sensors

Article

Epidemic Analysis of Wireless Rechargeable Sensor Networks Based on an Attack–Defense Game Model

Guiyun Liu [1], Baihao Peng [2,*] and Xiaojing Zhong [1]

[1] School of Mechanical and Electric Engineering, Guangzhou University, Guangzhou 510006, China; liugy@gzhu.edu.cn (G.L.); zhongxj@gzhu.edu.cn (X.Z.)
[2] School of Electronics and Communication Engineering, Guangzhou University, Guangzhou 510006, China
* Correspondence: 2111807063@e.gzhu.edu.cn

Abstract: Energy constraint hinders the popularization and development of wireless sensor networks (WSNs). As an emerging technology equipped with rechargeable batteries, wireless rechargeable sensor networks (WRSNs) are being widely accepted and recognized. In this paper, we research the security issues in WRSNs which need to be addressed urgently. After considering the charging process, the activating anti-malware program process, and the launching malicious attack process in the modeling, the susceptible–infected–anti-malware–low-energy–susceptible (SIALS) model is proposed. Through the method of epidemic dynamics, this paper analyzes the local and global stabilities of the SIALS model. Besides, this paper introduces a five-tuple attack–defense game model to further study the dynamic relationship between malware and WRSNs. By introducing a cost function and constructing a Hamiltonian function, the optimal strategies for malware and WRSNs are obtained based on the Pontryagin Maximum Principle. Furthermore, the simulation results show the validation of the proposed theories and reveal the influence of parameters on the infection. In detail, the Forward–Backward Sweep method is applied to solve the issues of convergence of co-state variables at terminal moment.

Keywords: wireless rechargeable sensor network; cyber security; stability analysis; optimal control

Citation: Liu, G.; Peng, B.; Zhong, X. Epidemic Analysis of Wireless Rechargeable Sensor Networks Based on an Attack–Defense Game Model. *Sensors* **2021**, *21*, 594. https://doi.org/10.3390/s21020594

Received: 21 December 2020
Accepted: 12 January 2021
Published: 15 January 2021

1. Introduction

Wireless sensor networks (WSNs) are the research hotspot worldwide over the last few years [1–3]. Sensor nodes which serve the function of data storing and data transmitting capacities form WSNs in the way of multi-hop or single-hop, as depicted in Figure 1. To monitor the physical parameters, such as temperature, humidity, pressure, etc., sensor nodes are randomly deployed in unattended areas. WSNs have widespread applications which are ranging from everyday life to various manufacturing industries [4]. However, due to the vulnerability of the sensor nodes and battery capacity limitations, the issues of security [5] and short lifespan [6] of WSNs are urgent to be tackled.

Focusing on optimizing energy utilization, scholars have proposed efficient schemes. However, comparing with the optimizing strategies, the operation of deploying rechargeable batteries can figure out the energy problem radically. Networks which are composed of rechargeable sensor nodes are named as wireless rechargeable sensor networks (WRSNs). Research hotspots on WRSNs mainly focus on solving the problems of both charging scheduling and system performance optimizations [7–9] in recent years. However, security issues in WRSNs are seldom attracting the attention of scholars. Malware, as a self-replicating malicious code, can lead to network interruption and paralysis once it propagates in the networks. Even worse, rechargeable sensor nodes also suffer from the Denial of Charge (DOC) attacks [10]. Such attacks will cause catastrophic consequence to real-time and pre-warning application fields [11]. Thus, it is urgent to study the security of WRSNs based on the rechargeable characteristics.

For the past few years, some scholars have made contributions to security issues of WRSNs based on the characteristics of information transmission. Recent relevant studies are listed in Table 1.

