Hindawi
Discrete Dynamics in Nature and Society
Volume 2017, Article ID 5743801, 9 pages
https://doi.org/10.1155/2017/5743801

Research Article

A Dynamic Programming Model for Internal Attack Detection in Wireless Sensor Networks

Qiong Shi,[1] Li Qin,[2] Lipeng Song,[1] Rongping Zhang,[1] and Yanfeng Jia[1]

[1] *School of Computer Science and Control Engineering, North University of China, Taiyuan, Shan'xi 030051, China*
[2] *School of Instrument and Electronics, North University of China, Taiyuan, Shan'xi 030051, China*

Correspondence should be addressed to Qiong Shi; shiqiong0641@nuc.edu.cn

Received 10 March 2017; Accepted 9 May 2017; Published 1 June 2017

Academic Editor: Lu-Xing Yang

Internal attack is a crucial security problem of WSN (wireless sensor network). In this paper, we focus on the internal attack detection which is an important way to locate attacks. We propose a state transition model, based on the continuous time Markov chain (CTMC), to study the behaviors of the sensors in a WSN under internal attack. Then we conduct the internal attack detection model as the epidemiological model. In this model, we explore the detection rate as the rate of a compromised state transition to a response state. By using the Bellman equation, the utility for the state transitions of a sensor can be written in standard forms of dynamic programming. It reveals a natural way to find the optimal detection rate that is by maximizing the total utility of the compromised state of the node (the sum of current utility and future utility). In particular, we encapsulate the current state, survivability, availability, and energy consumption of the WSN into an information set. We conduct extensive experiments and the results show the effectiveness of our solutions.

1. Introduction

WSN (wireless sensor network) is always vulnerable because it is usually deployed in hostile environments [1]. The attack behaviors in WSN are mainly divided into two types: external attack and internal attack. For the improvement of hardware performance, which makes the public cryptography possible, the external attacks in WSN can be prevented effectively with the security structure based on cryptography [2–4]. Thus, the focus of the study is about internal attack such as detection, revocation, and tolerance of the compromised nodes and replicated nodes that have been physically captured. Normally, there are three ways to detect internal attacks: analyzing the attack behavior [5–8], detecting the compromised nodes [9–13], and verifying replica attack [14–17].

In a WSN, the states of a sensor are typically distinguished into healthy, compromised, responsive, or fail state. At any time, a sensor stays precisely at one of the four states. For the existence of internal attacks, the sensor transits among the states in its lifecycle. In this paper, we leverage the continuous time Markov chain (CTMC) to model the state transition of sensors. In addition, we built up an internal attack detection model for WSN based on classical SIR epidemiological model. The model described the behaviors of the sensors in a WSN under internal attacks.

Thereafter, we can detect the internal attacks over the models. According to our study, the detection rate can be viewed as the rate of the transitions from a compromised state to a responsive state. In this way, the system responds immediately when a sensor changes its state to a compromised state; that is, the node has been attacked. Traditionally, the existing studies on internal attack detection in WSN focus on more efficient detection methods and higher detection rates [18–20], while the detection rate is actually not the higher the better in practice, especially when it is constrained with limits of network characteristics of a WSN such as power and computing capability. In contrast, we are more concerned with the trade-off between detection rate and network characteristics.

Therefore, we proposed a solution to find the optimal detection rate rather than choose the highest rate. By using the Bellman equation, the utility for the state transitions of a sensor can be written in standard forms of dynamic programming. In addition, we encapsulate the four parameters, that is, current state, survivability, availability, and energy consumption, into information set. The information set is a good indicator for achieving the balance between network characteristics and security. We can find the optimal detection rate by maximizing the total utility. Extensive experiments have been conducted to show the effectiveness of our solutions. The experimental results show that our solution can indeed improve the survivability of WSN and therefore guide the design of WSN.

The rest of this paper is organized as follows. In Section 2, we give related work and outline the perspectives and approaches in the existing literatures. In Section 3, we propose the state transition model of internal attack and internal attack detection model, based on CTMC and epidemiological model, respectively. Thereafter, we establish dynamic programming model via the Bellman equation to find the optimal detection rate. In Sections 4 and 5, we present the numerical simulation study for our methods. Finally, we conclude our study in the paper and the future work in Section 6.

2. Related Work

The epidemiological model has been widely used to analyze the spread of malware in wired networks [21–25]. In literature [26], the impact of the network topology on the viral prevalence was studied and author proposed a node-based approach. In literature [27], epidemic processes were studied in complex networks. In literature [28], a theoretical assessment approach was proposed on the impact of patch forwarding on the prevalence of computer virus.

In recent years, application of the epidemiological model in WSN has become increasingly widespread [29]. The analyses based on the simulation and experiment research show that the epidemiological model can effectively describe the dynamic propagation of malware when the number of nodes in the network is large enough. In literature [30], the attack behavior of malware was studied by combining the epidemiological model with a loss equation. In literature [31], the reactive diffusion equation model of malware propagation was proposed based on the theory of epidemiological diseases.

Normally the state of the sensors in a WSN is either healthy, compromised, responsive, or failed. At any time, a sensor stays precisely at one of the four states. The state of a sensor will transit to other types if it suffers an internal attack. Therefore, we use the CTMC to model the state transition of a sensor, though the decision of the "malicious attacker" is not random in the attacked WSN, while the attack time is randomly distributed. The lifecycle of sensors can be regarded as a dynamic system, so the stochastic process can be used to establish the corresponding model. In some related papers, the Markov chain [32] is also widely used to simulate the spread of malware in WSN.

3. Model and Methods

3.1. State Transition Model. The various epidemic models are actually state transition models. These states are mutually exclusive: every sensor is in a precisely specific state at any time. The sensor transits diversely among different states during its lifecycle.

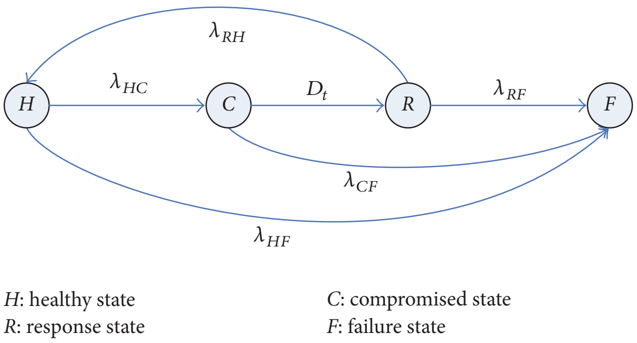


Figure 1: The value of D_t for several planning horizons.

