Modeling and analyzing malware diffusion in wireless sensor networks based on cellular automaton

Hong Zhang1, Shigen Shen2, Qiying Cao1, Xiaojun Wu3, and Shaofeng Liu1

Abstract
Wireless sensor networks, as a multi-hop self-organized network system formed by wireless communication, are vulnerable to malware diffusion by breaking the data confidentiality and service availability, owing to their low configuration and weak defense mechanism. To reveal the rules of malware diffusion in the really deployed wireless sensor networks, we propose a model called Malware Diffusion Based on Cellular Automaton to describe the dynamics of malware diffusion based on cellular automaton. According to the model, we first analyze and obtain the differential equations, which can reflect the various state dynamics of sensor nodes with cellular automaton. Then, we attain the equilibrium points of the model Malware Diffusion Based on Cellular Automaton to determine the threshold for whether malware will diffuse or die out in wireless sensor networks. Furthermore, we compute the basic regeneration number of the model Malware Diffusion Based on Cellular Automaton using the next-generation matrix and prove the stability of the equilibrium points. Finally, via experimental simulation, we verify the effectiveness of the model Malware Diffusion Based on Cellular Automaton, which can provide administrators with the theoretical guidance on suppressing malware diffusion in wireless sensor networks.

Keywords
Wireless sensor networks, malware, cellular automaton, equilibrium point, stability

Date received: 1 June 2020; accepted: 16 October 2020

Handling Editor: Yanjiao Chen

Introduction
Wireless sensor networks (WSNs) are extensively used in the real deployments, such as military and civil applications.1,2 WSNs are characterized by self-organization, dynamic topology, and limited capacity, and each sensor node (SN) has a limited communication range,3,4 so they are vulnerable to malware diffusion because of their low configuration and weak defense mechanism.5,6 Once WSNs are targeted by malware by exploiting network vulnerabilities, SN systems, or hardware and software vulnerabilities, the malware will quickly diffuse from one SN to another within communication range via communication.7,8

Malware is an application with malicious intent, which is intentionally developed by attackers to cause damage to SN systems by injecting malicious data,
breaking data transmission, blocking the network, or exhausting the capacity of SNs to lead to the WSNs paralyzed.\textsuperscript{9–13} To solve the problem with malware diffusion in WSNs, the primary issue is to construct a malware diffusion model and to reveal the rules of malware diffusion which is helpful for suppressing malware diffusion.\textsuperscript{14–16}

Epidemiology is commonly used to solve the problem with the dynamics of malware diffusion, because malware diffusion has the same characteristics as the propagation of epidemic.\textsuperscript{17,18} Researchers have presented many models,\textsuperscript{19,20} such as SI, SIS, SIRD, and SEIRD, to exhibit the change of states which consist of states susceptible (S), exposed (E), infected (I), recovered (R), and dead (D) for SNs.

To deal with the problem with malware diffusion in WSNs, we propose a model to describe the dynamics of malware diffusion based on cellular automaton (CA)\textsuperscript{21–23} that is more appropriate for describing the really deployed WSNs, compared with Markov chain. First, it can reflect the heterogeneity of WSNs by considering the networking and communication process among SNs and raising spatial-time discrete models of dynamical systems.\textsuperscript{24} Second, the stochastic model established by Markov chain is usually in lack of space consideration and not applicable to describe the dynamics of malware diffusion, while the model based on CA can effectively overcome these problems. In the proposed model, one cellular lattice represents a cell, and the states of the cell can be obtained from the fraction of the number of SNs in states S, E, I, R, and D.

In view of the above problem to be solved, we first propose a model called Malware Diffusion Based on Cellular Automaton (MDBCA), in which the SNs can be described by the five states S, E, I, R, and D. Second, we formulate differential equations to reflect the state dynamics of SNs. To explore the threshold whether malware will diffuse or die out in WSNs, we compute the equilibrium points of the model MDBCA for the malware-infected WSNs. Finally, we compute the basic reproduction number at the equilibrium points using the next-generation matrix and prove the stability of the equilibrium points.

The rest of this article is presented as follows: in the second part, we review the related work. In the third section, we propose the model MDBCA and analyze and obtain differential equations of the model, which can reflect the dynamics of the fraction of SNs in states S, E, I, R, and D. In the fourth section, we prove the existence of the equilibrium points of the model MDBCA and compute the basic reproduction number at the equilibrium points and finally prove the stability of the model MDBCA at the equilibrium points. In the fifth section, we present the experimental simulation and data analysis using relevant parameters. In the sixth section, we give the conclusion of this article.

