point failure, enhance the network reliability, and enable the terminals of other DCNs to accurately control one or a group of sensor nodes.

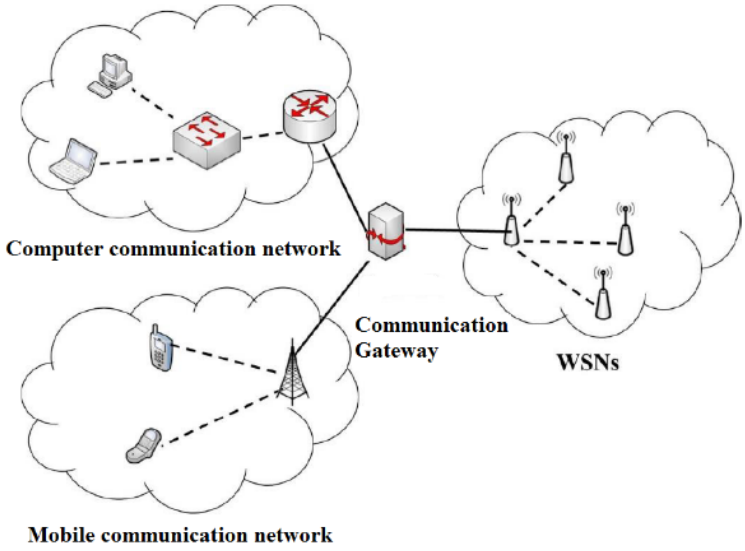


Fig. 1. Gateway connection between WSNs and DCNs

The proliferation of IPv6 WSNs, great changes have taken place in the data propagation behaviour in WSNs, raising new concerns about WSN informaiton security. The introduction of IPv6 to WSNs eliminates broadcast traffic and optimizes network bandwidth. However, the multicast and broadcast features of IPv6 may alter the original data propagation mode of WSNs, and also the features of virus propagation and network attack. To ensure the data security, it is necessary to explore the data propagation features of IPv6 WSNs.

2 Propagation Dynamics Model of Complex Networks

The research into complex networks mainly aims to determine the physical and logical topology, understand the stability and functional features, and ascertain the relationship between network topology and dynamic propagation of data. Among the diverse studies on propagation dynamics in complex networks, the spread of biological viruses remains as the focal point of the research. Over the years, virus propagation models with different dynamic features have been created for biological viruses like malaria, influenza and SARS[2-4].

Considering the lack of empirical data, the virus communication in DCNs is often examined based on the existing propagation models of biological viruses. The current models are coupled with different environments to form new virus propagation models. The typical biological virus propagation models include: susceptible infectious (SI) model [5], susceptible infectious susceptible (SIS) model [6], susceptible infectious recovered (SIR) model [7], worm-anti-worm model [8], etc.

In these models, the different individuals in the population are abstracted to a number of individual states according to their respective states. There are usually three states: susceptible (S), infected (I) and recovered (R). The S state, also known as the healthy state, means that the individual is not immune to the virus; the I state means that the individual has been infected by the virus, which is capable of infecting the healthy node; the R state means that the original infected virus has been cleared, and the individual is now healthy and immune to the virus.

2.1 SI model

The SI model is the simplest virus propagation model. In this model, there are only two states for each individual: S and I. When a susceptible individual is infected by the virus, it turns into and remains in the infected state. The schematic diagram of the model is shown in Figure 2.

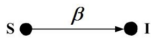


Fig. 2. The SI model

The differential equation of the model can be expressed as:

$$\begin{cases} \frac{dS(t)}{dt} = -\beta I(t)S(t) \\ \frac{dI(t)}{dt} = \beta I(t)S(t) \end{cases} \tag{1}$$

To sum up, the SI model satisfies the following definitions:

(1) There are only two individual states: S and I.

(2) S(t) and I(t) are respectively the number of susceptible individuals and the number of infected individuals in the network at time t.