The state transition of a node in WSN can be modeled with a CTMC. Figure 1 depicts the state transition diagram of a node under an internal attack. A circled node in the diagram stands for a state which is either healthy, compromised, responsive, or failed, which are marked with H, C, R, or F, respectively. Each arc in the diagram associates with a rate $\lambda_{ij}, i, j \in \{H, C, R, F\}$, which indicates the rate of the transition from state i to state j when the node suffered an internal attack.

State transition processes are as follows: a node in WSN in H was functioning correctly at the beginning. We suppose that the healthy sensor becomes a compromised node under an attack; that is, the state of the sensor turns to C from H. When the compromised state has been detected, the state of it will change to R; otherwise, the state of it will change to F or remain at C. If a sensor stays in R, a response action will be carried out. If we get an acknowledgement from the node, then it moves to H. Otherwise, it will be viewed as F. The response actions include software rejuvenation and reconfiguration as a countermeasure against attacks. Since a WSN is usually deployed in hostile environments or areas, the sensors could be failed for the influence of environment and outage of power.

3.2. Internal Attack Detection Model. We explore the impact of detection rate on sensors under internal attack and metrics by combining a classical epidemiological model and an economic behavioral model based on a forward-looking, representative agent. Detection efforts determine the detection rate that will determine nodes from C to R by some specific rate. It will affect the survivability and availability of nodes. The survivability and availability of one single node will have influence on the entire cluster and network.

There are four types of nodes in the WSN. Assume we have N sensors in total, and let H_t, C_t, R_t, and F_t be the number of healthy nodes, compromised nodes, responsive nodes, and failed nodes, respectively. Then we have the following differential equations:

$$\frac{dH_t}{dt} = -\lambda_{HC} H_t C_t + \lambda_{RH} R_t - \lambda_{HF} H_t,$$

$$\frac{dC_t}{dt} = \lambda_{HC} H_t C_t - D_t C_t - \lambda_{CF} C_t,$$

$$\frac{dR_t}{dt} = D_t C_t - \lambda_{RH} R_t - \lambda_{RF} R_t,$$

$$\frac{dF_t}{dt} = \lambda_{RF} R_t + \lambda_{CF} C_t + \lambda_{HF} H_t. \tag{1}$$

Equations (1) formalize four-state transition processes when a sensor in the WSN is under an internal attack. D_t in the equations is the detection rate, that is, the rate that nodes detected in C at every interval. The transition rate from C to R is taken as the detection rate D_t; that is, $\lambda_{CR} = D_t$. In other words, response measures should be taken immediately as long as the node is recognized as C. However, the other types of state transition do not depend on the detection rate.

The above model (model 1) illustrates the dynamic evolution process of WSN under internal attack within a certain period. The dynamics of internal attack detection model cannot be analyzed thoroughly in a short period of time, so we will focus on the process of the long-term dynamic evolution on the WSN. With the power of WSN limited and deployed in harsh environments, a large number of redundant sensors are normally deployed in WSN for the sensors cannot be able to be repaired once they transited to the failure state. After the sensor fails, the redundant node will be the suitable alternatives. We will call it "death" and "birth"; we will put forward model 2:

$$\begin{aligned}
\frac{dH_t}{dt} &= N_0 - \lambda_{HC} H_t C_t + \lambda_{RH} R_t - \lambda_{HF} H_t,\\
\frac{dC_t}{dt} &= \lambda_{HC} H_t C_t - D_t C_t - \lambda_{CF} C_t,\\
\frac{dR_t}{dt} &= D_t C_t - \lambda_{RH} R_t - \lambda_{RF} R_t.
\end{aligned} \tag{2}$$

Assume the immutability of the sum of the sensors (including H_t, C_t, R_t, and F_t, excluding abundant nodes), N_0 is the number of the "births", and it is equal to the number of "deaths," namely the abundant nodes which replaced the "death". To simplify the counting process, let $\lambda_{HF} = \lambda_{CF} = \lambda_{RF} = \lambda$.

Dynamic analysis is carried out on model 2 and both the existence and stability of the equilibrium point will be discussed. According to (2), we find the steady state as follows:

(i) $E_0 = (1, 0, 0)$.

(ii) Interior equilibrium point $E^*(H_t^*, R_t^*, C_t^*)$

$$\begin{aligned}
H_t^* &= \frac{\lambda + D_t}{\lambda_{HC}},\\
R_t^* &= \frac{D_t(\lambda_{HC} - \lambda - D_t)}{\lambda_{HC}(D_t + \lambda + \lambda_{RH})},\\
C_t^* &= \frac{(\lambda_{HC} - \lambda - D_t)(\lambda + \lambda_{RH})}{\lambda_{HC}(D_t + \lambda + \lambda_{RH})}.
\end{aligned} \tag{3}$$

The Jacobi matrix of the model is acquired:

$$J = \begin{pmatrix} -\lambda_{HC} C_t - \lambda & -\lambda_{HC} H_t & \lambda_{RH} \\ \lambda_{HC} C_t & \lambda_{HC} H_t - D_t - \lambda & 0 \\ 0 & D_t & -\lambda_{RH} - \lambda \end{pmatrix}. \tag{4}$$

(1) The Jacobian corresponding to $E_0(1, 0, 0)$ is that

$$J_0 = \begin{pmatrix} -\lambda & -\lambda_{HC} & \lambda_{RH} \\ 0 & \lambda_{HC} - D_t - \lambda & 0 \\ 0 & D_t & -\lambda_{RH} - \lambda \end{pmatrix} \tag{5}$$

and, thus, the eigenvalues of the Jacobian at $E_0(1, 0, 0)$ must have negative real parts, which are equivalent to $\lambda_1 = -\lambda < 0$, $\lambda_2 = \lambda_{HC} - D_t - \lambda < 0$, and $\lambda_3 = -\lambda_{RH} - \lambda < 0$.