Related work

At present, many researchers have presented various methods applicable to solve the problems with malware diffusion in WSNs. Liu et al.\textsuperscript{25} used the stochastic game to propose a method for WSNs to predict the probability of malware adopting the spread behavior. Shen et al.\textsuperscript{26} developed traditional epidemic theory and constructed a malware propagation model by differential equations to represent the dynamics between states. Shen et al.\textsuperscript{27} considered heterogeneous wireless sensor networks (HWSNs) and set up a dependability assessment mechanism for HWSNs with malware diffusion. Shen et al.\textsuperscript{28} considered a clustered WSN under epidemic-malware propagation conditions. Jiang et al.\textsuperscript{29} considered that WSNs can prevent from malware based on Stackelberg game. Acarali et al.\textsuperscript{30} applied the principles of epidemic modeling to IoT networks consisting of WSNs. Wang et al.\textsuperscript{31} used the pulse differential equation and the epidemic theory to propose a method for WSNs preventing from malware diffusion.

Many researchers have studied epidemic spread using CA. Holko et al.\textsuperscript{32} presented a new numerical, two-dimensional CA framework for simulation of the spread of an infectious disease. Sharma and Gupta\textsuperscript{33} analyzed the SEIR (susceptible-exposed-infected-recovered) epidemic spread with time delay through a two-dimensional CA model. López et al.\textsuperscript{34} addressed population heterogeneity and distribution in epidemics models using a CA framework for simulation of the spread of an approach. White et al.\textsuperscript{35} introduced a theoretical model based on CA framework for simulation of the epidemic spreading.

However, some malware diffusion issues based on CA in the malware-infected WSNs still have not been considered. The first issue is the elements mapping between SNs and CA, and the second issue is how to determine the condition in which malware will diffuse or die out in the malware-infected WSNs. In this study, we solve the first issue by proposing the model MDBCA, which can reflect the dynamics of the fraction of SNs by the differential equations. Furthermore, we solve the second issue by proving the stability of the model MDBCA at the equilibrium points, which is mathematically verified for theoretical correctness.

Description of the model MDBCA

To simplify the research, we consider the malware-infected WSNs are deployed in a two-dimensional cellular lattice with a side length of L. The lattice is divided into identical square areas, and each of them represents a cell of CA. The spatial location of each cell is shown with the two-dimensional coordinates.\textsuperscript{34} The
SNs are randomly or uniformly distributed in the two-dimensional cellular lattice.

As for the application of CA to the model MDBCA, it is important to describe model elements, including cell, cellular state, cellular neighbor, and cellular state transition function, under the diverse characteristics of malware diffusion.

**Definition 1.** CA can be described by the 5-tuplet, $CA = \{C, N, Q, V, F\}$, where $C$ is the cell set, $N$ is the cell capacity, $Q$ is the cellular state set, $V$ is the cellular neighbor set, and $F$ is the transition function of cellular state.

**Definition 2.** $C$ (cell set) represents the number of areas that are divided into the two-dimensional cellular lattice ($L \times L$), and each area represents one cell. The spatial position of the cell is uniquely identified by the horizontal coordinate ($i$) and the vertical coordinate ($j$) in the lattice; $c_{i,j}$ represents the cell located in the coordinate $(i, j)$. $C$ can be described by

$$C = \{ c_{i,j} \mid 0 \leq i, j \leq L \}$$

**Definition 3.** $N$ (cell capacity) is the number of active SNs in each cell, which is a constant.

**Definition 4.** $Q$ is the cellular state set, and $Q = \{S, E, I, R, D\}$.

Note that $Q$ includes the susceptible state $S$, the exposed state $E$, the infected state $I$, the immune state $R$, and the dead state $D$. Correspondingly, in cells, we classify a SN into state $S$ at the time when it is prone to be infected by malware, but has not been infected by malware; we classify a SN into state $E$ at the time when it has been infected by malware and can diffuse the malware to its neighbor; we classify a SN into state $I$ at the time when it is immune to the malware; we classify a SN into state $D$ at the time when it loses all functions, as it has either entirely consumed its energy or been damaged by malware. The state transform rates among SNs in cell are shown in Figure 1.

In Figure 1, the symbol $\mu$ denotes the probability of joining in the malware-infected WSNs for the new SNs in state $E$ every time step. To simplify the research, we suppose the total number of active SNs $N$ is a constant in each cell, and $\mu$ is equal to the death rate; in other words, the birth rate and the death rate are considered to be the same. When the SNs in state $S$ communicate with the SNs in state $I$, the SNs in state $S$ will be infected; note that one part of the SNs transforms from $S$ to $I$ by the rate $\tau$, and the other part transforms from $S$ to $E$ by the rate $\lambda$. After the latent period, the SNs in state $E$ can transform from $E$ to $I$ by the rate $\sigma$. For the known malware, we will patch security programs to cure the infected SNs, so the SNs in state $I$ can transform from $I$ to $R$ by the rate $\epsilon$.