(3) When a susceptible individual comes into contact with an infected individual, the susceptible individual is infected with the virus carried by the infected individual at the probability of β. The probability β varies with the virus types and individuals.

2.2 SIS model

Similar to the SI model, the SIS model has only two states for each individual, namely, the susceptible state and the infected state. This model differs from the SI model in that, when a susceptible individual is infected, the virus it carries can be removed by scavenging means, turning it back to the susceptible state; then, the

individual can still be infected again by the same virus. The schematic diagram of the model is shown in Figure 3.

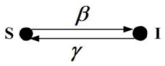


Fig. 3. The SIS model

The differential equation of the model can be expressed as:

$$\begin{cases} \frac{dS(t)}{dt} = -\beta I(t)S(t) + \gamma I(t) \\ \frac{dI(t)}{dt} = \beta I(t)S(t) - \gamma I(t) \end{cases} \tag{2}$$

To sum up, the SIS model satisfies the following definitions:

(1) There are only two individual states: S and I.

(2) S(t) and I(t) are respectively the number of susceptible individuals and the number of infected individuals in the network at time t.

(3) When a susceptible individual comes into contact with an infected individual, the susceptible individual is infected with the virus carried by the infected individual at the probability of β. The probability β varies with the virus types and individuals.

(4) By scavenging means, the infected individual can be restored into a susceptible individual at the probability of γ. The probability γ varies with the scavenging effect and virus types. After being restored to the susceptible state, the individual can still be infected again by the same virus at the probability of β.

2.3 SIR model

Unlike the former two models, the SIR model has three states for each individual. In this model, after the virus on the infected individual is cleared, the individual becomes immune to the virus, that is, it will not be infected again by the same virus in future. The schematic diagram of the model is shown in Figure 4.

Fig. 4. The SIR model

The differential equation of the model can be expressed as:

$$\begin{aligned} &\frac{dS(t)}{dt} = -\beta I(t)S(t) \\ &\frac{dI(t)}{dt} = \beta I(t)S(t) - \gamma I(t) \\ &\frac{dR(t)}{dt} = \gamma I(t) \end{aligned} \tag{3}$$

To sum up, the SIR model satisfies the following definitions:

1. There are there individual states: S, I and R.
2. $S(t)$, $I(t)$ and $R(t)$ are respectively the number of susceptible individuals, the number of infected individuals, and the number of individuals immune to the virus in the network at time t.
3. When a susceptible individual comes into contact with an infected individual, the susceptible individual is infected with the virus carried by the infected individual at the probability of β. The probability β varies with the virus types and individuals.
4. By scavenging means, the infected individual can be restored into a susceptible individual at the probability of γ. The probability γ varies with the scavenging effect and virus types. After being restored to the susceptible state, the individual becomes immune to the same virus.

3 Effects of IPv6 on Propagation Features of WSN Data

The WSNs serve as the perceptive layer in the overall architecture of the Internet of things. There are many nodes in each WSN, some of which have mobility. To ensure the validity of the sensed data, the data security must be protected at the WSN nodes.

The IPv6 WSNs come into being to fulfil the demand from sensor networks for address resources. The use of IPv6 protocol can provide WSNs with a massive IP address space. Compared with IPv4, IPv6 does not need to use IP address allocation servers like DHCP to implement IP address settings. Instead, the sensor nodes in IPv6 WSNs can quickly set a globally unique IP address using the EUI-64 mechanism inherent in IPv6. This unique identifier allows the terminals of other DCNs to send precise control signals directly to the sensing node. Moreover, the integrated IPSec feature in the IPv6 protocol enables encrypted propagation of the sensed data, and thus protect the confidentiality.

In the IPv6 protocol, IP addresses fall into three categories according to their functions: unicast address, multicast address and anycast address. Each category corresponds to a unique way of data propagation. Specifically, the unicast address identifies a single network interface for point-to-point communication, i.e., unicast communication. The multicast address identifies a group of network interfaces for point-to-multipoint communication, i.e., multicast communication. Note that multicast communication sends the data to a few nodes rather than flood the entire network as broadcast communication. In other words, multicast communication has a limited range of data propagation. The anycast address functions similarly as the multicast address. The only difference between the two lies in data propagation. In anycast communication, when the terminal sends data to an anycast address, only one optimal network interface can receive data. Anycast communication can achieve the optimal data propagation at the network layer.

