Research Article

Stochastic Stabilization of Malware Propagation in Wireless Sensor Network via Aperiodically Intermittent White Noise

Xiaojing Zhong 1, Baihao Peng 1, Feiqi Deng 2, and Guiyun Liu 1

1 School of Mechanical and Electrical Engineering, Guangzhou University, Guangzhou 510006, China
2 School of Automation Science and Engineering, South China University of Technology, Guangzhou 510640, China

Correspondence should be addressed to Guiyun Liu; liugy@gzhu.edu.cn

Received 22 May 2020; Accepted 10 July 2020; Published 13 August 2020

Academic Editor: Shuping He

Copyright © 2020 Xiaojing Zhong et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

In this paper, we propose a novel heterogeneous model to describe the propagation dynamics of malware (viruses, worms, Trojan horses, etc.) in wireless sensor networks. Our model takes into consideration different battery-level sensor nodes contrary to existing models. In order to control the spread of malware, we design an aperiodically intermittent controller driven by white noise, which has striking advantages of lower cost and more flexible control strategy. We give a distinct condition on stability in probability one using graph-theoretical Lyapunov function and stochastic analysis method. Our results show that the nonlinear malware propagation system can be stabilized by intermittent stochastic perturbation under the intermittent time related to stochastic perturbation intensity. Our theoretical results can be applied to understand the observed mechanisms of malware and design interventions to control the spread of malware. Numerical simulations illustrate our analytical results clearly.

1. Introduction

With the improvement of wireless sensor technology, wireless sensor networks (WSNs) are used in many new scenarios: intelligent transportation network, water quality monitoring, military target detection, etc. Due to wireless feature and special structure of wireless sensor network, it is vulnerable to malware attack which can eavesdrop and paralyze the network [1–3]. Consequently, mathematical modeling and control strategies of malware propagation are of vital importance in order to predict its effects and defend it. In recent years, many scientific literatures have appeared, specifically, global model and the related global behaviour of WSNs by the concept of epidemiology. In the epidemic system, all people separate into different compartments such as $S$ (Susceptible), $E$ (Exposed), $I$ (Infectious), $R$ (Recovered), and so on. Toutonji et al. [4] proposed a VEIS-V worm attack propagation model which considers security countermeasures during worm attack. Bimal and Keshri [5] established a SEIRSV model by introducing a maintenance mechanism to sleep nodes. Zhu and Zhao [6] considered a SIR model which has logistic growth. Wang et al. [7] proposed a SCI model to describe the propagation dynamics of mobile sensor worm.

However, the above global models cannot cover individual feature and capability. In this sense, individual-based model will be more accurate to model malware propagation since it values individual diversity and derives both malware relationship and individual feature from malware propagation. Under the framework of heterogeneous complex network theory, the connection topology of nodes can be defined by node degree and the related degree distribution. Several complex network models have been studied for the epidemic model [8–11], alcoholism model [12], information spreading model [13–17], etc. But for wireless sensor network, there are few achievements: del Rey et al. [18] established heterogeneous SIS and SIR models for malware propagation in WSNs; all nodes are separated into three
compartments based on the classic SIR epidemic model. Li et al. [19] considered a SIR network malware propagation model; Li’s SIR model is different from del Rey’s heterogeneous model which considers tree-based networks. Inspired by stifler state in the rumor spreading model, Hosseini and Azgomi [20] proposed a SEIRS model. They assumed that nodes could be vaccinated and immunized to the malware infection. All of the above models did not consider sensor’s energy consumption, which affects seriously the information transmission quality. Nodes may not have enough energy to propagate malware by sending information to their neighbors. Proceeding from this angle, infected state should be separated into infected state with high capacity level and infected state with low capacity level.

It is worth to mention that most of the results concentrate on dynamic analysis of the deterministic model (global or individual-based model) by the basic reproduction number $R_0$, which is calculated by the next generation matrix method. But there are rare results on malware control strategies if malware becomes endemic ($R_0 > 1$).

As is well known, stochastic noises can stabilize an unstable system [21–27]. Its application extends to many practical areas, such as sleep improvement, tone discrimination [28], and financial stability [21, 23]. From the consideration of reducing control cost and control time, discontinuous controllers have been designed to stabilize a given system such as feedback control [29–32], pinning control [33], impulsive control [34], adaptive control [35–40], and intermittent control [41–44]. As for intermittent control, control time is divided into periodic and aperiodic type. Periodically intermittent control has been studied by many authors especially in synchronization problems. Zhang et al. [41] designed a periodically intermittent linear controller driven by white noises to stabilize an unstable memristor-based system. As Liu and Chen [45, 46] have mentioned before, the requirement of periodicity is unusual in real world application, while aperiodically intermittent control strategy needs a complex management to study the dynamic behaviour of the controlled system. We highlight Liu and Chen [45, 46] who investigated aperiodically intermittent deterministic controller for complex coupled deterministic system, and sufficient conditions have been given to guarantee global synchronization.

Stochastic control has been proved to be sufficiently useful in many fields. But for the best of our knowledge, there is no work on aperiodically intermittent stochastic stabilization for malware propagation; the application on malware propagation needs to be explored. This motivates us to investigate this kind of scheme oriented to the security issue for WSNs. In this paper, we will design an aperiodically intermittent stochastic noise controller to control malware spreading. The control intensity expression reflects the relationship between system parameters and network topological structure. In Section 4, numerical simulations of the proposed model are given to show the power of aperiodically intermittent noise controller. Finally, we conclude the paper in Section 5.

2. Model Formulation

According to topological structures of WSNs, all nodes partition into $n$ groups based on different nodal degrees. Each group $i$ is further compartmentalized into four states:

(i) Susceptible ($S_2$): the nodes in this state are prone to being infected by the implantation of malware and will become an infected one if it connects to an infected node.