The state of the cell $c_{i,j}$ at time $t$ can be described as $Q_{i,j} = \{S^t_{i,j}, E^t_{i,j}, I^t_{i,j}, R^t_{i,j}\}$, where $S^t_{i,j}$, $E^t_{i,j}$, $I^t_{i,j}$, and $R^t_{i,j}$ indicate the rates of SNs in states $S$, $E$, $I$, and $R$, respectively, at time $t$ in the cell $c_{i,j}$. Because the number of active SNs $N$ in each cell is a constant, the SNs in state $D$ are not included; we can obviously conclude the following equation

$$S^t_{i,j} + E^t_{i,j} + I^t_{i,j} + R^t_{i,j} = 1$$

**Definition 5.** $V$ is the cellular neighbor set, $V = \{v_{\alpha, \beta} \mid 1 \leq \alpha, \beta \leq L\}$, where the $v_{\alpha, \beta}$ is one of the neighbors of the cell $c_{i,j}$, and the cellular neighbor set of the cell $c_{i,j}$ can be described by $v_{i,j}$

$$v_{i,j} = \{v_{\alpha, \beta} \mid i - \alpha \equiv r \land j - \beta \equiv r\}$$

where $r$ denotes the communication radius of cells.
Definition 6. \( F \) is the cellular state transition function, \( F = \{ Q^t_{i,j} \}_{1 \leq i, j \leq L} \), where \( Q^t_{i,j} \) is the state transition function of the cell \( c_{i,j} \) at time \( t \).

Since the state transition function of the cell \( c_{i,j} \) is jointly determined by its own state \( Q^t_{i,j} \) and its neighbor state \( Q^{t-1}_{i,j} \), the state transition function \( Q^t_{i,j} \) can be described by

\[
Q^t_{i,j} = f(Q^{t-1}_{i,j}, Q^{a,\beta}_{i,j}) 
\] (4)

With the effect of the state transition functions and the transition rate among SNs, the dynamic transition relationship among SNs of the cell can be summarized as system (5), which is the local transition system of predicting \( S^t_{i,j}, E^t_{i,j}, I^t_{i,j}, \) and \( R^t_{i,j} \) at time \( t \)

\[
\begin{align*}
S^{t}_{i,j} &= S^{t-1}_{i,j} - (\lambda + \tau)S^{t}_{i,j}I^{t}_{i,j} - (\lambda + \tau) \\
&\quad - \sum_{(a, \beta) \in V} \frac{N_{a, \beta}}{N_{i,j}} S^{t}_{i,j} I^{t-1}_{i,j} + \mu (1 - S^{t-1}_{i,j}) \\
E^{t}_{i,j} &= E^{t-1}_{i,j} + \left( \lambda S^{t-1}_{i,j} I^{t-1}_{i,j} - \frac{N_{a, \beta}}{N_{i,j}} \lambda S^{t-1}_{i,j} S^{t-1}_{i,j} I^{t-1}_{i,j} \right) \\
&\quad - (\sigma + \mu) E^{t-1}_{i,j} \\
I^{t}_{i,j} &= I^{t-1}_{i,j} + \left( \tau S^{t-1}_{i,j} I^{t-1}_{i,j} - \frac{N_{a, \beta}}{N_{i,j}} \tau S^{t-1}_{i,j} S^{t-1}_{i,j} I^{t-1}_{i,j} \right) \\
&\quad + \sigma E^{t-1}_{i,j} - \mu I^{t-1}_{i,j} \\
R^{t}_{i,j} &= R^{t-1}_{i,j} + \sigma E^{t-1}_{i,j} - \mu R^{t-1}_{i,j}
\end{align*}
\] (5)

subject to \( 1 \geq S^{t}_{i,j} > 0, 1 \geq E^{t}_{i,j} > 0, 1 \geq I^{t}_{i,j} > 0, \) and \( 1 \geq R^{t}_{i,j} > 0 \).

Here, the parameter \( m \) is defined as the communication connectivity between the cell \( c_{i,j} \) and its neighbor \( v_{i,j} \). The \( S^t_{i,j} \) enters states \( I^t_{i,j} \) and \( E^t_{i,j} \) at the fractions \( \lambda S^{t-1}_{i,j} I^{t-1}_{i,j} \) and \( \tau S^{t-1}_{i,j} I^{t-1}_{i,j} \), respectively. At the same time, the \( I^t_{i,j} \) enters states \( I^t_{i,j} \) and \( E^t_{i,j} \) at the fractions \( \lambda \sum_{(a, \beta) \in V} \frac{N_{a, \beta}}{N_{i,j}} S^{t}_{i,j} E^{t-1}_{i,j} \) and \( \tau \sum_{(a, \beta) \in V} \frac{N_{a, \beta}}{N_{i,j}} S^{t}_{i,j} I^{t-1}_{i,j} \), respectively. The \( E^t_{i,j} \) enters state \( I^t_{i,j} \) at the fraction \( \sigma E^{t-1}_{i,j} \). The \( I^t_{i,j} \) enters state \( R^t_{i,j} \) at the fraction \( \sigma E^{t-1}_{i,j} \). All states \( S^{t}_{i,j}, E^{t}_{i,j}, I^{t}_{i,j}, \) and \( R^{t}_{i,j} \) enter state \( D \) at the fraction \( \mu \), and the \( \mu \) is also the newly added fraction in state \( S \).