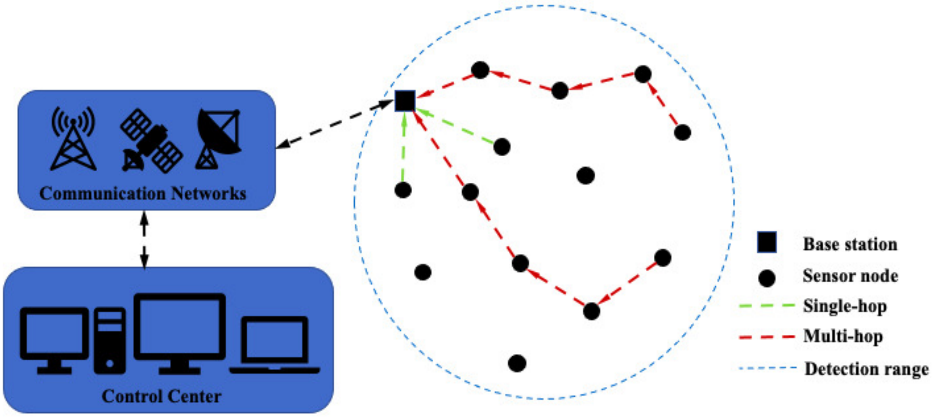


Figure 1. Communication architecture of wireless sensor networks.

Table 1. Research on WRSN security.

Authors	Problems	Methods	Results
A.N. Nguyen et al. [12]	Securing the physical layer	Time-switching power-splitting (TSPS) mechanism	The secrecy performance under TSPS is higher than the traditional scheme
J. Jung et al. [13]	Excessive energy consumption in the forward error correction(FEC) method	Energy-aware FEC method	The developed method performs better than the former one.
V.N. Vo et al. [14]	Securing energy harvesting wireless sensor networks(EH-WSNs) under eavesdropping and signal interception	An optimization scheme that uses a wirelessly powered friendly jammer	The hypotheses are supported.
A. EI Shafie et al. [15]	Securing a single-antenna rechargeable source node in the presence of a multi-antenna rechargeable cooperative jammer and a potential single-antenna eavesdropper	An efficient scheme which can optimize the transmission times of the source node	The average secrecy rate gain of the scheme is demonstrated significantly
B. Bhushan et al. [16]	Securing the mobile sinks position information	Energy Efficient Secured Ring Routing (E2SR2) protocol	E2SR2 achieves improved performance than the existing protocols
S. Lim et al. [17]	Securing EH-WSNs under the Denial-of-Service (DoS) attacks	Hop-by-hop Cooperative Detection (HCD) scheme	HCD scheme can significantly reduce the number of forwarding misbehaviors and achieve higher packet delivery ratio
K J.S.R. Kommuru et al. [18]	Balancing the trade-off between improving security and reducing energy consumption	Low complexity XOR technique and Hybrid LEACH-PSO algorithm	The proposed approach performs better than the existing approaches.
A. DI Mauro et al. [19]	Securing the communications under energy constraints	Adaptive approach which allows nodes to dynamically choose the most appropriate parameters	Adaptive solution performs better

Table 1. *Cont.*

Authors	Problems	Methods	Results
X. Hu et al. [20]	Securing the up-link (UL) transmission	Establishing the communication model; deriving the energy outage probabilities (EOP), connection outage probabilities (COP) and secrecy outage probabilities (SOP) through comprehensive analysis	The theoretical derivations are verified
O. Bouachir et al. [21]	Securing the transmission between sensor nodes and base stations	A novel strategy to select cluster heads and implement the non-orthogonal multiple access (NOMA) technique in the transmission	The secrecy performance can be improved

Due to the high similarity between infection mechanism of diseases in the population and the propagation mechanism of malware in WSNs, epidemic dynamics has also been widely used in the research of WSN security issues. In general, the applications of epidemic dynamics in WSNs mainly focus on the stability analysis of the built model. Recent relevant studies are listed in Table 2.

Table 2. Research on stability of epidemic model in WSNs.