(ii) Infectious with high energy level ($I_2^H$): the nodes in this state have already been infected by malware successfully and have stored up enough energy to continue propagating the malware.

(iii) Infectious with low energy level ($I_2^L$): the nodes in this state have already been infected by malware successfully but do not have sufficient energy to propagate malware by sending information to their neighbors.

(iv) Antimalware program activated ($A_i$): when nodes in state $I_2^H$ and state $I_2^L$ are detected to be infected, the nodes will activate antimalware program to clear up the infection. The node activated by the antimalicious program will no longer be invaded by the same malware.

Based on the sensor features and transition characters, the malware propagation process is described as follows: when a susceptible node connects to an infected node, the susceptible node with high energy level becomes an infected node with probability $\beta_2$, and the susceptible with low energy level node becomes an infected node with probability $\beta_3$. Both the contact rates $\beta_2$ and $\beta_3$ are positive constants. The malware itself will not cause additional cost to infected node. The infected node with low energy level can become infected
node with high level if it is recharged, and the charge rate is a positive constant $\gamma$. The influence of the malware on the natural mortality rate of infected nodes should be ignored and nodes in four states are assigned equal natural mortality rate $\eta$ which satisfies $\eta \geq 0$. Figure 1 shows state transition diagram of the model.

Thus, our model can be formulated by the following ordinary differential equations:

$$
\begin{align*}
S_i(t)' &= \Lambda - \beta_1 i \Theta(t) S_i(t) - \beta_2 i \Theta(t) S_i(t) - \eta S_i(t), \\
I_i^h(t)' &= \beta_1 i \Theta(t) S_i(t) - \gamma I_i^h(t) - \mu_1 I_i^h(t) - \eta I_i^h(t), \\
I_i^p(t)' &= \beta_2 i \Theta(t) S_i(t) + \gamma I_i^p(t) - \mu_2 I_i^p(t) - \eta I_i^p(t), \\
A_i(t)' &= \mu_1 I_i^h(t) + \mu_2 I_i^p(t) - \eta A_i(t),
\end{align*}
$$

(1)

with initial values

$$
\begin{align*}
S_i(0) &\geq 0, \\
I_i^h(0) &\geq 0, \\
I_i^p(0) &\geq 0, \\
A_i(0) &\geq 0,
\end{align*}
$$

(2)

where $i = 1, \ldots, n$, represents the nodal degree. $\Theta(t)$ represents the probability that an edge connects to an infectious sensor node at time $t$. Its expression is

$$
\Theta(t) = \frac{1}{\langle j \rangle} \sum_{j=1}^{n} j p(j) \frac{N_j^h(t)}{N_i(t)},
$$

(3)

where $\langle j \rangle = \sum_{j=1}^{n} j p(j)$ represents the average nodal degree. $p(j)$ represents the probability that a randomly chosen sensor node has degree $j$, $\sum_{j=1}^{n} p(j) = 1$. Obviously, for all $i$ and $t \geq 0$,

$$
N_i(t) = S_i(t) + I_i^h(t) + I_i^p(t) + A_i(t) = \frac{\Lambda}{\eta}.
$$

(4)

Then, we can deduce system (1) into

$$
\begin{align*}
S_i(t)' &= \Lambda - \beta_1 i \Theta(t) S_i(t) - \beta_2 i \Theta(t) S_i(t) - \eta S_i(t), \\
I_i^h(t)' &= \beta_1 i \Theta(t) S_i(t) - \gamma I_i^h(t) - \mu_1 I_i^h(t) - \eta I_i^h(t), \\
I_i^p(t)' &= \beta_2 i \Theta(t) S_i(t) + \gamma I_i^p(t) - \mu_2 I_i^p(t) - \eta I_i^p(t), \\
A_i(t)' &= \mu_1 I_i^h(t) + \mu_2 I_i^p(t) - \eta A_i(t),
\end{align*}
$$

(5)

About the dynamic behaviour of the above deterministic model (5), we give the following corollary.

**Corollary 1.** Define

$$
R_0 = \frac{[\beta_1 y + \beta_2 (y + \mu_1 + \eta)] \langle j \rangle}{(\eta + \mu_2)(y + \eta + \mu_1) \langle j \rangle}.
$$

(6)

(1) If $R_0 < 1$, the malware-free equilibrium is globally asymptotically stable.

(2) If $R_0 > 1$, there is an endemic equilibrium, and it is persistent.

**Remark 1.** The threshold is obtained by $R_0 = ((\beta_1 y + \beta_2 (y + \mu_1 + \eta)) \langle j \rangle) / (\eta + \mu_2)(y + \eta + \mu_1) \langle j \rangle)$, which depends on the fluctuations of the degree distribution and system parameters. Since malware will die out when $R_0 < 1$, malware prevention measures can be designed to decrease $R_0$, such as decreasing node connectivity to decrease the contact rates $\beta_1, \beta_2$ and increasing monitoring efforts on infective nodes to increase the detect rate $\mu_2$.

### 3. Control Strategy

In this section, we mainly concentrate on the control strategy of malware propagation. In the context of aperiodically intermittent stochastic noise stabilization of the complex heterogeneous network system, we propose a design procedure for the noise control input to stabilize system (5). At first, we consider a stochastic noise driven by Brownian motions and a g-type structure of the controller. The controller’s mathematical expression is $g(t, x(t))B(t)$, where $B(t)$ is a 3$n$-dimensional Brownian motion corresponding to system variables and $B(t)$ is the related white noise. To be flexible and to save cost, we design the control time as aperiodically intermittent type, which admits uncertain rest times. We give a sketch of aperiodically intermittent control strategy in Figure 2, under the perturbation of g-type; the time span $[t_k, t_{k+1})$ contains the work time $[t_k, t_k + c_k]$ and the rest time $[t_k + c_k, t_{k+1})$, and $c_k$ denotes the k-th noise width. Naturally, the noise widths satisfy $0 \leq c_k \leq t_{k+1} - t_k$.