**Stability analysis of the model MDBCA**

**System equilibrium points of the model MDBCA**

System equilibrium points mean that the system finally converges to a stable state over time. As shown in system (5) above, the system reaches a stable state, when the \( c_{i,j} \) in states \( S^t_{i,j}, E^t_{i,j}, I^t_{i,j}, \) and \( R^t_{i,j} \) do not change over time. The system equilibrium points can be divided into the malware-free equilibrium point and the endemic equilibrium point. The malware-free equilibrium point refers that the fractions of \( I^t_{i,j} \) and \( E^t_{i,j} \) converge to zero, that is, the SNs in states \( I \) and \( E \) in the system are extinct, while the endemic equilibrium point refers that the fraction of \( I^t_{i,j} \) and \( E^t_{i,j} \) are greater than 0, that is, the SNs in states \( S^t_{i,j}, I^t_{i,j}, \) and \( E^t_{i,j} \) are present. In other words, if the system exists the malware-free equilibrium point, the malware in the WSNs will eventually die out, while if the system exists the endemic equilibrium point, the malware in the WSNs will continuously diffuse, and the fractions of \( I^t_{i,j} \) and \( E^t_{i,j} \) will eventually reach a stable state.

Performing Taylor expansion on the system (5) and keeping only the first two terms, we obtain system (6)

\[
\begin{align*}
\frac{dS^{t-1}_{i,j}}{dt} &= - (\lambda + \tau)S^{t-1}_{i,j}I^{t-1}_{i,j} - (\lambda + \tau) \\
&\quad - \sum_{(a, \beta) \in V} \frac{N_{a, \beta}}{N_{i,j}} S^{t-1}_{i,j} I^{t-1}_{i,j} + \mu (1 - S^{t-1}_{i,j}) \\
\frac{dE^{t-1}_{i,j}}{dt} &= \left( \lambda S^{t-1}_{i,j} I^{t-1}_{i,j} + \frac{N_{a, \beta}}{N_{i,j}} \lambda S^{t-1}_{i,j} S^{t-1}_{i,j} I^{t-1}_{i,j} \right) \\
&\quad - (\sigma + \mu) E^{t-1}_{i,j} \\
\frac{dI^{t-1}_{i,j}}{dt} &= \left( \tau S^{t-1}_{i,j} I^{t-1}_{i,j} + \frac{N_{a, \beta}}{N_{i,j}} \tau S^{t-1}_{i,j} S^{t-1}_{i,j} I^{t-1}_{i,j} \right) \\
&\quad + \sigma E^{t-1}_{i,j} - \mu I^{t-1}_{i,j} \\
\frac{dR^{t-1}_{i,j}}{dt} &= e I^{t-1}_{i,j} - \mu R^{t-1}_{i,j}
\end{align*}
\] (6)

When \( \frac{dS^{t-1}_{i,j}}{dt} = 0, \frac{dE^{t-1}_{i,j}}{dt} = 0, \frac{dI^{t-1}_{i,j}}{dt} = 0, \) and \( \frac{dR^{t-1}_{i,j}}{dt} = 0 \), system (6) achieves an equilibrium solution. To simply the calculation, a special case is taken into consideration. When the SNs are uniformly distributed in the cellular lattice, then we can have \( N_{a, \beta}/N_{i,j} = 1 \). Furthermore, we can analyze the reduced system \( X = (S^t_{i,j}, I^t_{i,j}, E^t_{i,j}) \) and compute \( R^t_{i,j} \) from equation (2). Therefore, we obtain system (7)

\[
\begin{align*}
\frac{dS^{t-1}_{i,j}}{dt} &= - (\lambda + \tau)S^{t-1}_{i,j}I^{t-1}_{i,j} - (\lambda + \tau) \\
&\quad - \sum_{(a, \beta) \in V} \frac{N_{a, \beta}}{N_{i,j}} S^{t-1}_{i,j} I^{t-1}_{i,j} + \mu (1 - S^{t-1}_{i,j}) \\
\frac{dE^{t-1}_{i,j}}{dt} &= \left( \lambda S^{t-1}_{i,j} I^{t-1}_{i,j} + \frac{N_{a, \beta}}{N_{i,j}} \lambda S^{t-1}_{i,j} S^{t-1}_{i,j} I^{t-1}_{i,j} \right) \\
&\quad - (\sigma + \mu) E^{t-1}_{i,j} \\
\frac{dI^{t-1}_{i,j}}{dt} &= \left( \tau S^{t-1}_{i,j} I^{t-1}_{i,j} + \frac{N_{a, \beta}}{N_{i,j}} \tau S^{t-1}_{i,j} S^{t-1}_{i,j} I^{t-1}_{i,j} \right) \\
&\quad + \sigma E^{t-1}_{i,j} - \mu I^{t-1}_{i,j} \\
\frac{dR^{t-1}_{i,j}}{dt} &= e I^{t-1}_{i,j} - \mu R^{t-1}_{i,j}
\end{align*}
\] (7)
After directly solving system (7), we can identify two equilibrium points: \( G_0 = (S_0, I_0, E_0, R_0) = (1, 0, 0, 0) \) and \( G_s = (S_s, I_s, E_s, R_s) \). Here