The anycast data propagation method was first defined in RFC 1546 [9] published by the International Engineering Task Force (IETF) in 1993. This document describes the anycast data communication, and suggests assigning a separate address space like multicast, aiming to promote the use of anycast. Besides, RFC 1546 discusses the impact of anycast on transport layer protocol and proposes some modifications to the TCP

protocol. Nevertheless, these modifications are difficult to implement, owing to the extensive use of the TCP protocol. As a result, anycast communication is rarely used in the IPv4 era.

To embrace the new addressing architecture of IPv6, the IETF revised the design framework for anycast communication in 1998 and released a new definition of anycast protocol in RFC 2373 [10]: in anycast communication, when a source sends data to an anycast address, the data is only sent to a network node with the lowest metric from its routing protocol. An anycast address no longer uses a separate partitioned address space, but the same address space as a unicast address. The new definition solves the technical obstacles to the use of anycast in the IPv6 era. In IPv6 addressing, anycast communication may appear as unicast and multicast in various network environments.

The introduction of IPv6 not only alters the way of data communication of WSNs, but also the propagation behaviour of abnormal traffics like viruses and network attacks. Nonetheless, IPv6 is a mixed blessing to WSNs: on the upside, it facilitates internetwork connection of heterogeneous WSNs; on the downside, it brings new threats to information security. Currently, IPv6 WSNs often use the clustering architecture for networking (Figure 5). The sensor nodes only communicate with the head node of the local cluster, and the latter communicate with the head node of the superior cluster or other networks. Logically, IPv6 WSNs are a hierarchical DCN.

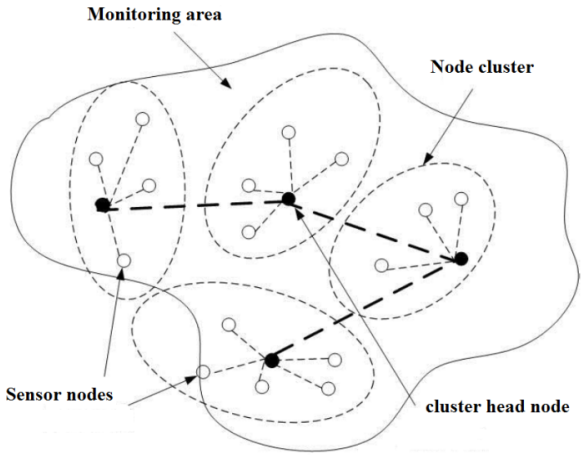


Fig. 5. Cluster Structure of IPv6 WSNs

4 Empirical Analysis on Data Propagation Behaviour of IPv6 WSNs

In IPv6 WSNs, the traditional broadcast communication is replaced by multicast and anycast, resulting in changes to the data propagation mode and virus propagation behaviour of WSNs. The multicast data propagation and anycast data propagation are illustrated in Figures 6 and 7, respectively.