The stochastic control input system is

$$
dx(t) = f(t, x(t))dt + g(t, x(t))dB(t),
$$

(7)

where
with $i, k \in N, g_i: (t_0, \infty) \times \mathbb{R}^n \rightarrow \mathbb{R}^{n \times m}$. For the aperiodically intermittent perturbation strategy, the start time and the noise width might be different, but the total perturbation time ratio should be fixed in the long term. Mathematically, there exists a positive scalar $\tau$, such that the above time nodes satisfy the following assumption:

$$\lim_{t \to \infty} \frac{\sum_{k=0}^{n-1} c_k}{t_{m+1} - t_0} = \tau. \quad (9)$$

We call $\tau$ as the control time ratio. Moreover, we assume $g(t, 0) \equiv 0$ for stochastic stability analysis, which guarantees the existence of a trivial solution $x(t, t_0, 0) \equiv 0$.

**Theorem 1.** If the aperiodically perturbed intensity $\sigma$ satisfies $\sigma^2 > (\mathbb{E}[(2[\beta_1, \beta_2 (y + \mu_1 + \eta) \mathbb{E}(j^2)]/\mathbb{E}(y + \mu_1 + \eta))(j)]) - (2(\eta + \mu_2)/\tau)$, then the infected nodes will die out with probability one.

**Proof.** Define a matrix $M$:

$$M = \begin{bmatrix}
\beta_1 \mathbb{E}(j) & \mathbb{E}(j^2)
\end{bmatrix}$$

$(10)$

We can calculate that $\rho(M) = (|\beta_1| + \beta_2(y + \mu_1 + \eta) \mathbb{E}(j^2))/(y + \mu_1 + \eta) \mathbb{E}(j)$. Let $\omega = (\omega_1, \omega_2, \ldots, \omega_n)$ be the eigenvector of $M$ corresponding to $\rho(M)$; then, we have

$$\omega_1 > 0, i = 1, 2, \ldots, n. \text{ Define a Lyapunov function:}$$

$$V(t_1, t_2, t_3, \ldots, t_n, \eta) = \omega^T \mathbb{E} \omega, \quad (12)$$

where

$$\omega_i > 0,$$
where $E$ represents an elementary matrix or an identity matrix. By condition (11), the above inequation becomes

$$\int_{t_0}^{t} J V(\omega(s))ds \leq \int_{t_0}^{t} \left[ a(\rho(M) - \mu_2 - \eta)(\omega(s))^p dt + \int_{t_0}^{t} \frac{a(a - 1)(\omega(s))^{-2}}{2} Tr\left[ \Phi_1^{T}(\omega)\Phi_1(\omega) \right] dt. \right.$$ 

Then, we discuss the time $t$ in different time intervals. Obviously, there exists one positive integer $m$ such that $t \in [t_m, t_{m+1})$.

(1) If $t \in [t_m, t_m + c_m)$, then

$$\int_{t_0}^{t} \frac{a(a - 1)(\omega(s))^{-2}}{2} Tr\left[ \Phi_1^{T}(\omega)\Phi_1(\omega) \right] dt = \int_{t_0}^{t_0 + c_m} \frac{a(a - 1)(\omega(s))^{-2}}{2} Tr\left[ \Phi_1^{T}(\omega)\Phi_1(\omega) \right] dt + 0$$

$$+ \int_{t_0 + c_m}^{t} \frac{a(a - 1)(\omega(s))^{-2}}{2} Tr\left[ \Phi_1^{T}(\omega)\Phi_1(\omega) \right] dt + 0 + \ldots$$

$$= \int_{t_0}^{t_0 + c_m} \frac{a(a - 1)(\omega(s))^{-2}}{2} Tr\left[ \Phi_1^{T}(\omega)\Phi_1(\omega) \right] dt + 0 + \int_{t_0 + c_m}^{t} \frac{a(a - 1)(\omega(s))^{-2}}{2} Tr\left[ \Phi_1^{T}(\omega)\Phi_1(\omega) \right] dt + 0 + \ldots$$

which means

$$\int_{t_0}^{t} J V(\omega(s))ds = \int_{t_0}^{t_0 + c_m} \left[ \rho(M) - \mu_2 + \frac{1}{2}(a - 1)(a - 1)^p dt \right.\left. a(\omega(s))^p dt + \int_{t_0 + c_m}^{t} \left[ \rho(M) - \mu_2 + \frac{1}{2}(a - 1)(a - 1)^p \right] a(\omega(s))^p dt + \ldots \right.$$ 