\[
S_s = \frac{(\sigma + \mu)(\mu + e)}{\lambda \sigma + \sigma \tau + \tau \mu} \\
I_s = \frac{\mu(\lambda \sigma + \sigma \mu - \sigma \mu + \mu \tau - \mu^2 - \sigma e - \mu e)}{(\lambda + \tau)(\sigma + \mu)(\mu + e)} \\
E_s = \frac{\lambda \mu(\lambda \sigma + \sigma \mu - \sigma \mu + \mu \tau - \mu^2 - \sigma e - \mu e)}{(\lambda + \tau)(\sigma + \mu)(\mu + e)} \\
R_s = \frac{e(\lambda \sigma + \sigma \tau - \sigma \mu + \mu \tau - \mu^2 - \sigma e - \mu e)}{(\lambda + \tau)(\sigma + \mu)(\mu + e)}
\]

From the viewpoint of epidemiology, the equilibrium point \( G_0 \) is called a malware-free equilibrium point, while \( G_s \) is called an endemic equilibrium point. These equilibrium points can be used to analyze the dynamics of malware diffusion based on the model MDBCA in malware-infected WSNs.

**Stability analysis of the malware-free equilibrium point of the model MDBCA**

In order to verify the stability of system (7) at the malware-free equilibrium point \( G_0 \), it is necessary to apply the next-generation matrix method to compute the basic reproduction number \( R_0 \) of the system (7) at the malware-free equilibrium point \( G_0 \), because \( R_0 \) can be used to quantify the fraction of infected SNs by the SNs in state \( I \).

If \( R_0 < 1 \), the infectious SNs will infect less than one SN, which means that malware will die out and there is a malware-free equilibrium point. In other words, system (7) will asymptotically stable at the malware-free equilibrium point \( G_0 \).

If \( R_0 > 1 \), then the infectious SNs will infect more than one SN, meaning that the malware will continue to diffuse and there is an endemic equilibrium point. In other words, system (7) will asymptotically stable at the endemic equilibrium point \( G_s \).

In this article, the basic reproduction number \( R_0 \) of system (7) at the malware-free equilibrium point \( G_0 \) following the next-generation matrix method is expressed as

\[
R_0 = \frac{(1 + m)(\sigma \tau + \mu \tau + \lambda \sigma)}{(e + \mu)(\sigma + \mu)}
\]

**Theorem 1.** If \( R_0 < 1 \), the malware-free equilibrium point \( G_0 \) is locally asymptotically stable, whereas \( R_0 > 1 \), the malware-free equilibrium point \( G_0 \) is unstable.

**Proof.** According to stability theory for ordinary differential equations, if and only all the eigenvalues of the Jacobian matrix of an equilibrium point are less than zero, the equilibrium point is locally asymptotically stable. When system (7) is subjected to Taylor series expansion at \( G_0 \), the linear approximation system of system (7) is obtained by ignoring the higher-order infinitesimal. Then, the Jacobian matrix of system (7) at \( G_0 \) is shown as follows

\[
dS_{1,j}^{-1} = J_{11}(S - S_0) + J_{12}(I - I_0) + J_{13}(E - E_0) \\
dI_{1,j}^{-1} = J_{21}(S - S_0) + J_{22}(I - I_0) + J_{23}(E - E_0) \\
dE_{1,j}^{-1} = J_{31}(S - S_0) + J_{32}(I - I_0) + J_{33}(E - E_0)
\]

Here, \( J_{11} \), \( J_{12} \), \( J_{13} \), \( J_{21} \), \( J_{22} \), \( J_{23} \), \( J_{31} \), \( J_{32} \), and \( J_{33} \) are the values of system (7) corresponding to the Jacobian matrix at the malware-free equilibrium point \( G_0 \). When it is denoted as \( J(G_0) \), the expression is shown as follows

\[
J(G_0) = \begin{bmatrix} J_{11} & J_{12} & J_{13} \\ J_{21} & J_{22} & J_{23} \\ J_{31} & J_{32} & J_{33} \end{bmatrix}
\]

The submatrix of matrix (15) and its determinant value are evaluated as follows

\[
A_1 = [-\mu], \ det(A_1) = -\mu < 0 \\
A_2 = \begin{bmatrix} -\mu & 0 \\ 0 & -(\sigma + \mu) \end{bmatrix}, \ det(A_2) = -\mu(\sigma + \mu) > 0 \\
J(G_0) = \begin{bmatrix} -\mu & 0 & -(1 + m)(\lambda + \tau) \\ 0 & -(\sigma + \mu) & (1 + m)\lambda \\ 0 & \sigma & (1 + m)\tau - (e + \mu) \end{bmatrix}, \ det(A_3) = \mu(1 + m)(\sigma + \lambda \sigma)
\]

Therefore, when \( R_0 > 1 \), \( det(A_3) < 0 \), all the eigenvalues of matrix (15) are less than zero, and the malware-free equilibrium point \( G_0 \) is locally asymptotically stable, while \( R_0 > 1 \), some eigenvalues of matrix (15) are greater than zero; in other words, the malware-free equilibrium point \( G_0 \) is unstable.