(2) The Jacobian corresponding to $E^*(H_t^*, R_t^*, C_t^*)$ is that

$$J^* = \begin{pmatrix} -\dfrac{(\lambda_{HC} - \lambda - D_t)(\lambda + \lambda_{RH})}{D_t + \lambda + \lambda_{RH}} - \lambda & -\lambda - D_t & \lambda_{RH} \\ \dfrac{(\lambda_{HC} - \lambda - D_t)(\lambda + \lambda_{RH})}{D_t + \lambda + \lambda_{RH}} & 0 & 0 \\ 0 & D_t & -\lambda_{RH} - \lambda \end{pmatrix}. \tag{6}$$

The eigenvalues of the Jacobian at $E^*(H_t^*, R_t^*, C_t^*)$ are obtained $\lambda_1 = -\lambda < 0$ and λ_2 and λ_3 meet $(\lambda')^2 + (\lambda_{RH} + \lambda + (\lambda_{HC} - \lambda - D_t)(\lambda + \lambda_{RH})/(D_t + \lambda + \lambda_{RH}))\lambda' + ((\lambda_{HC} - \lambda - D_t)(\lambda + \lambda_{RH})/(D_t + \lambda + \lambda_{RH}))D_t = 0$, because $\lambda_{HC} - \lambda - D_t > 0$, then $\lambda_2 \lambda_3 > 0$, $\lambda_2 + \lambda_3 < 0$, and thus $\lambda_2 < 0$, $\lambda_3 < 0$.

By using linear analysis, we can find that E^* is always stable.

Model 1, which is the key of the article, is the basis of the model behind and simulation test. The dynamics analysis is only carried out on model 2.

3.3. Dynamic Programming.

We next present a dynamic programming paradigm to find the optimal detection rate. The method is based on an interesting observation that the highest detection rate does not always act as the best choice. So many factors influence the detection rate in WSN, such as availability, survivability, and energy. Suppose we have a healthy sensor under attack. The sensor still can provide service even though it transits to C due to the attack. However, the service will break off if the sensor, currently staying in C, moves to R. The service continues when the sensor restores to a healthy state successfully. The availability of the WSN declines when the sensor in R is doing that recovery. The utility of C is greater than R and the compromised nodes might as well have not been detected in this case. So higher detection rate does not always mean better utility. Moreover, higher detection rate means more energy consumption, which violates the efficiency rules in WSNs. Above all, we focus on the optimal rate instead of the highest one. All the factors we were concerned about have been abstracted to be part of the information set.

We propose a new objective, namely, utility, measuring the quality of the information set. The detection rate will maximize the expected net value of the present utility, while influencing current utility and expected utility in future periods. To model this dynamic maximization, we define utility within a period and define the probability of transiting across states. We switch to a discrete-time formulation, with time incremented in days and transition probabilities reformulated below on the basis of (1).

Suppose that we have complete statistics about the current value of utility, including the negative utilities, with its information set including knowledge about survivability, availability, energy consumption, and H_t, C_t, R_t, and F_t.

Let $u_t(S)$ be the current utility of a sensor at time t in S ($S \in \{H, C, R, F\}$). Then, the utility of the sensor in C at time t is formally defined as follows:

$$u_t(C, D_t) = \left(bD_t - D_t^2\right)^{\gamma} - a. \tag{7}$$

The utility function u_t is a hybrid indicator measuring the content of the information set that has been mentioned before, which can simplify the model and enhance the generality of it. The utility function is concave and unimodal. The coefficients, a and b, in (7) can be adjusted according to the application.

According to (1), the transition probabilities between a pair of states are written as follows:

$$\begin{aligned} P_{HC} &= 1 - e^{(-\lambda_{HC} C_t)}, \\ P_{RH} &= 1 - e^{(-\lambda_{RH})}, \\ P_{HF} &= 1 - e^{(-\lambda_{HF})}, \\ P_{CR} &= D_t, \\ P_{CF} &= 1 - e^{(-\lambda_{CF})}, \\ P_{RF} &= 1 - e^{(-\lambda_{RF})}. \end{aligned} \tag{8}$$

The detection rate is determined by the current utility, at time t, and the expected utility at time $t + 1$, of compromised nodes. We use the Bellman equation to calculate the optimal detection rate and utility equations can be written as standard forms of dynamic programming

$$\begin{aligned} V_t(H) &= u_t(H) \\ &\quad + \delta\left[P_{HH} V_{t+1}(H) + P_{HC} V_{t+1}(C) + P_{HF} V_{t+1}(F)\right], \end{aligned} \tag{9}$$

$$\begin{aligned} V_t(C) &= u_t(C, D_t) \\ &\quad + \delta\left[P_{CC} V_{t+1}(C) + P_{CR} V_{t+1}(R) + P_{CF} V_{t+1}(F)\right], \end{aligned} \tag{10}$$

$$\begin{aligned} V_t(R) &= u_t(R) \\ &\quad + \delta\left[P_{RR} V_{t+1}(R) + P_{RF} V_{t+1}(F) + P_{RH} V_{t+1}(H)\right], \end{aligned} \tag{11}$$

$$V_t(F) = u_t(F) + \delta\left[P_{FF} V_{t+1}(F)\right]. \tag{12}$$

In the equation system, $V_t(S)$ $(S = H, C, R, F)$ is the utility for a sensor staying in S at time t and δ is the discount factor. $u_t(S)$ is current utility. $V_{t+1}(S)$ is the expected utility and P_{ij} stands for the transition probabilities between states (see (8)). The second term of the right member in each equation indicates that the utility of the future $(t + 1)$ moments is discounted to the present (t) utility.

Since the utilities are written in the standard form of dynamic programming, we can optimize the detection rate D_t dynamically with a planning horizon of length τ. If $t = 0$, then D_0 is chosen to solve the problem formalized by (9)–(12). In period $t = 1$, the system updates knowledge on information set and uses (9)–(12) to optimize anew over the next τ planning periods. The process continues in this way. For example, if $\tau = 7$, then on February 1 the horizon is through February 8, but on February 2 the horizon extends to February 9, and so on:

$$\begin{aligned} V_t(C) &= \max\{u_t(C, D_t) \\ &\quad + \delta\left[P_{CC} V_{t+1}(C) + P_{CR} V_{t+1}(R) + P_{CF} V_{t+1}(F)\right]\}. \end{aligned} \tag{13}$$

In (13), if we take the maximum value of (10), the optimal D_t can be obtained. So partial derivative of (13) is formalized as

$$\frac{\partial u_t(C, D_t)}{\partial D_t} = \delta\left[-\frac{\partial P_{CC}}{\partial D_t} V_{t+1}(C) - \frac{\partial P_{CR}}{\partial D_t} V_{t+1}(R)\right]. \tag{14}$$

The left member in (14) stands for the gain of utility, at time t, for a unit increase of the detection rate. The right member in (14) is the expected benefit from a unit increase of the detection rate at time t, which comes from future discounts.