(2) If $t \in [t_m + c_m, t_{m+1})$, then

$$\int_{t_0}^{t} \frac{a(a - 1)(\omega(s))^{-2}}{2} Tr\left[ \Phi_1^{T}(\omega)\Phi_1(\omega) \right] dt = \int_{t_0}^{t_0 + c_m} \frac{a(a - 1)(\omega(s))^{-2}}{2} Tr\left[ \Phi_1^{T}(\omega)\Phi_1(\omega) \right] dt + 0$$

$$+ \int_{t_0 + c_m}^{t} \frac{a(a - 1)(\omega(s))^{-2}}{2} Tr\left[ \Phi_1^{T}(\omega)\Phi_1(\omega) \right] dt + 0 + \ldots$$

$$= \int_{t_0}^{t_0 + c_m} \frac{a(a - 1)(\omega(s))^{-2}}{2} Tr\left[ \Phi_1^{T}(\omega)\Phi_1(\omega) \right] dt + 0 + \int_{t_0 + c_m}^{t} \frac{a(a - 1)(\omega(s))^{-2}}{2} Tr\left[ \Phi_1^{T}(\omega)\Phi_1(\omega) \right] dt + 0 + \ldots$$

$$+ \int_{t_0 + c_m}^{t} \frac{a(a - 1)(\omega(s))^{-2}}{2} Tr\left[ \Phi_1^{T}(\omega)\Phi_1(\omega) \right] dt + 0,$$
which means

\[
\int_{t_0}^{t} LV(\bar{\omega}(s))ds = \int_{t_0}^{t} \left[ \rho(M) - \eta - \mu_2 + \frac{1}{2} (a - 1)\sigma^2 \right] a(\bar{\omega} \bar{y})^a dt \\
+ \int_{t_0}^{t_1} \left[ \rho(M) - \eta - \mu_2 \right] a(\bar{\omega} \bar{y})^a dt + \int_{t_1}^{t_2} \left[ \rho(M) - \eta - \mu_2 + \frac{1}{2} (a - 1)\sigma^2 \right] a(\bar{\omega} \bar{y})^a dt \\
+ \int_{t_2}^{t_3} \left[ \rho(M) - \eta - \mu_2 \right] a(\bar{\omega} \bar{y})^a dt + \cdots + \int_{t_{m-1}}^{t_m} \left[ \rho(M) - \eta - \mu_2 + \frac{1}{2} (a - 1)\sigma^2 \right] a(\bar{\omega} \bar{y})^a dt \\
+ \int_{t_m}^{t} \left[ \rho(M) - \eta - \mu_2 \right] a(\bar{\omega} \bar{y})^a dt
\]

\[
\leq \sup_{t_0 \leq s \leq t} (\bar{\omega} \bar{y})^a \left[ \rho(M) - \eta - \mu_2 \right] (t - t_0) + \frac{1}{2} (a - 1) \left( \sigma^2 \sum_{i=0}^{m} c_i \right) .
\]

Comparing Case (1) and Case (2), we can conclude for \( t_m \leq t < t_{m+1} \) that

\[
(\bar{\omega} \bar{y})^a \leq (\bar{\omega} \bar{y})_0)^a + \sup_{t_0 \leq s \leq t} (\bar{\omega} \bar{y})^a \left[ \rho(M) - \eta - \mu_2 \right] (t_m + t_0) + \frac{1}{2} (a - 1) \left( \sigma^2 \sum_{i=0}^{m} c_i \right) \\
+ \int_{t_0}^{t} a(\bar{\omega} \bar{y})^{a-1} \bar{\omega} \bar{y} dB(s).
\]

Taking the expectation on both sides of the above inequation gives

\[
E(\bar{\omega} \bar{y})^a \leq (\bar{\omega} \bar{y}_0)^a + E \sup_{t_0 \leq s \leq t} (\bar{\omega} \bar{y})^a \left[ \rho(M) - \eta - \mu_2 \right] (t_{m+1} + t_0) + \frac{1}{2} (a - 1) \left( \sigma^2 \sum_{i=0}^{m} c_i \right) \\
= (\bar{\omega} \bar{y}_0)^a + a E \left( \sup_{t_0 \leq s \leq t} (\bar{\omega} \bar{y})^a \right) \left[ \rho(M) - \eta - \mu_2 \right] (t_{m+1} + t_0) + \frac{1}{2} (a - 1) \left( \sigma^2 \sum_{i=0}^{m} c_i \right) \\
= (\bar{\omega} \bar{y}_0)^a + a (t_{m+1} + t_0) \left( \rho(M) - \eta - \mu_2 \right) + \frac{1}{2} (a - 1) \sigma^2 \tau_m E \left( \sup_{t_0 \leq s \leq t} (\bar{\omega} \bar{y})^a \right) \\
= (\bar{\omega} \bar{y}_0)^a + \zeta_{m,a} E \left( \sup_{t_0 \leq s \leq t} (\bar{\omega} \bar{y})^a \right),
\]

where \( \zeta_{m,a} = a(t_{m+1} + t_0) \left( \rho(M) - \eta - \mu_2 \right) + (1/2) (a - 1)\sigma^2 \tau_m \). Since \( \lim_{m \to \infty} \tau_m = \tau \), there exists a positive integer \( m_0 \) such that when \( m > m_0 \),

\[
1 - \zeta_{m,a} \geq \left( \rho(M) - \eta - \mu_2 \right) \left( 1 - \zeta_{m,a} \right) \leq (\bar{\omega} \bar{y}_0)^a,
\]

which implies

\[
E(\|\bar{x}\|^a) \leq E(\bar{\omega} \bar{y})^a \leq (\bar{\omega} \bar{y}_0)^a, \quad \zeta_{m,a} \leq (\bar{\omega} \bar{y}_0)^a,
\]

where \( \xi = \min \{ (\gamma/\alpha + \eta + m + \mu_i) \omega + \mu_i \} \).