Theorem 1 indicates that when \( R_0 < 1 \), the rate of SNs in states \( S, I, E, \) and \( R \) converges to 1, 0, 0, and 0, respectively. That is to say, when \( R_0 < 1 \), the
administer will only keep implementing current security measures, and the malware will eventually die out, regardless of the initially state fraction of SNs in infected-malware WSNs.

Simulations and verification
The experimental simulation and data analysis in this article are completed by VC6.0 and MATLAB R2013a. The key parameters of the experimental simulation are set as follows: 30,000 SNs are distributed in the two-dimensional square area with a side of 100 × 100, and each square lattice is a cell, and all cells are fully connected with a communication radius 1. The Moore neighborhoods of each cell are its surrounding eight cells, and the m is set as 0.125. In order to validate the accuracy of Theorem 1, we design two cases: (1) the SNs uniformly distributed in the cells and (2) the SNs randomly distributed in the cells.

When $R_0 < 1$, the other parameters based on the characteristics of WSNs are set as $\mu = 0.053$, $\lambda = 0.064$, $\tau = 0.2572$, $\sigma = 0.3028$, and $\epsilon = 0.3298$, satisfying the condition of Theorem 1.

Case 1: the SNs uniformly distributed in cells
Validating stability of the malware-free equilibrium point. In this section, the initial state $I^0_{i,j}$ is set as 0.01, 0.1, and 0.2, respectively. Figure 2 shows the changeable fraction trends of susceptible SNs under the condition of Theorem 1 for $I^0_{i,j} = 0.01$, $I^0_{i,j} = 0.1$, and $I^0_{i,j} = 0.2$. We observe different trends. When $I^0_{i,j} = 0.01$, the fraction of susceptible SNs slowly decreases to 97% in the first five time steps and then slowly decreases to a stable value of 100%. However, when $I^0_{i,j} = 0.1$ and $I^0_{i,j} = 0.2$, the fractions of susceptible SNs, respectively, decrease to 80% and 68% in the first 10 time steps and then gradually increase to a stable value of 100%.

Figure 3 shows the changeable fraction trends of infectious SNs under the condition of Theorem 1 for $I^0_{i,j} = 0.01$, $I^0_{i,j} = 0.1$, and $I^0_{i,j} = 0.2$. We observe different trends. When $I^0_{i,j} = 0.01$, the fraction of infectious SNs slowly decreases to a stable value of 0. When $I^0_{i,j} = 0.1$ and $I^0_{i,j} = 0.2$, the fractions of infectious SNs gradually decrease to 2% in the first 20 time steps and then slowly decrease to a stable value of 0.

Figure 4 shows the changeable fraction trends of exposed SNs under the condition of Theorem 1 for $I^0_{i,j} = 0.01$, $I^0_{i,j} = 0.1$, and $I^0_{i,j} = 0.2$. We observe different trends. When $I^0_{i,j} = 0.01$, the fraction of exposed SNs gradually increases to 0.2% in the first five time steps and then slowly decreases to a stable value of 0. When $I^0_{i,j} = 0.1$ and $I^0_{i,j} = 0.2$, the fractions of exposed SNs, respectively, gradually increase to 1.05% and 1.7% in the first five time steps and then gradually decrease to a stable value of 0.

Figure 5 shows the changeable fraction trends of recovered SNs under the condition of Theorem 1 for $I^0_{i,j} = 0.01$, $I^0_{i,j} = 0.1$, and $I^0_{i,j} = 0.2$. We observe different trends. When $I^0_{i,j} = 0.01$, the fraction of recovered SNs slowly increases to 2% in the first 20 time steps and then slowly decreases to a stable value of 0. When $I^0_{i,j} = 0.1$ and $I^0_{i,j} = 0.2$, the fractions of recovered SNs, respectively, gradually increase to 15% and 26% in the first five time steps and then gradually decrease to a stable value of 0.

According to the simulation experiments shown in Figures 2–5, we can conclude that when the SNs uniformly distribute in the cells, the fractions of susceptible, infectious, exposed, and recovered SNs all converge.
to the malware-free equilibrium $G_0$, regardless of the initial states distribution of the SNs in state $I$.

**Case 2: the SNs randomly distributed in cells**

**Validating stability of the malware-free equilibrium point.** In this section, the initial state $I_{i,j}^0$ is set as 0.01, 0.1, and 0.2, respectively. Figure 6 shows the changeable fraction trends of susceptible SNs under the condition of Theorem 1 for $I_{i,j}^0 = 0.01$, $I_{i,j}^0 = 0.1$, and $I_{i,j}^0 = 0.2$. We observe different trends. When $I_{i,j}^0 = 0.01$, the fraction of susceptible SNs slowly decreases to 98% in the first five time steps and then slowly decreases to a stable value of 100%. When $I_{i,j}^0 = 0.1$ and $I_{i,j}^0 = 0.2$, the fractions of susceptible SNs, respectively, decrease to 81% and 68% in the first nine time steps and then gradually increase to a stable value of 100%.