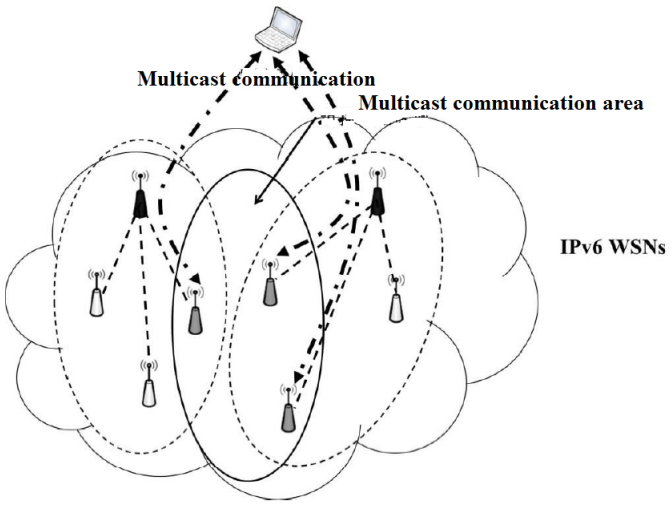


Fig. 6. Multicast communication on IPv6 WSNs

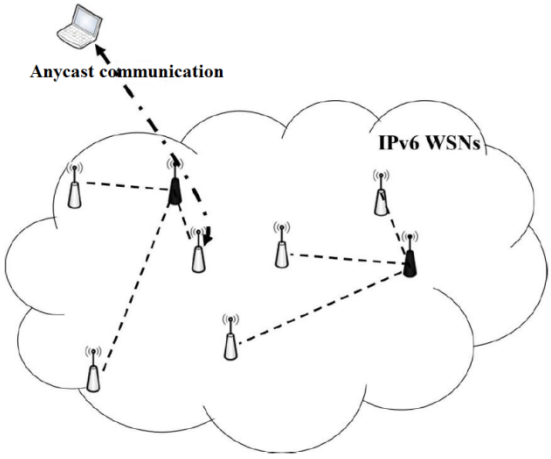


Fig. 7. Anycast communication on IPv6 WSNs

4.1 Virus propagation experiment for IPv6 WSNs

To disclose the virus propagation features of IPv6 WSNs, an IPv6 WSNs simulation experiment was designed to verify virus propagation behaviour and set up an example model for virus propagation in IPv6 WSNs.

The topology of IPv6 WSNs change continuously with the variation in node energy consumption and communication quality. However, the node death is not considered because the focus of our research lies in the features of virus propagation in a stable network. The simulation experiment was carried out in the following steps:

1. 250 sensor nodes were randomly deployed in a 100m×100m area. For convenience, the data acquisition nodes were placed at the centre of the area.
2. The WSNs were clustered by the popular low-energy adaptive clustering hierarchy (LEACH) algorithm, so that the sensor nodes could self-organize into a data propagation network. Figure 8 shows the adjacency relationship between cluster head node and neighbouring nodes. In Figure 8, the × in the centre of the area is the gateway node, the circles are cluster head nodes, and the black dots are common sensor nodes.
3. Three sensor nodes were randomly selected to be infected with a virus at the probability of 100% and serve as the initial virus sources. Then, each infected node could infect its neighbouring nodes at the probability of p_s . Meanwhile, each infected node could be restored as an immune node at the probability of p_r. The multicast communication mode was adopted for the communication between each head node and the sensor node in its cluster, and the anycast communication mode was adopted for the communication between each sensor node and its neighbouring nodes.
4. The network health of IPv6 WSNs in the process of virus propagation was calculated and the overall performance of the network was evaluated objectively. For a new virus, it is impossible to determine its code features, killing method and immunization strategy at the first time. Hence, the sensor nodes infected by the virus might not be scavenged and immunized properly at the first time. According to the experimental results, the peak number of infected nodes generally appeared at about 3 time-steps and at 10 time-steps at the latest. Thus, delayed immunization experiments were performed at $p_r = 0.1$, $p_r = 0.5$, and $p_r = 0.9$, respectively, with $p_s = 0.5$. The results of these experiments are displayed in Figures 9~11.