By Chebyshev's inequality, for any \( \varepsilon > 0 \), we have

\[
P(\|\bar{x}\| \geq \varepsilon) \leq E(\|\bar{\omega} \bar{y}\|^a) \leq \frac{(\bar{\omega} \bar{y}_0)^a}{\varepsilon^a}.
\]

If \( (\rho(M) - \eta - \mu_2) + (1/2) (a - 1)\sigma^2 \tau_m < 0 \), from the definition of \( \zeta_{m,a} \), we can obtain \( \zeta_{m,a} \to -\infty \) when \( m \to \infty \). Consequently, we have
\begin{align}
\lim_{t \to \infty} P[\|x\| \geq \epsilon] &\leq \lim_{t \to \infty} \frac{(\omega x_0)^a}{(\epsilon \xi)^a (1 - \tau_{ma})} \\
&= \lim_{t \to \infty} \frac{(\omega x_0)^a}{(\epsilon \xi)^a (1 - \tau_{ma})} = 0.
\end{align}

Then, we deduce that

\[ P\left( \lim_{t \to \infty} \|x\| \geq \epsilon \right) = 0. \tag{28} \]

Since \( \epsilon \) is arbitrary, we obtain

\[ P\left( \lim_{t \to \infty} \|x\| = 0 \right) = 1. \tag{29} \]

Then, sending \( a \to 0 \), we obtain the minimum control intensity expression:

\[ \sigma^2 = \frac{2(\beta_1 y + \beta_2 (y + \mu_1 + \eta))}{\tau (y + \mu_1 + \eta)} \langle j^2 \rangle - \frac{2(\eta + \mu_2)}{\tau^2} \tag{30} \]

Therefore, system (7) is almost surely stable if \( \sigma^2 \) is bigger than the minimum control intensity. The proof is complete.

In Theorem 1, we give the global stability of the malware-free equilibrium. It is worth to mention that we separate interaction terms in the stochastic model (7) by using the group-theoretic approaching method, and then the infected groups \( I_i^L(t) \) and \( I_i^H(t) \) can be considered separately. Calculating the Lyapunov exponents, we obtain the global stability of the malware-free equilibrium. \( \square \)

**Proof of Corollary 1.** Set \( \sigma = 0 \); then, stochastic model (7) becomes deterministic model (5). The control intensity mathematical expression becomes

\[ 0 > \frac{2[\beta_1 y + \beta_2 (y + \mu_1 + \eta)]}{\tau (y + \mu_1 + \eta)} \langle j^2 \rangle - \frac{2(\eta + \mu_2)}{\tau^2} \tag{31} \]

It implies

\[ \frac{2T[\beta_1 y + \beta_2 (y + \mu_1 + \eta)]}{\delta (y + \mu_1 + \eta)} \langle j^2 \rangle > \frac{2(\eta + \mu_2)}{\tau^2}, \tag{32} \]

which means \( R_0 < 1 \). Applying Theorem 1, the malware-free equilibrium is globally asymptotically stable.

To get the endemic equilibrium solution \( S_i^* + I_i^L^* + I_i^H^* + A_i^* \), the right side of system (1) should equal to zero. The solution definitely satisfies the restrictive condition on the total quality of nodes:

\[ S_i^* + I_i^L^* + I_i^H^* + A_i^* = \frac{\Lambda}{\eta}, \quad \text{for all } i. \tag{33} \]

Combining and solving all the above equations, we can obtain an equation containing \( \Theta(t) \) and \( S_i^*, I_i^L^*, I_i^H^*, A_i^* \). To guarantee a nontrivial solution of it, \( R_0 \) need to be bigger than one, and thus we obtain that there is an endemic equilibrium when \( R_0 > 1 \).

Then, we prove the malware will be persistent when \( R_0 > 1 \). If \( R_0 > 1 \), the derivative of function \( V \) becomes positive for \( S_i(t) \) \((i = 1, 2, \ldots, n)\) sufficiently close to \( \Lambda/\eta \) except when \( I_i^L = I_i^H = 0 \) \((i = 1, 2, \ldots, n)\). Otherwise, system (1) reduces to \( dS_i = \Lambda - \eta S_i \delta_i \), which implies \( S_i \to (\Lambda/\eta) \) as \( t \to \infty \). This establishes the malware-free equilibrium's unstable property. Since the necessary and sufficient condition for uniform persistence is equivalent to the malware-free equilibrium being unstable, system (1) is persistent. \( \square \)

**Remark 2.** If \( t_{k+1} - t_k = T \) and \( c_k = \delta \) for all \( k \in \mathbb{N} \), system (7) becomes a periodic intermittent system. The minimum control intensity becomes

\[ \sigma^2 > \frac{2T[\beta_1 y + \beta_2 (y + \mu_1 + \eta)]}{\delta (y + \mu_1 + \eta)} \langle j^2 \rangle - \frac{2T(\eta + \mu_2)}{\delta^2}. \tag{34} \]

This agrees with Theorem 1 in Zhang et al. [41]. Our results can be regarded as a generalization of Zhang et al. [41].

**Remark 3.** According to the expression of \( \sigma \), the control intensity depends on the network topological structure and system parameters. Apparently, if the degree distribution of WSNs follows a power law (like a scale-free network) and the number of nodes is huge enough, then \( \langle j^2 \rangle / \langle j \rangle \to \infty \), so the absence of control intensity, i.e., \( \sigma \to \infty \), is observed. Moreover, the disappearance of malware is related to perturbation time ratios \( \tau \). Thus, we can enhance or weaken noise intensity to decrease or increase the corresponding control time ratios. Control strategy would be designed based on our theoretical results.