Figure 7 shows the changeable fraction trends of infectious SNs under the condition of Theorem 1 for $I_{i,j}^0 = 0.01$, $I_{i,j}^0 = 0.1$, and $I_{i,j}^0 = 0.2$. We observe different trends. When $I_{i,j}^0 = 0.01$, the fraction of infectious SN slowly decreases to a stable value of 0. When $I_{i,j}^0 = 0.1$ and $I_{i,j}^0 = 0.2$, the fractions of infectious SNs gradually decrease to 2% in the first 20 time steps and then slowly decrease to a stable value of 0.

Figure 8 shows the changeable fraction trends of exposed SNs under the condition of Theorem 1 for $I_{i,j}^0 = 0.01$, $I_{i,j}^0 = 0.1$, and $I_{i,j}^0 = 0.2$. We observe different trends. When $I_{i,j}^0 = 0.01$, the fraction of exposed SNs slowly decreases to a stable value of 0. When $I_{i,j}^0 = 0.1$ and $I_{i,j}^0 = 0.2$, the fractions of exposed SNs gradually decrease to 0% in the first 20 time steps and then slowly decrease to a stable value of 0.
SNs gradually increases to 0.15% and then slowly decreases to a stable value of 0. When $I_{0,ij}^0 = 0.1$ and $I_{0,ij}^0 = 0.2$, the fractions of exposed SNs, respectively, gradually increase to 1.05% and 1.7% in the first 10 time steps and then gradually decrease to a stable value of 0.

Figure 9 shows the changeable fraction trends of recovered SNs under the condition of Theorem 1 with random distribution in the cells. We observe different trends. When $I_{0,ij}^0 = 0.01$, the fraction of recovered SNs slowly increases to 2% in the first 20 time steps and then slowly decreases to a stable value of 0. When $I_{0,ij}^0 = 0.1$ and $I_{0,ij}^0 = 0.2$, the fractions of recovered SNs, respectively, gradually increase to 15% and 26% in the first five time steps and then gradually decrease to a stable value of 0.

According to the simulation experiments shown in Figures 6–9, we conclude that while the SNs randomly distribute in cells, regardless of the initial state distribution of the SNs in state $I$, the fractions of SNs in different states all converge to the malware-free equilibrium $G_0$.

From these two cases, regardless of the SNs distributed in cells (randomly or uniformly) and the initial state distribution of the SNs in state $I$, the SNs in state $E$, $I$, and $R$ will die out over time. In this matter, when $R_0 < 1$, the fractions of susceptible, infectious, exposed, and recovered SNs all converge to the malware-free equilibrium point $G_0$. Therefore, the effectiveness of Theorem 1 is verified.

Conclusion

To discover the rules of malware diffusion in WSNs, this article proposes the model MDBCA, which is more appropriate for describing the really deployed WSNs, and can reflect the networking among SNs more realistically. First, after the elements of SNs in the malware-infected WSNs are mapped to the model elements of CA, we obtained the differential equations, which can reflect the various state dynamics of the SNs. Then, we attain two equilibrium points of the model MDBCA: one is the malware-free equilibrium point and the other is the endemic equilibrium point. Finally, we prove the stability of the malware-free equilibrium points by the basic regeneration number $R_0$. Using numerical calculations and simulation experiments, we can acquire the stability condition of the malware-free equilibrium point, which provides a theoretical guidance for administrators to suppress malware diffusion in WSNs effectively.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This work was supported by National Natural Science Foundation of China under grant No. 61772018.

ORCID iDs

Hong Zhang https://orcid.org/0000-0003-3607-0177
Shigen Shen https://orcid.org/0000-0002-7558-5379
Xiaojun Wu https://orcid.org/0000-0002-8519-104X
References