If $t = \tau$, we have $t + 1 = \tau + 1$. Each utility at $\tau + 1$ is 0, since $\tau + 1$ exceeds the planning horizon.

The optimal detection rate D_t is determined by the information set at time t and its effects on the future values of H, C, R, and F. It is reasonable to assume that the system adapts to forecasts on the basis of the current information set.

The optimal detection rate can be reached with the equation system (9)–(14) by using backward induction over the planning period $[0, \tau]$.

4. Experiments

In this section we present the experimental studies of our models. In the experiments, we simulate two different WSNs that are under internal attacks and conduct three groups of experiments with them. The first group of experiments is designed to find the optimal detection rate D_t by using the dynamic programming paradigm. In the second group, we verify the models. In the third one, we present comparative studies by varying the value of detection rate D_t.

4.1. Experimental Setup. We simulate two different WSNs in the experiments:

(1) For the first WSN, the number of healthy sensors is much larger than that of compromised sensors, where $H_t = 0.9$, $C_t = 0.1$, $R_t = 0$, and $F_t = 0$.

Table 1: The parameters in models.

Parameter	Description
δ	Discount factor
λ_{HC}	Compromised rate
λ_{CR}	Responsive rate
λ_{RH}	Recovery rate
λ_{CF}	Failure from compromised rate
λ_{HF}	Failure rate
λ_{RF}	Failure from responsive rate

Table 2: The parameter value.

Parameter	Value
γ	0.25
a	1
b	0.5
δ	0.9
λ_{HC}	0.1
λ_{CR}	D_t, 0.3, 0.9
λ_{RH}	0.8
λ_{CF}	0.000278
λ_{HF}	0.01
λ_{RF}	0.0417

(2) In the second one, the number of healthy sensors is almost the same as that of compromised sensors, where $H_t = 0.6, C_t = 0.4, R_t = 0$, and $F_t = 0$.

The settings of the parameters of the models are summarized in Tables 1 and 2. Particularly, the utilities of H, C, R, and F fall in $[0, 1]$. To note is that the parameters can be changed according to various application scenarios.

5. Experimental Results

The Optimal Detection Rate. In the first group of experiments, we are to find the optimal detection rate D_t. In this experiment, the current utilities of H, F, and R are initially set to 1, 0, and 0.6, respectively. We evaluated the detection rate D_t for the two WSNs. As we can see from Figure 2, there is no significant difference of the detection rates between the two WSNs. The results show that the ratio of healthy sensors and the compromised sensors have little influence on the detection rate D_t and the value of D_t gradually converges to 0.75 after $\tau = 5$. The optimal value of D_t will be obtained when $\tau = 9$, where the optimal values for both WSNs fall into $[0.74, 0.75]$.

Verifying the Models. We apply the optimal detection rate $D_t = 0.75$ in second group of experiments. Figures 3–6 plot the change in the number of sensors in H, C, R, and F for WSNs in nine days. As we can see from Figure 3, the number of sensors in H decreases when t is in $[0, 1]$. After the decline, there is a sudden increase and the number of healthy sensors gradually converges to a constant value after $t = 4$. For example, the ratio of healthy sensors is around 0.9. Since we have more healthy sensors, the WSN is therefore robust. In contrast, as shown by Figure 4, the number of sensors in C drops quickly to 0. The results justify the effectiveness of our detection mechanism and the optimal detection rate is very effective for the transition of compromised nodes (detection rate in the model is transition rate). From Figure 5, we observe that the number of responsive sensors jumps quickly to a peak at $t = 1$ and then gradually decreases to 0. When t is in $[0, 1]$, the number of nodes in C is greatest and it is the period of most numbers of nodes from C to R. So the number of nodes in R increases quickly and reaches the peak. In Figure 6, we can see that the number of failed sensors increases monotonically as the time is elapsing. This is because a WSN is usually deployed in hostile environments and the sensors cannot get repaired once they failed. From Figures 3–6, we observe that there are big deviations between the dashed lines and solid line at beginning, but the deviation drops off gradually to 0 as time is increasing. It means that each of the WSNs used in our experiments converges to a steady state regardless of the initial condition during an observation period. Therefore, we can conclude that our model is general enough and it is applicable to a large range of WSNs.

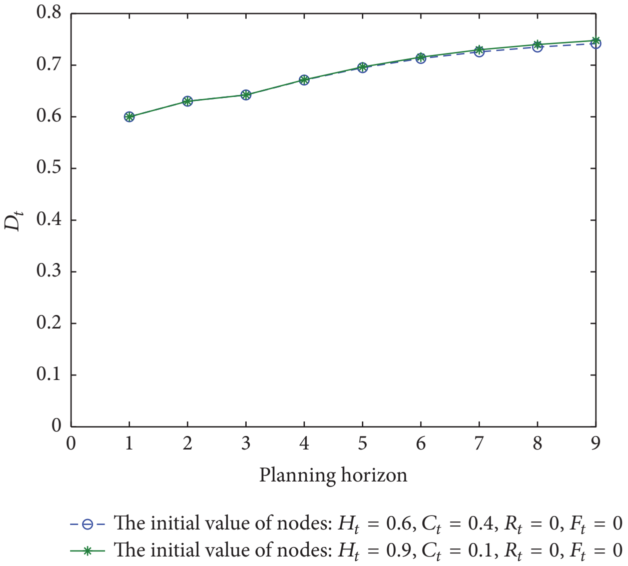


Figure 2: The value of D_t for several planning horizons.

Comparative Studies. In Section 3, we have made an assumption that the optimal detection rate is better than the highest one. To justify this assumption, in this group of experiments, we census the number of sensors being in $(H, C, R,$ and $F)$ by varying the detection rate D_t. In the previous simulation, we have got the optimal detection rate $D_t = 0.75$ and we have also proved that our model is valid for both WSNs. So we can conduct the comparative experiments over only one WSN. We use the WSN with $H_t = 0.9, C_t = 0.1, R_t = 0$, and $F_t = 0$. In the literature [33], the author chose five empirical values at the transition rate from C to R, and we select the highest value 0.3 as D_t. In addition, we select another detection rate,

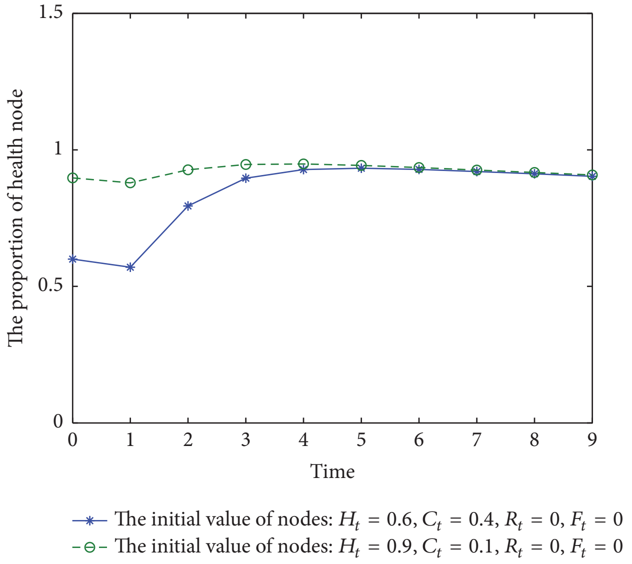


Figure 3: The proportion of healthy sensors.