Authors	Characteristics	Model	Stability
S.Y. Huang et al. [22]	Heterogeneity	Susceptible-Infected-Quarantined-Recovered-Susceptible (SIQRS)	1
P.K. Srivastava et al. [23]	Anti-malware process	Susceptible-Exposed-Infectious-Antimalware-Recovered (SEIAR)	2
L.H. Zhu et al. [24]	Time delay	Susceptible-Believed-Denied (SBD)	2
G.Y. Liu et al. [25]	Low-energy	Susceptible-Infected-Low-energy-Susceptible(SILS)	1
S. Hosseini et al. [26]	User awareness, network delay and diverse configuration of nodes	Susceptible–Exposed–Infected–Recovered-Susceptible with Vaccination and Quarantine state	2
R.P. Ojha et al. [27]	Quarantine and vaccination techniques	Susceptible–Exposed–Infectious–Quarantined–Recovered–Vaccinated (SEIQRV)	2
D.W. Huang et al. [28]	Patch injection mechanism	Susceptible–Infected–Patched–Susceptible (SIPS)	3
L.H. Zhu et al. [29]	Time delay in homogeneous and heterogeneous networks	Ignorants–Spreaders1–Spreaders2–Stiflers1–Stiflers2 (I2S2R)	1
J.D. Hernández Guillén et al. [30]	Carrier state	Susceptible–Carrier–Infectious–Recovered–Susceptible (SCIRS)	1
S.G. Shen et al. [31]	Heterogeneity and Mobility	Vulnerable–Compromised–Quarantined–Patched–Scrapped (VCQPS)	2

1: Local and global stability in malware-free and epidemic points; 2: Local and global stability in malware/rumor/worm-free point; 3: local and global stability in epidemic point.

Although the above models consider the characteristics of WSNs from various aspects, they do not analyze and model the networks based on the energy level. Besides, to our knowledge, the studies combining epidemic dynamics with WRSNs are very few. Therefore, this paper divides sensor nodes in WRSNs according to the residual energy and infection of sensor nodes and introduces the charging process. Differential games are also widely used in WSNs as a method of studying optimal dynamic strategies. Recent relevant studies are listed in Table 3.

Table 3. Research on differential game applied in WSNs.

Authors	Players	Goal	Strategies
S. Eshghi et al. [32]	Malware and mobile WSNs	Leverage the heterogeneity of malware propagation	Optimal patching policies
M.H.R. Khouzani et al. [33]	Malware and Mobile WSNs	Attain desired tradeoffs between security risks and bandwidth consumption	Optimal control in activating dispatchers and selecting their transmission rate
L.T. Zhang, et al. [34]	Malware and device to Device (D2D) offloading-enabled mobile network	Understand the malware propagation process in D2D offloading-enabled mobile network	Optimal dynamic defense and attack strategies
H. Al-Tous et al. [35]	An energy-harvesting multi-hop WSN	Balance the normalized buffer states of all sensor nodes and minimize the amount of energy used for data transmission.	An online power control and data scheduling algorithm
Y.H. Huang et al. [36]	Virus and sensor nodes	Mitigate virus spreading	Virus-resistant weight adaptation policies
Y. Sun et al. [37]	Edge nodes (ENs)	Realize the balance between reward and energy consumption cost of ENs in the deployment of defense measures	Optimal defense strategy
S.G. Shen et al. [38]	malware and WSNs	Limit malware in WSNs	Optimal dynamic strategies for the system and malware
J.H. Hu et al. [39]	A healthcare-based wireless sensor network (HWSN)	Minimize the transmission cost	Optimal data transmission strategies
S. Sarkar et al. [40]	Multi-hop wireless networks	Optimize network throughput	Optimal routing and scheduling policies

Based on the previous works [41] and inspired by [23], this paper proposes an epidemic model that includes the anti-malware (A) state, constructs game between malware and WRSNs, and obtains the optimal control strategies for both parties.

In the research on the security of WRSNs, few scholars analyze the issues by applying the relevant knowledge of epidemic dynamics. By establishing the dynamic differential equations of the propagation of malware in WRSNs, both the propagation mechanism of malware and the defense mechanism of WRSNs can be dynamically understood so as to provide novel thoughts and directions for resisting the invasion of malware.

In this paper, a susceptible infected anti-malware low-energy susceptible (SIALS) model is proposed by considering the charging process and the process of activating of the anti-malware program.The SIALS model can not only reflect the infection in WRSNs but also reveal the trend of the residual energy of the sensor nodes. At the same time, to describe the attack modes of malware, this paper considers the hardware attacks launched by malware and charging process compromised with malware.