1. Kim B, Park H, Kim KH, et al. A survey on real-time communications in wireless sensor networks. Wirel Commun Mob Com 2017; 2017: 1864847.
2. Patel H, Singh Rajput D, Thippa Reddy G, et al. A review on classification of imbalanced data for wireless sensor networks. Int J Distrib Sens N 2020; 16: 1–16.
3. González AV, Brisolara L and Ferreira PR. Efficiency evaluation of strategies for dynamic management of wireless sensor networks. Wirel Commun Mob Com 2017; 2017: 5618065.
4. Deng S, Cao B, Xiao X, et al. Cognitive routing optimization protocol based on multiple channels in wireless sensor networks. Int J Distrib Sens N 2020; 16: 1–14.
5. Xu H, Wang D, Shen S, et al. An efficient approach for stimulating cooperation among nodes in wireless sensor networks. Int J Distrib Sens N 2016; 12: 1–13.
6. Shen S, Huang L, Fan E, et al. Trust dynamics in WSNs: an evolutionary game-theoretic approach. J Sensors 2016; 2016: 4254701.
7. Cheng Z. A differential game model between intrusion detection system and attackers for wireless sensor networks. Wireless Pers Com 2016; 90: 1211–1219.
8. Jiang G, Shen S, Hu K, et al. Evolutionary game-based secrecy rate adaptation in wireless sensor networks. Int J Distrib Sens N 2015; 11: 1–13.
9. Liu J, Yu J and Shen S. Energy-efficient two-layer cooperative defense scheme to secure sensor-clouds. IEEE T Inf Foren Sec 2018; 13: 408–420.
10. Chen Z, Qiao C, Qiu Y, et al. Dynamics stability in wireless sensor networks active defense model. J Comput Syst Sci 2014; 80: 1534–1548.
11. Zhu L and Zhao H. Dynamical analysis and optimal control for a malware propagation model in an information network. Neurocomputing 2015; 149: 1370–1386.
12. Liu J, Xu M, Wang X, et al. A Markov detection tree-based centralized scheme to automatically malicious webpages on cloud platforms. IEEE Access 2018; 6: 74025–74038.
13. Yalew SD, Maguire GQ, Haridi S, et al. DroidPosture: a trusted posture assessment service for mobile devices. In: 2017 IEEE 13th international conference on wireless and mobile computing, networking and communications (WiMob), Rome, 9–11 October 2017, p. 12. New York: IEEE.
14. Sayad Haghighi M, Wen S, Xiang Y, et al. On the race of worms and patches: modeling the spread of information in wireless sensor networks. IEEE T Inf Foren Sec 2016; 12: 2854–2865.
15. Wang Y, Wen S, Xiang Y, et al. Modeling the propagation of worms in networks: a survey. IEEE Compur Surv Tut 2014; 2: 942–960.
16. Hosseini S, Azgomi MA and Rahmani AT. Malware propagation modeling considering software diversity and immunization. J Comput Sci 2016; 13: 49–67.
17. Pratap Srivastava A, Awasthi S, Pratap Ojha R, et al. Stability analysis of SIDR model for worm propagation in wireless sensor network. Indian J Sci Technol 2016; 9: 1–5.
18. Shen S, Zhou H, Feng S, et al. HSIRD: a model for characterizing dynamics of malware diffusion in heterogeneous WSNs. J Netw Comput Appl 2019; 146: 102420.
19. Mahboubi A, Camtepe S and Morarji H. A study on formal methods to generalize heterogeneous mobile malware propagation and their impacts. IEEE Access 2017; 5: 27740–27756.
20. Shen S, Huang L, Liu J, et al. Reliability evaluation for clustered WSNs under malware propagation. Sensors 2016; 16: 855.
21. Zhen J and Quan-Xing L. A cellular automata model of epidemics of a heterogeneous susceptibility. Chin Phys 2006; 15: 1248.
22. Wang Y, Li D and Dong N. Cellular automata malware propagation model for WSN based on multi-player evolutionary game. IET Netw 2018; 7: 129–135.
23. Wolfram S. Universality and complexity in cellular automata. Physica D 1984; 10: 1–35.
24. Byun H and Yu J. Cellular-automaton-based node scheduling control for wireless sensor networks. IEEE T Veh Technol 2014; 63: 3892–3899.
25. Liu J, Shen S, Yue G, et al. A stochastic evolutionary coalition game model of secure and dependable virtual service in Sensor-Cloud. Appl Soft Comput 2015; 30: 123–135.
26. Shen S, Li H, Han R, et al. Differential game-based strategies for preventing malware propagation in wireless sensor networks. IEEE T Inf Foren Sec 2014; 9: 1962–1973.
27. Shen S, Ma H, Fan E, et al. A non-cooperative non-zero-sum game-based dependability assessment of heterogeneous WSNs with malware diffusion. J Netw Comput Appl 2017; 91: 26–35.
28. Jiang W, Ma Z and Deng X. An attack-defense game based reliability analysis approach for wireless sensor networks. Int J Distrib Sens N 2019; 15: 1–14.
29. Acarali D, Rajarajan M, Komninns N, et al. Modelling the spread of botnet malware in IoT-based wireless sensor networks. Secur Commun Netw 2019; 2019: 1–13.
30. Wang X, He Z and Zhang L. A pulse immunization model for inhibiting malware propagation in mobile wireless sensor networks. Chin J Electron 2014; 23: 810–815.
31. Holko A, Medrek M and Pastuszak Z. Epidemiological modeling with a population density map-based cellular automata simulation system. Expert Syst Appl 2016; 48: 1–8.
32. Sharma N and Gupta AK. Impact of time delay on the dynamics of SEIR epidemic model using cellular automata. Physica A 2017; 471: 114–125.
33. López L, Burgeruner G and Giovanini L. Addressing population heterogeneity and distribution in epidemics models using a cellular automata approach. BMC Res Notes 2014; 7: 234.
34. White SH, Del Rey AM and Sánchez GR. Modeling epidemics using cellular automata. Appl Math Comput 2007; 186: 193–202.
35. Wolfram S. Cellular automata as models of complexity. Nature 1984; 311: 419–424.
36. van den Driessche P and Watmough J. Reproduction numbers and sub-threshold endemic equilibria for compartmental models of disease transmission. Math Biosci 2002; 180: 29–48.