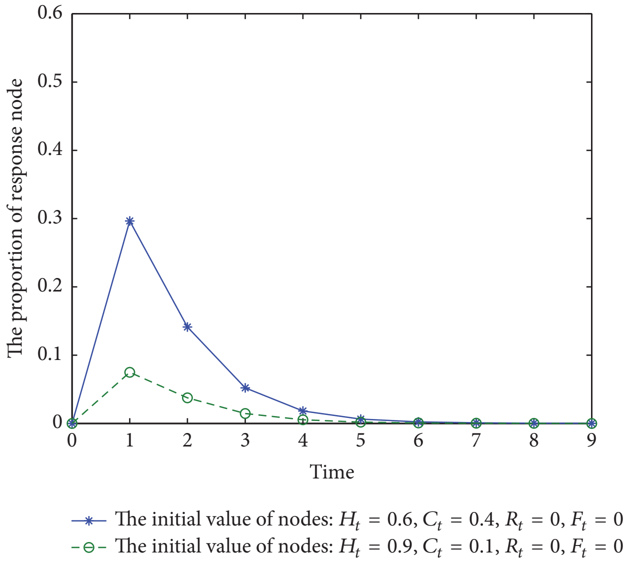


Figure 5: The proportion of responsive sensors.

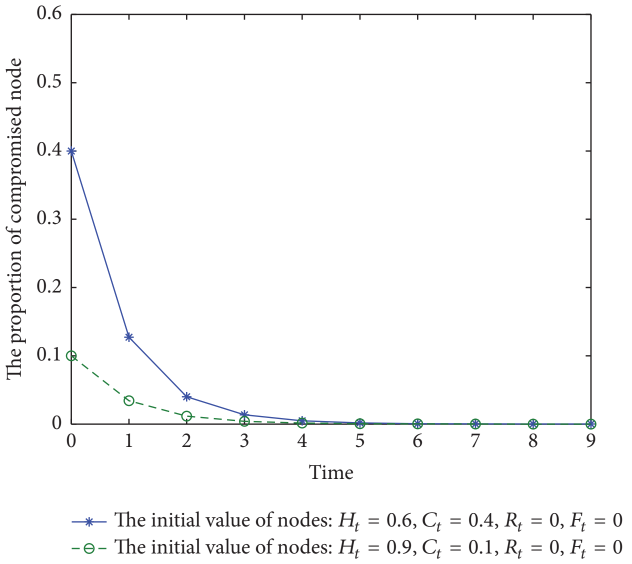


Figure 4: The proportion of compromised sensors.

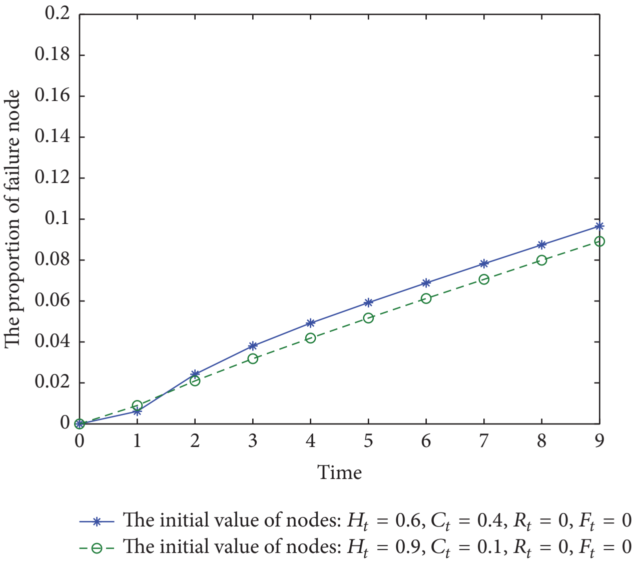


Figure 6: The proportion of failed sensors.

$D_t = 0.9$, to compare with. We plot the results in Figures 7–10, where the blue solid line represents the results $D_t = 0.75$, the green dashed line represents the results $D_t = 0.3$, and the red dashed line represents the results for $D_t = 0.9$.

As shown in Figure 7, there is a drop at the beginning for each line, but the blue solid one rises immediately when $t = 1$. The other two lines, $D_t = 0.9$ and $D_t = 0.3$, get to rise until $t = 2$. This shows that our model can make the WSN more robust, since it gets restored faster. Figure 8 shows the number of compromised sensors. We observe that the higher the detection rate D_t the faster the line drops. The red dotted line and the blue solid line move gradually close to zero after $t = 2$, which means that the reliability of the WSN is getting improved. We can also observe that the blue solid line converges in almost the same speed with the red dashed line. In other words, our model and $D_t = 0.9$ have the same performances, which are much better than that of $D_t = 0.3$. Figure 9 plots the number of the responsive sensors. As we can see from the figure, the blue solid line is completely below the other red dashed line. It is clear that optimal detection rate is better than the higher one. Although it only beats by $D_t = 0.3$ at $t = 1$, it gets improved fast after that time. In addition, we observe the blue solid line drops first, which indicates the recovery process starts earlier than other choices. Figure 10 plots the change of the failed sensors, where the three lines show similar trend. To note is that the WSN has more failed nodes when the detection rate D_t goes larger. when D_t is 0.75 and D_t is 0.3, the number of failure nodes is similar.