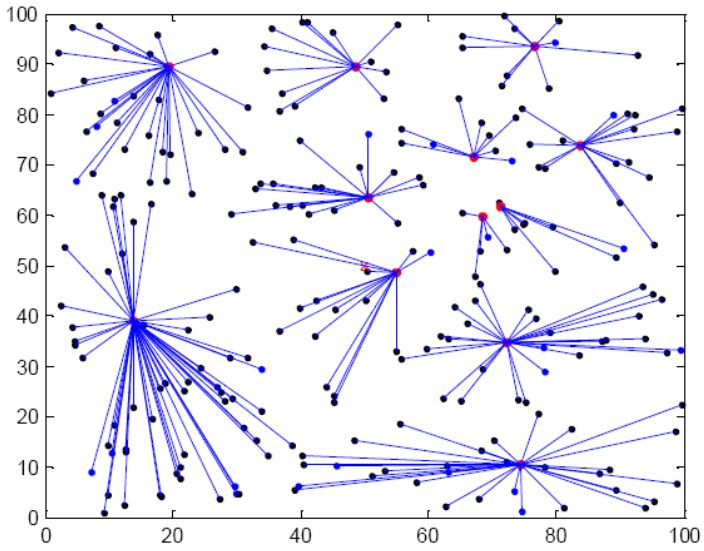


Fig. 8. Adjacency relationship between cluster head node and neighbouring nodes

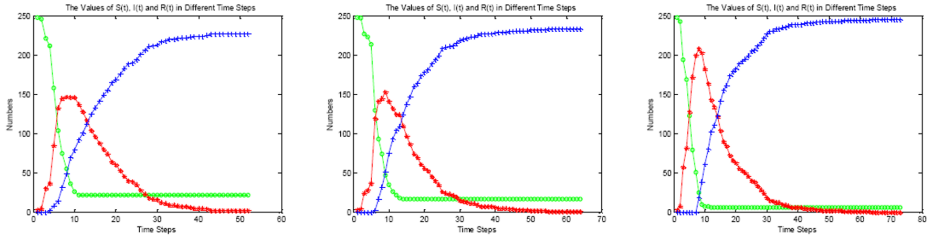


Fig. 9. Results of delayed immunization experiment at $p_s = 0.5$ and $p_r = 0.1$

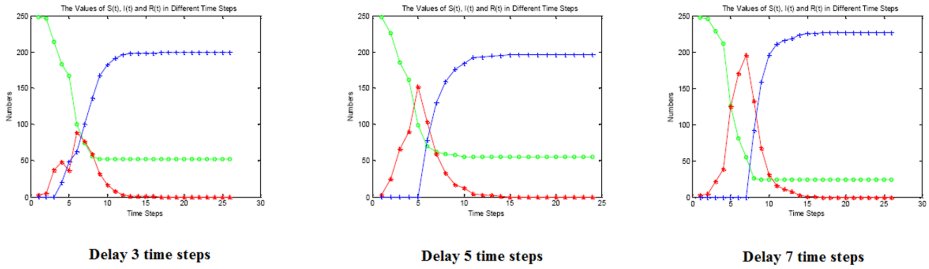


Fig. 10. Results of delayed immunization experiment at $p_s = 0.5$ and $p_r = 0.5$

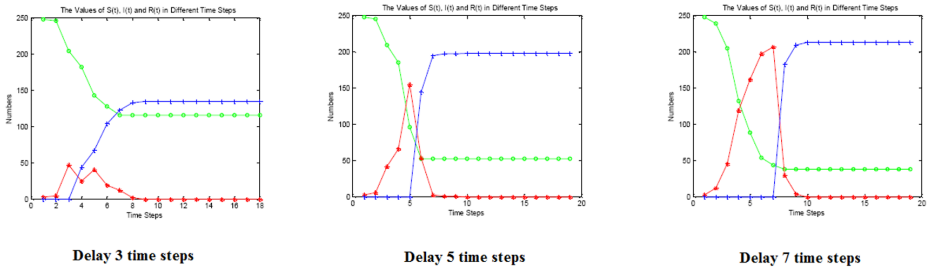


Fig. 11. Results of delayed immunization experiment at $p_s = 0.5$ and $p_r = 0.9$