### 4. Numerical Simulation

The aperiodically intermittent noise controller can stabilize system (1) under the intensity \( \sigma \). From the expression, control intensity is directly proportional to the contact rates \( \beta_1, \beta_2 \) and inversely proportional to the control time ratio. Using Milstein’s higher order method [47], the discretized equations for the system (7) are

\begin{align}
I_{i,k+1}^L &= I_{i,k}^L + \left( \beta_1 \Theta(t) S_i - \gamma I_{i,k}^L(t) - \mu_1 I_{i,k}^L(t) - \eta I_{i,k}^H(t) \right) \Delta t + \sigma I_{i,k}^I \sqrt{\Delta t} \xi_i + \frac{1}{2} \sigma^2 (I_{i,k}^I)^2 (\xi_i^2 - 1) \Delta t, \\
I_{i,k+1}^H &= I_{i,k}^H + \left( \beta_2 \Theta(t) S_i + \gamma I_{i,k}^L(t) - \mu_2 I_{i,k}^H(t) - \eta I_{i,k}^H(t) \right) \Delta t + \sigma I_{i,k}^I \sqrt{\Delta t} \xi_i + \frac{1}{2} \sigma^2 (I_{i,k}^I)^2 (\xi_i^2 - 1) \Delta t, \\
A_{i,k+1} &= A_{i,k} + \left( \mu_1 I_{i,k}^L(t) + \mu_2 I_{i,k}^H(t) - \eta A_i \right) \Delta t + A_{i,k} \sqrt{\Delta t} \xi_i + \frac{1}{2} \sigma^2 A_{i,k} (\xi_i^2 - 1) \Delta t,
\end{align}
where $\xi_i$ are independent random variables $N(0, 1)$, $i = 1, 2, \ldots, n$. Generally, we assume WSN is a scale-free network with the power law distribution $P(j) = aj^{-\gamma}$, where $a$ satisfies $\sum_{j=1}^{\infty} aj^{-\gamma} = 1$. We set the initial values to $S_i(0) = 900$, $I^H_i(0) = 50$, $I^B_i = 50$, $A_i = 0$, $i = 1, 2, \ldots, n$ and $n = 50$.

Choosing parameter values in Table 1, the reproduction number is

$$R_0 = \frac{\beta_1 \gamma + \beta_2 (\gamma + \mu_1 + \eta) \langle j^2 \rangle}{(\eta + \mu_2) (\gamma + \eta + \mu_1) \langle j \rangle} = 3.2678 > 1.$$  \hspace{1cm} (36)

According to Corollary 1, the malware is persistent. The top two pictures in Figure 3 show that the solution of system (1) converges to the endemic equilibrium. The last two pictures in Figure 3 show clearly that the number of infected nodes $I^H_k$ and $I^B_k$ converge to a positive constant.

To stabilize the above deterministic model, we choose different control intensities $\sigma$ by adjusting control time to compare the stabilization effects.

(i) Let control time ratio $\tau = 0.5$ and initial value (900, 50, 50, 0, $\ldots$, 900, 50, 50, 0). Generating the
Figure 4: The time series and orbits of system (7) with $R_0 > 1$ and stochastic control. The top two pictures are the sample paths of $S_{15}(t), I_{15}(t), A_{15}(t)$ and $S_{35}(t), I_{35}(t), A_{35}(t)$. The middle pictures are two different time strategies with $\tau = 0.5$ and $\sigma = 0.2$. The last two pictures are sample paths of $I^L(t)$ and $I^H(t)$ with degree $k = 5, 15, 25, 35, 40, 45$. The malware will be extinct in the end.
Figure 5: The time series and orbits of system (7) with $R_0 > 1$ and stochastic control. The top two pictures are the sample paths of $S_{15}(t), I^H_{15}(t), A_{15}(t)$ and $S_{35}(t), I^H_{35}(t), A_{35}(t)$. The middle pictures are two different time strategies with $\tau = 0.8$ and $\sigma = 0.2$. The last two pictures are sample paths of $I^S(t)$ and $I^H(t)$ with degree $k = 5, 15, 25, 35, 40, 45$. The malware will be extinct in the end.
aperiodically intermittent time intervals randomly, we give two examples in the middle two pictures of Figure 4. We can calculate that $\sigma^2 = 0.04 > 0.0254$; according to Theorem 1, $I^H_k$ and $I^L_k$ all tend to zero; Figure 4 shows clearly that the malware disappears. (ii) Increase the control time ratio to $\tau = 0.8$; specific aperiodically intermittent time intervals are shown in the middle two pictures of Figure 5. We can obtain that $\sigma^2 = 0.04 > 0.0211$, the condition in Theorem 1 is satisfied, and $I^H_k$ and $I^L_k$ all tend to zero. The top two and the last two pictures of Figure 5 show clearly that all the infected nodes go to zero. (iii) Adding control time to full time. Figure 6 shows the solution of system (7) converges to the malware-free equilibrium, $I^H_k$ and $I^L_k$ all tend to zero, and the malware nodes will disappear. Comparing Figures 4–6, we can conclude that the bigger the perturbation intensity is, the faster the steady speed is.

5. Conclusion

Based on network topology and malware propagation property, we established a heterogeneous wireless sensor network model which considers the influence of energy consumption to node communication. The basic reproduction number $R_0$ has been given which determines the extinction or persistence of malware: if $R_0 < 1$, the malware will die out; if $R_0 > 1$, the malware will be persistent. To control malware spreading, we design a kind of aperiodically
intermittent stochastic noise controller, starting time and control length of which are arbitrary. We can control steady rate autonomously by adjusting the work width. Using the straightening operator and Markov inequality, we calculate the specific stochastic noise intensity \( \sigma \), which is inversely proportional to intermittent time. When stochastic noise controller’s intensity is greater than \( \sigma \), malware propagation will be controlled with probability 1. Otherwise, the malware program will destroy the wireless sensor networks. This stochastic stabilization method presents a new theoretical strategy for wireless sensor network security: stochastic noise controller. Numerical simulations are given to illustrate the stabilization effect of stochastic noise.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This study was supported by the Guangzhou Education Bureau science foundation project (1201630502) and Research Fund for Guangzhou University (YG2020010).