We have compared our solution with other ones from the recovery time, the recovery rate, the number of the final

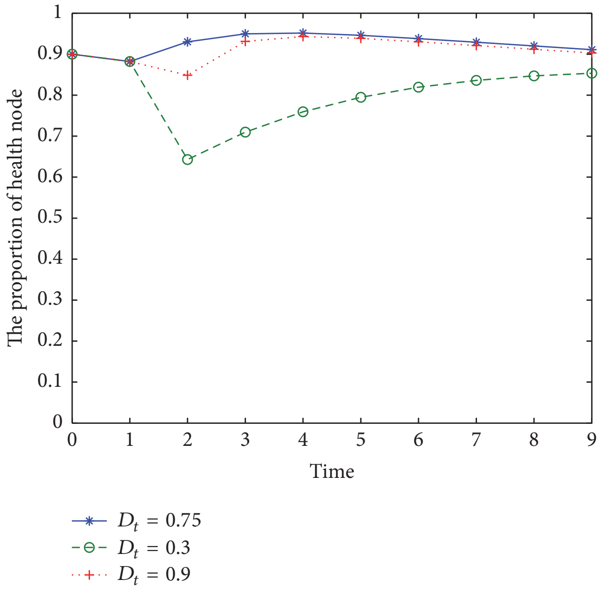


Figure 7: The proportion of responsive sensors.

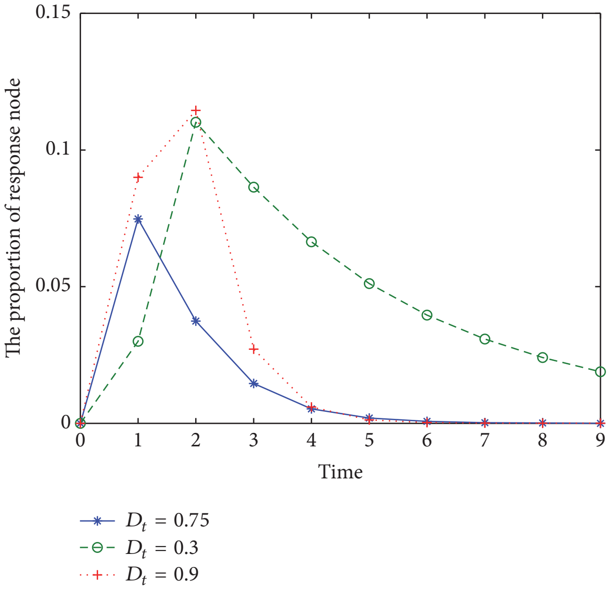


Figure 9: The proportion of responsive sensors.

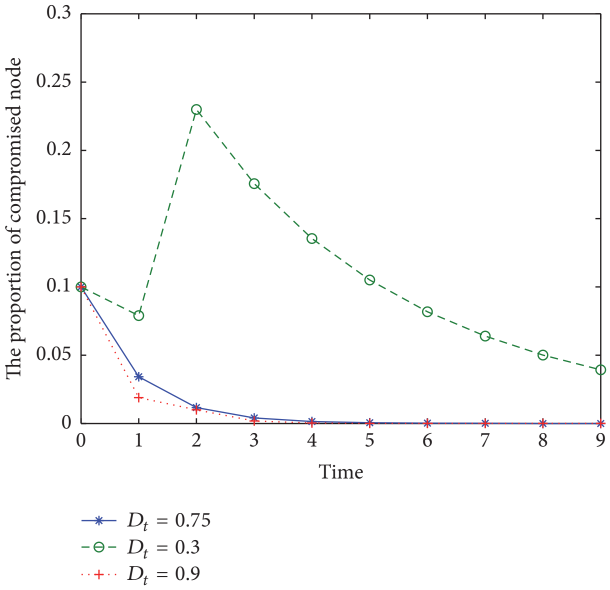


Figure 8: The proportion of compromised sensors.

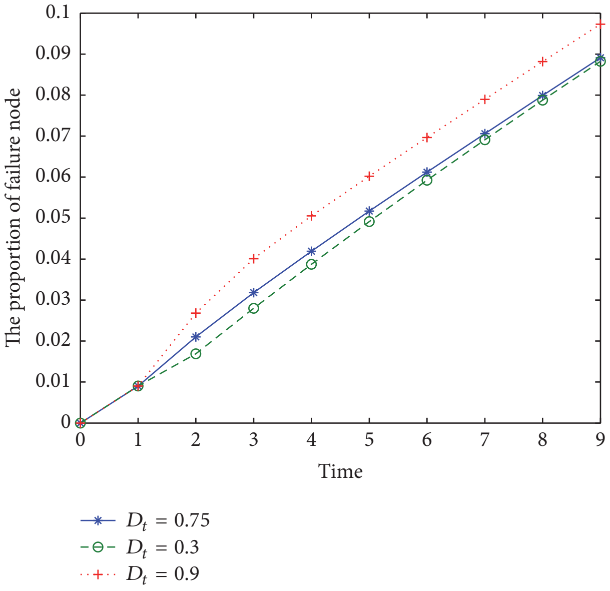


Figure 10: The proportion of failed sensors.

failed nodes, and the energy consumption. In general, the simulation results show that our solution outperforms the other ones. It justifies our observation that the highest detection rate is not always servers as the best choice.

6. Conclusion

In this work, we investigated the problem of finding the detection rate of WSN under internal attacks. Firstly, we established a state transition model of sensors based on the CTMC. The model described the behaviors of sensors in a WSN under attacked nodes and the transition between states. We are the first to observe that detection rate is irrelevant to other state transitions except the transition from C to R. Therefore, we take the detection rate as the transition rate from C to R. Secondly, we modeled the state transition process of the sensors in a WSN under internal attacks by using the epidemic model and make a formal description about this model. Thirdly, by using the dynamic programming paradigm (Bellman equation), we can easily find the optimal detection rate for WSN under internal attacks. In addition, we encapsulated the influencing factors into an information set which captures the current utility and the utility in future time. In this way, the detection rate can be optimized by maximizing the total utility of the current and future utility discount in C. The experimental studies justified the validity of our models.

In the future, we would like to quantize the influencing factors with respect to survivability, availability, and energy consumption in order to improve the accuracy and practicability of detection rate. Moreover, it is more meaningful to set the parameters applied in the simulation according to a real world application. In addition, we will introduce the immune state into the model and refer to the SIRS model [34, 35] for further study. Therefore, it will accelerate the design of WSN and then improve the availability and survivability of WSN.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work is supported by the National Sciences Foundation of China (61379125).

References

[1] Y. Wang, G. Attebury, and B. Ramamurthy, “A survey of security issues in wireless sensor networks,” *IEEE Communications Surveys and Tutorials*, vol. 8, no. 2, pp. 2–22, 2006.