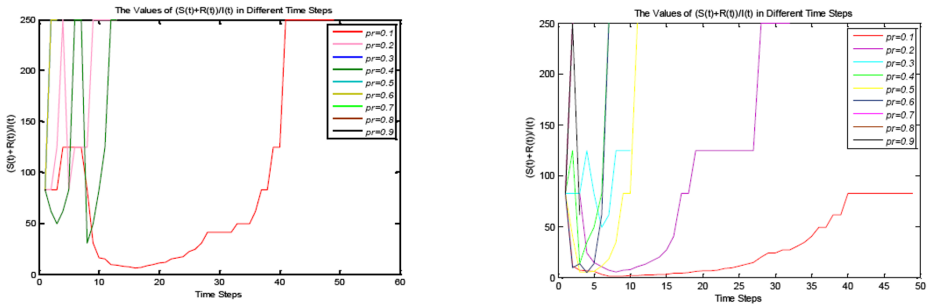
4.2 Analysis on virus propagation behaviour

To visualize the impacts of p_r and p_s values on network health, three groups of simulations were carried out with multiple combinations of p_r and p_s values. The simulated results are shown in Figure 12.

From these simulations, it can be seen that the network quickly converged to the steady state after the start of virus infection. However, the network health underwent considerable ups and downs in the convergence process, which directly affected the data propagation function of the network.

Comparing the network health at $p_s = 0.1$ and that at $p_s = 0.3$, it is clear that, when a virus with known features (i.e. p_s was small) entered the network, the proportion of healthy nodes remained at a high level albeit increase of the value of p_r. By contrast, when a new virus (i.e. p_s was large) entered the network, the proportion of healthy

nodes was extremely low from time to time, despite the adoption of effective virus scavenging and immunization measures ($p_r = 0.9$). In this case, the network was unstable and likely to collapse. In addition, with the growth of the value of p_s, the half-lives of viruses in IPv6 WSNs exhibited a gradual decreasing trend. Thus, the impacts of new viruses should be the focus of the research on virus immunization for IPv6 WSNs, and the viruses must be cleared as soon as possible to ensure the effect of virus removal and immune algorithms.



$p_s = 0.1$ $p_s = 0.3$

Fig. 12. Network health at different combinations of p_s and p_r values

4.3 Construction of virus propagation model for IPv6 WSNs

In light of the above experimental data, a new virus propagation model was created with both multicast and anycast modes for IPv6 WSNs based on the existing biological virus propagation models of complex networks.

According to the SIR model for biological viruses, the following equation is valid for WSNs at time t:

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

where $S(t)$, $I(t)$, and $R(t)$ are respectively the number of susceptible nodes, the number of infected nodes, and the number of immune nodes in WSNs at time t.

Let r_c be the communication radius of the sensor nodes and A be the area of the WSNs. Then, the node degree distribution of the WSNs can be expressed as:

$$P(k) = e^{-<k>} \frac{<k>^k}{k!} \tag{5}$$

The average degree distribution is:

$$< k >= \pi {r_c}^2 \rho \tag{6}$$

where $\rho = \frac{N_t}{A}$ is the node density.

In WSNs, each head node communicates with the sensor nodes in its cluster via multicast communication. Thus, each healthy node is infected at a probability of β_m.

As for the common nodes, the anycast mode is usually adopted for their communication with neighbouring nodes, aiming to achieve network connectivity with the minimum energy. Since anycast only propagates the virus to a sensor node, each healthy node is infected at a probability of β_a/ρ', where $\rho' = N(t)/\pi {r_c}^2$. Suppose there are δ head nodes and $(1-\delta)$ non-cluster head nodes in I_t. According to average degree distribution, the SIR model in IPv6 WSNs can be defined as:

$$\begin{aligned}
\frac{dS(t)}{dt} &= -\beta_m \delta I(t) \frac{\pi {r_c}^2}{A} S(t) - \frac{\beta_a}{\rho'}(1-\delta) I(t) \frac{\pi {r_c}^2}{A} S(t) \\
\frac{dI(t)}{dt} &= \beta_m \delta I(t) \frac{\pi {r_c}^2}{A} S(t) + \frac{\beta_a}{\rho'}(1-\delta) I(t) \frac{\pi {r_c}^2}{A} S(t) - \gamma I(t) \\
\frac{dR(t)}{dt} &= \gamma I(t)
\end{aligned} \tag{8}$$