References

[1] E. Fadel, V. C. Gungor, L. Nassef et al., “A survey on wireless sensor networks for smart grid,” Computer Communications, vol. 71, pp. 22–33, 2015.
[2] A. M. del Rey and A. Peinado, “Mathematical models for malware propagation in wireless sensor networks: an analysis,” in Computer and Network Security Essentials, K. Daimi, Ed., Springer, Cham, Switzerland, pp. 299–313, 2018.
[3] V. Karyotis and M. H. R. Khouzani, Malware Diffusion Models for Modern Complex Networks: Theory and Applications, Morgan Kaufmann, Burlington, MA, USA, 2016.
[4] O. A. Toutonji, S.-M. Yoo, and M. Park, “Stability analysis of VEISV propagation modeling for network worm attack,” Applied Mathematical Modelling, vol. 36, no. 6, pp. 2751–2761, 2012.
[5] K. M. Bimal and N. Keshri, “Mathematical model on the transmission of worms in wireless sensor network,” Applied Mathematical Modelling, vol. 37, no. 6, pp. 4103–4111, 2013.
[6] L. Zhu and H. Zhao, “Dynamical analysis and optimal control for a malware propagation model in an information network,” Neurocomputing, vol. 149, pp. 1370–1386, 2015.
[7] T. Wang, Q. Wu, S. Wen et al., “Propagation modeling and defending of a mobile sensor worm in wireless sensor and actuator networks,” Sensors, vol. 17, no. 12, pp. 139–156, 2017.
[8] P. S. Romualdo and V. Alessandro, “Epidemic spreading in scale-free networks,” Physical Review Letters, vol. 86, no. 14, pp. 3200–3203, 2000.
[9] S. Huang, F. Chen, and L. Chen, “Global dynamics of a network-based SIQRS epidemic model with demographics and vaccination,” Communications in Nonlinear Science and Numerical Simulation, vol. 43, pp. 296–310, 2017.
[10] G. Zhu, X. Fu, and G. Chen, “Spreading dynamics and global stability of a generalized epidemic model on complex heterogeneous networks,” Applied Mathematical Modelling, vol. 36, no. 12, pp. 5808–5817, 2012.
[11] G. Zhu, G. Chen, and X. Fu, “Effects of active links on epidemic transmission over social networks,” Physica A: Statistical Mechanics and Its Applications, vol. 468, pp. 614–621, 2017.
[12] H. Xiang, Y.-P. Liu, and H.-F. Huo, “Stability of an SAIRS alcoholism model on scale-free networks,” Physica A: Statistical Mechanics and Its Applications, vol. 473, pp. 276–292, 2017.
[13] T. Li, X. Liu, J. Wu, C. Wan, Z.-H. Guan, and Y. Wang, “An epidemic spreading model on adaptive scale-free networks with feedback mechanism,” Physica A: Statistical Mechanics and Its Applications, vol. 450, pp. 649–656, 2016.
[14] X. Liu, T. Li, H. Xu, and W. Liu, “Spreading dynamics of an online social information model on scale-free networks,” Physica A: Statistical Mechanics and Its Applications, vol. 514, pp. 497–510, 2019.
[15] W. Liu, T. Li, X. Liu, and H. Xu, “Spreading dynamics of a word-of-mouth model on scale-free networks,” IEEE Access, vol. 6, pp. 65563–65572, 2018.
[16] Y. Lei, T. Li, Y. Wang, G. Ye, S. Sun, and Z. Xia, “Spreading dynamics of a CPFB group booking preferential information model on scale-free networks,” IEEE Access, vol. 7, pp. 156287–156300, 2019.
[17] X. D. Liu, T. Li, X. Cheng, W. Liu, and H. Xu, “Spreading dynamics of a preferential information model with hesitation psychology on scale-free networks,” Advances in Difference Equations, vol. 2019, pp. 1–13, 2019.
[18] A. M. del Rey, J. D. H. Guillen, and G. R. Sánchez, “Modeling malware propagation in wireless sensor networks with individual-based models,” in Advances in Artificial Intelligence, vol. 9868, pp. 194–203, Springer, Cham, Switzerland, 2016.
[19] Q. Li, B. Zhang, L. Cui, Z. Fan, and V. V. Athanasios, “Epidemics on small worlds of tree-based wireless sensor networks,” Journal of Systems Science and Complexity, vol. 27, no. 6, pp. 1095–1120, 2014.
[20] S. Hosseini and M. A. Azgomi, “A model for malware propagation in scale-free networks based on rumor spreading process,” Computer Networks, vol. 108, pp. 97–107, 2016.
[21] R. Khasminskii, “Stochastic stability of differential equations,” in Stieltjes & Noordhoff, Springer, Berlin, Germany, 1980.
[22] L. Arnold, H. Crauel, and V. Wihstutz, “Stabilization of linear systems by noise,” SIAM Journal on Control and Optimization, vol. 21, no. 3, pp. 451–461, 1983.
[23] X. R. Mao, Stochastic Differential Equations and Applications, Woodhead Publishing, Cambridge, UK, 2nd edition, 2008.
[24] L. Huang, “Stochastic stabilization and destabilization of nonlinear differential equations,” Systems & Control Letters, vol. 62, no. 2, pp. 163–169, 2013.
[25] T. Caraballo, A. Settati, M. E. Fatini, A. Lahrouz, and A. Imlahi, “Global stability and positive recurrence of a stochastic SIS model with lévy noise perturbation,” Physica A: Statistical Mechanics and Its Applications, vol. 523, pp. 677–690, 2019.
[26] L. Liu and T. Caraballo, “Analysis of a stochastic 2D-navier-stokes model with infinite delay,” Journal of Dynamics and Differential Equations, vol. 31, no. 4, pp. 2249–2274, 2019.