[2] A. Liu and P. Ning, “TinyECC: a configurable library for elliptic curve cryptography in wireless sensor networks,” in *Proceedings of the 7th International Conference on Information Processing in Sensor Networks (IPSN ’08)*, pp. 245–256, St. Louis, Mo, USA, April 2008.

[3] H. D. Wang, B. Sheng, C. C. Tan, and Q. Li, “Comparing symmetric–key and public–key based security schemes in sensor networks: a case study of user access control,” in *Proceedings of the 28th International Conference on Distributed Computing Systems (ICDCS ’08)*, pp. 11–18, China, 2008.

[4] R. H. Wang, W. Du, X. Liu, and P. Ning, “ShortPK: a short–term public key scheme for broadcast authentication in sensor networks,” *ACM Transactions on Sensor Networks*, vol. 6, no. 1, article 9, pp. 1–29, 2009.

[5] P. Ballarini, L. Mokdad, and Q. Monnet, “Modeling tools for detecting DoS attacks in WSNs,” *Security and Communication Networks*, vol. 6, no. 4, pp. 420–436, 2013.

[6] Y. Zhang, W. Liu, W. Lou, and Y. Fang, “Location–based compromise–tolerant security mechanisms for wireless sensor networks,” *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 247–260, 2006.

[7] Y. Chen, J. Yang, W. Trappe, and R. P. Martin, “Detecting and localizing identity–based attacks in wireless and sensor networks,” *IEEE Transactions on Vehicular Technology*, vol. 59, no. 5, pp. 2418–2434, 2010.

[8] J. Katiravan, D. N, and D. N, “A two level detection of routing layer attacks in hierarchical wireless sensor networks using learning based energy prediction,” *KSII Transactions on Internet and Information Systems*, vol. 9, no. 11, pp. 4644–4661, 2015.

[9] A. Ahmed, K. Abu Bakar, M. . Channa, K. Haseeb, and A. W. Khan, “A survey on trust based detection and isolation of malicious nodes in ad–hoc and sensor networks,” *Frontiers in Computer Science*, vol. 9, no. 2, pp. 280–296, 2015.

[10] Y. Zhang, J. Yang, W. Li, L. Wang, and L. Jin, “An authentication scheme for locating compromised sensor nodes in WSNs,” *Journal of Network and Computer Applications*, vol. 33, no. 1, pp. 50–62, 2010.

[11] A. Al-Riyami, N. Zhang, and J. Keane, “An adaptive early node compromise detection scheme for hierarchical wsns,” *IEEE Access*, vol. 4, pp. 4183–4206, 2016.

[12] N. Labraoui, M. Gueroui, and L. Sekhri, “A risk–aware reputation–based trust management in wireless sensor networks,” *Wireless Personal Communications*, vol. 87, no. 3, pp. 1037–1055, 2016.

[13] A. Le, J. Loo, A. Lasebae, M. Aiash, and Y. Luo, “6LoWPAN: a study on QoS security threats and countermeasures using intrusion detection system approach,” *International Journal of Communication Systems*, vol. 25, no. 9, pp. 1189–1212, 2012.

[14] B. Zhu, S. Setia, S. Jajodia, S. Roy, and L. Wang, “Localized multicast: efficient and distributed replica detection in large–scale sensor networks,” *IEEE Transactions on Mobile Computing*, vol. 9, no. 7, pp. 913–926, 2010.

[15] Y. P. Zeng, J. N. Cao, S. G. Zhang, S. Guo, and L. Xie, “Random–walk based approach to detect clone attacks in wireless sensor networks,” *IEEE Journal on Selected Areas in Communications*, vol. 28, no. 5, pp. 677–691, 2010.

[16] W. T. Zhu, J. Zhou, R. H. Deng, and F. Bao, “Detecting node replication attacks in wireless sensor networks: a survey,” *Journal of Network and Computer Applications*, vol. 35, no. 3, pp. 1022–1034, 2012.

[17] W. Z. Khan, M. S. Hossain, M. Y. Aalsalem, N. M. Saad, and M. Atiquzzaman, “A cost analysis framework for claimer reporter witness based clone detection schemes in WSNs,” *Journal of Network and Computer Applications*, vol. 63, pp. 68–85, 2016.

[18] S. S. Wang, K. Q. Yan, and C. Liu, “An integrated intrusion detection system for cluster-based wireless sensor networks,” *Expert Systems with Applications*, vol. 38, no. 12, pp. 15234–15243, 2011.

[19] I. Almomani, B. Al-Kasasbeh, and M. AL-Akhras, “WSN-DS: a Dataset for intrusion detection systems in wireless sensor networks,” *Journal of Sensors*, vol. 2016, article 4731953, pp. 1–16, 2016.

[20] N. Labraoui, M. Gueroui, and M. Aliouat, “Secure DV-Hop localization scheme against wormhole attacks in wireless sensor networks,” *European Transactions on Telecommunications*, vol. 23, no. 4, pp. 303–316, 2012.

[21] L. Song, J. Zhen, G. Sun, J. Zhang, and X. Han, “Influence of removable devices on computer worms: dynamic analysis and control strategies,” *Computers and Mathematics with Applications*, vol. 61, no. 7, pp. 1823–1829, 2011.

[22] P. Van Mieghem, J. Omic, and R. Kooij, “Virus spread in networks,” *IEEE/ACM Transactions on Networking*, vol. 17, no. 1, pp. 1–14, 2009.

[23] F. D. Sahneh, C. Scoglio, and P. Van Mieghem, “Generalized epidemic mean–field model for spreading processes over multilayer complex networks,” *IEEE/ACM Transactions on Networking*, vol. 21, no. 5, pp. 1609–1620, 2013.

[24] X. Yang, Y. Zhu, J. Hong, L.-X. Yang, Y. Wu, and Y. Y. Tang, “The rationality of four metrics of network robustness: a viewpoint of robust growth of generalized meshes,” *PLoS ONE*, vol. 11, no. 8, Article ID e0161077, 2016.

[25] L.-X. Yang and X. Yang, “A new epidemic model of computer viruses,” *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 6, pp. 1935–1944, 2014.

[26] L.-X. Yang, M. Draief, and X. Yang, “The impact of the network topology on the viral prevalence: a node–based approach,” *PLoS ONE*, vol. 10, no. 7, article e0134507, 2015.