To accurately depict the network health of IPv6 WSNs, and assess whether WSNs can realize normal data propagation, the health degree of WSNs can be defined as:

$$H = \frac{S(t)+R(t)}{I(t)} \tag{9}$$

5 Conclusions

This paper explores the features of virus propagation in IPv6 WSNs. Considering the lack of empirical data in relevant research, sufficient examples were examined to determine the virus propagation behaviour of IPv6 WSNs. Different types of viruses were taken into account, and their impacts on network performance were investigated one by one. On this basis, a virus propagation model was construction for IPv6 WSNs in light of the classical virus propagation models of complex networks. The research findings shed new light on virus propagation and immunization in IPv6 WSNs.

6 References

[1] Motaharul, I. M., Eui-Nam, H. (2011). Sensor Proxy Mobile IPv6 (SPMIPv6)—A Nov-el Scheme for Mobility Supported IP-WSNs. Sensors, 11(2): 1865-1872. https://doi.org/10.3390/s110201865

[2] Wu, K. (2004). Malaria mathematical model and propagation dynamics. Chinese trop-ical medicine, 5(3): 873-876.

[3] Huo, K., Li, S., Allen, L. (2010). Study on the SIR Model of H1N1 Influenza A Trans-mission. Journal of Hunan University of Technology, 40-42.

[4] Ding, G., Liu, C., Gong, J., Wang, L., Cheng, K., Zhang, D. (2004). SARS epidemical fore-cast research in mathematical model. Chinese Science Bulletin, 49(21): 2332-2338. https://doi.org/10.1360/04we0073

[5] Pei, Y., Liu, S., Li, C. (2009). The dynamics of an impulsive delay SI model with vari-able coefficients. Applied Mathematical Modelling, 33(6): 2766-2776. https://doi.org/10.1016/j.apm.2008.08.011

[6] Britton, T. (2010). Stochastic epidemic models: a survey. Mathematical Biosciences, 225(1): 24-35. https://doi.org/10.1016/j.mbs.2010.01.006

[7] Kermack, W. O., Mckendrick, A. G. (1991). A Contributions to the mathematical theo-ry of epidemics—I. Bulletin of Mathematical Biology, 53(1): 33-55.
[8] Yao, Y., Feng, X., Yang, W. (2014). Analysis of a Delayed Internet Worm Propagation Model with Impulsive Quarantine Strategy. Mathematical Problems in Engineering, 2014(5): 1-18. https://doi.org/10.1155/2014/369360
[9] Basu, P., Ke, W., Little, T. D. C. (2003). Dynamic Task-Based Anycasting in Mobile Ad Hoc Networks. Mobile Networks & Applications, 8(5): 593-612. https://doi.org/10.1023/A:1025198129990
[10] Wang, R. C., Chang, R. S. (2007). Cross-layer binding update for TCP performance enhancement over Mobile IPv6 networks. Iet Communications, 1(5): 924-932. https://doi.org/10.1049/iet-com:20060298

7 Authors

Zhinan Zhou male, Chengde, Hebei Province, now work in modern education and technology centre of Hebei Agricultural University, Research Associate, research direction computer science and technology, Master of Engineering in Agricultural Mechanization Engineering,Hebei Agricultural University.

Wendi Wang female, Hengshui, Hebei Province, now work in College of Mechanical and Electrical Engineering of HebeiAgricultural University, Research Associate, research direction Computer detection and control, Master of Engineering in Agricultural Mechanization Engineering, Hebei Agricultural University.

Yuxia Li worked in hebei agricultural university network center, the jiangsu maritime college library technician, intelligence, deputy director of the institute, sichuan university, master of software engineering, electronic information engineers, part-time teachers school curricula, any information IT community guide teacher!

Article submitted 23 July 2018. Resubmitted 13 August 2018. Final acceptance 23 September 2018. Final version published as resubmitted by the authors.