[27] T. Caraballo, R. Colucci, J. López-de-la-Cruz, and A. Rapaport, “A way to model stochastic perturbations in population dynamics models with bounded realizations,” Communications in Nonlinear Science and Numerical Simulation, vol. 77, pp. 239–257, 2019.
[28] R. K. Christensen, H. Lindén, M. Nakamura, and T. R. Barkat, "White noise background improves tone discrimination by suppressing cortical tuning curves," Cell Reports, vol. 29, no. 7, pp. 2041–2053, 2019.
[29] W. Chen, S. Xu, and Y. Zou, "Stabilization of hybrid neutral stochastic differential delay equations by delay feedback control," Systems & Control Letters, vol. 88, pp. 1–13, 2016.
[30] Q. Zhu and Q. Zhang, "Pth moment exponential stabilisation of hybrid stochastic differential equations by feedback controls based on discrete-time state observations with a time delay," IET Control Theory & Applications, vol. 11, no. 12, pp. 1992–2003, 2017.
[31] G. Song, B.-C. Zheng, Q. Luo, and X. Mao, "Stabilisation of hybrid stochastic differential equations by feedback control based on discrete-time observations of state and mode," IET Control Theory & Applications, vol. 11, no. 3, pp. 301–307, 2017.
[32] R. Yong, W. S. Yin, and R. Sakthivel, "Stabilization of stochastic differential equations driven by G-Brownian motion with feedback control based on discrete-time state observation," Automatica, vol. 95, pp. 146–151, 2018.
[33] H. Ren, Y. Peng, F. Deng, and C. Zhang, "Impulsive pinning control algorithm of stochastic multi-agent systems with unbounded distributed delays," Nonlinear Dynamics, vol. 92, no. 4, pp. 1453–1467, 2018.
[34] P. Cheng, F. Deng, and F. Yao, "Almost sure exponential stability and stochastic stabilization of stochastic differential systems with impulsive effects," Nonlinear Analysis: Hybrid Systems, vol. 30, pp. 106–117, 2018.
[35] Y.-J. Liu, S. Lu, D. Li, and S. Tong, "Adaptive controller design-based ABLF for a class of nonlinear time-varying state constraint systems," IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 47, no. 7, pp. 1546–1553, 2017.
[36] S. He, H. Fang, M. Zhang, F. Liu, and Z. Ding, "Adaptive optimal control for a class of nonlinear systems: the online policy iteration approach," IEEE Transactions on Neural Networks and Learning Systems, vol. 31, no. 2, pp. 549–558, 2020.
[37] S. He, H. Fang, M. Zhang, F. Liu, X. Luan, and Z. Ding, "Online policy iterative-based h optimization algorithm for a class of nonlinear systems," Information Sciences, vol. 495, no. 1, 2019.
[38] P. Cheng, J. Wang, S. He, X. Luan, and F. Liu, "Observer-based asynchronous fault detection for conic-type nonlinear jumping systems and its application to separately excited DC motor," IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 67, no. 3, pp. 1–12, 2020.
[39] P. Cheng and S. He, "Observer-based finite-time asynchronous control for a class of hidden Markov jumping systems with conic-type nonlinearities," IET Control Theory and Applications, vol. 14, no. 2, pp. 244–252, 2020.
[40] P. Cheng, S. He, J. Cheng, X. Luan, and F. Liu, "Asynchronous output feedback control for a class of conic-type nonlinear hidden markov jump systems within a finite-time interval," IEEE Transactions on Systems, Man, and Cybernetics: Systems, pp. 1–8. In press, 2020.
[41] B. Zhang, F. Deng, S. Peng, and S. Xie, "Stabilization and destabilization of nonlinear systems via intermittent stochastic noise with application to memristor-based system," Journal of the Franklin Institute, vol. 355, no. 9, pp. 3829–3852, 2018.
[42] S. Yang, C. Li, and T. Huang, "Exponential stabilization and synchronization for fuzzy model of memristive neural networks by periodically intermittent control," Neural Networks, vol. 75, pp. 162–172, 2016.
[43] G. Zhang and Y. Shen, "Exponential stabilization of memristor-based chaotic neural networks with time-varying delays via intermittent control," IEEE Transactions on Neural Networks and Learning Systems, vol. 26, no. 7, pp. 1431–1441, 2015.
[44] L. Liu, M. Perc, and J. Cao, "Aperiodically intermittent stochastic stabilization via discrete time or delay feedback control," Science China Information Sciences, vol. 62, no. 7, pp. 1–13, 2019.
[45] X. Liu and T. Chen, "Synchronization of nonlinear coupled networks via aperiodically intermittent pinning control," IEEE Transactions on Neural Networks and Learning Systems, vol. 26, no. 10, pp. 113–126, 2015.
[46] X. Liu and T. Chen, "Synchronization of complex networks via aperiodically intermittent pinning control," IEEE Transactions on Automatic Control, vol. 60, no. 2, pp. 3316–3321, 2015.
[47] D. J. Higham, "An algorithmic introduction to numerical simulation of stochastic differential equations," SIAM Review, vol. 43, no. 3, pp. 525–546, 2001.
[48] P. van den Driessche and J. Watmough, "Reproduction numbers and sub-threshold endemic equilibria for compartmental models of disease transmission," Mathematical Biosciences, vol. 180, no. 1-2, pp. 29–48, 2002.
[49] M. Y. Li and Z. Shuai, "Global-stability problem for coupled systems of differential equations on networks," Journal of Differential Equations, vol. 248, no. 1, pp. 1–20, 2010.