[27] R. Pastor-Satorras, C. Castellano, P. Van Mieghem, and A. Vespignani, “Epidemic processes in complex networks,” *Reviews of Modern Physics*, vol. 87, no. 3, pp. 925–979, 2015.

[28] L.-X. Yang, X. Yang, and Y. Wu, “The impact of patch forwarding on the prevalence of computer virus: a theoretical assessment approach,” *Applied Mathematical Modelling*, vol. 43, pp. 110–125, 2017.

[29] L. Feng, L. Song, Q. Zhao, and H. Wang, “Modeling and stability analysis of worm propagation in wireless sensor network,” *Mathematical Problems in Engineering*, Article ID 129598, Art. ID 129598, 8 pages, 2015.

[30] M. H. R. Khouzani, S. Sarkar, and E. Altman, “Optimal control of epidemic evolution,” in *Proceedings of the IEEE International Conference on Computer Communications (INFOCOM ’11)*, pp. 1683–1691, April 2011.

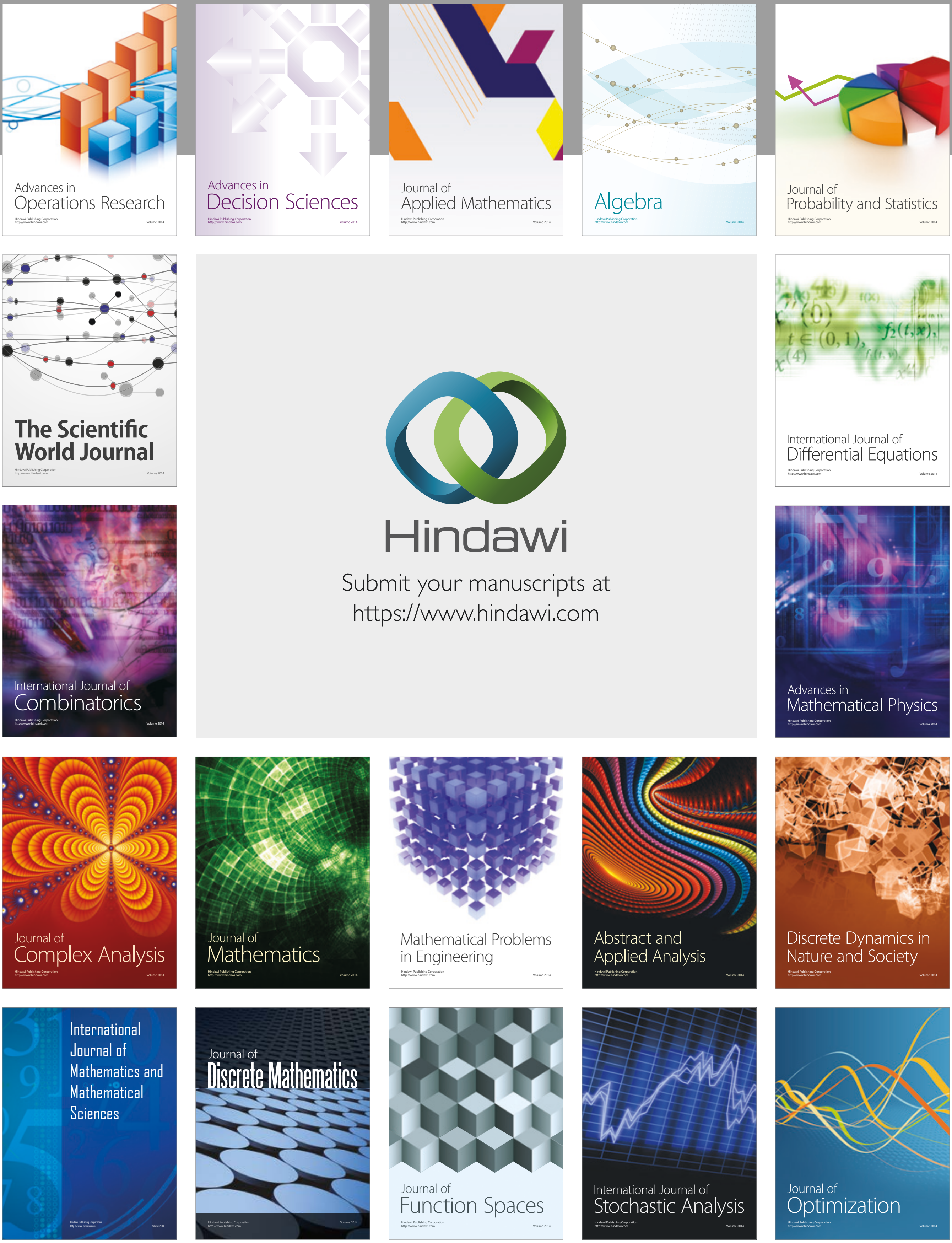
[31] Z. B. He and X. M. Wang, “A spatial–temporal model for the malware propagation in MWSNs based on the reaction–diffusion equations,” in *Proceedings of the WAIM 2012 Workshops*, pp. 45–56.

[32] S. Shen, L. Huang, J. Liu, A. C. Champion, S. Yu, and Q. Cao, “Reliability evaluation for clustered WSNs under malware propagation,” *Sensors*, vol. 16, no. 6, article no. 855, 2016.

[33] S. Parvin, F. K. Hussain, J. S. Park, and D. S. Kim, “A survivability model in wireless sensor networks,” *Computers and Mathematics with Applications*, vol. 64, no. 12, pp. 3666–3682, 2012.

[34] L.-X. Yang, M. Draief, and X. Yang, “The optimal dynamic immunization under a controlled heterogeneous node–based SIRS model,” *Physica A.*, vol. 450, pp. 403–415, 2016.

[35] L. Yang, M. Draief, and X. Yang, “Heterogeneous virus propagation in networks: a theoretical study,” *Mathematical Methods in the Applied Sciences*, vol. 40, no. 5, pp. 1396–1413, 2017.



Advances in Operations Research
Advances in Decision Sciences
Journal of Applied Mathematics
Algebra
Journal of Probability and Statistics
The Scientific World Journal
International Journal of Differential Equations
International Journal of Combinatorics
Advances in Mathematical Physics
Journal of Complex Analysis
Journal of Mathematics
Mathematical Problems in Engineering
Abstract and Applied Analysis
Discrete Dynamics in Nature and Society
International Journal of Mathematics and Mathematical Sciences
Journal of Discrete Mathematics
Journal of Function Spaces
International Journal of Stochastic Analysis
Journal of Optimization