Additionally, through the theory of stability analysis, the local and global stabilities of the disease-free equilibrium point and the epidemic equilibrium point of SIALS model are proved. Furthermore, this paper analyzes the game composed of malware and WRSNs by applying the Pontryagin Maximum Principle and obtains the optimal control strategies. Consequently, this work enriches the application of epidemic dynamics and differential games in addressing the security issues on WRSNs.

The rest of the paper is organized as follows. The introduction of the modeling of SIALS is presented in Section 2. Theorems of the local and global stability and the optimal strategies are proved in Section 3. The simulation results are shown in Section 4. The conclusions are drawn in Section 5.

2. Modeling

2.1. Dynamic Equation

In this paper, WRSNs consist of homogeneous rechargeable nodes which are randomly distributed. Meanwhile, the number of nodes increase at rate Λ, where Λ is greater than 0. Suppose that nodes in the networks belong to one of six possible compartment: susceptible (S), infected (I), anti-malware (A), low-energy and susceptible (LS), low-energy and infected (LI), and dysfunction (D). The relationship between the six compartments are depicted in Figure 2. S nodes are vulnerable to malware; I nodes are compromised with attacker; A nodes clear malware by activating anti-malware program; LS and LI nodes are both in low-energy level and remain dormant; and D nodes are totally out of function. Now, let us impose a set of hypotheses as follows.

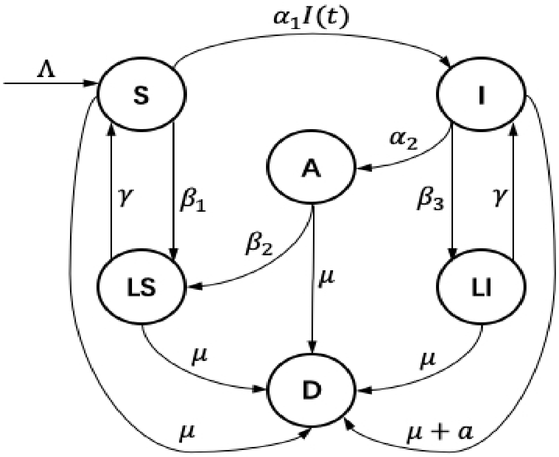


Figure 2. Flow diagram of the improved epidemic model.

(a) Malware propagates by broadcasting. Assuming that the ratio of I nodes successfully infecting S nodes is $\alpha_1 S(t)$, where α_1 is greater than 0, then the proportion of the new infected in the network is $\alpha_1 S(t)I(t)$.

(b) Considering mobile chargers and rechargeable modules, after the nodes in A drop to LS at β_2, anti-malware programs stop running, and the nodes return to S at rate γ when they are fully charged. β_2 and γ are all greater than 0.

(c) Nodes in S, I, and A drop to low-energy level at different ratios β_1, β_3, and β_2, where $\beta_1 < \beta_2 < \beta_3$. Among them, owing to the running of anti-malware program, β_2 is greater than β_1. Due to the software attack launched by malware, β_3 is greater than β_1 and β_2. β_1, β_2, and β_3 are all greater than 0.

(d) Suppose that, except for I, the four remaining compartments S, A, LS, and LI have the same mortality μ. I is different in that malware also launches hardware attacks at rate a to cause damage. μ and a are all greater than 0.

(e) Regardless of other protective measures, this paper only considers activating anti-malware program to achieve the purpose of clearing malware temporarily.

In particular, the parameters are summarized in Table 4.

Table 4. Epidemiological coefficients of the model.

Symbol	Description
Λ	Birth rate
γ	The rate of charging sensor nodes from low-energy to high-energy
β_1	Depletion rate determined by the working strength of susceptible nodes
β_2	Depletion rate determined by the working strength of anti-malware nodes
β_3	Depletion rate determined by malware
α_1	Transmission rate of malware
α_2	The rate of activating anti-malware
μ	Death rate
a	The rate of hardware attack determined by malware

On the basis of the above hypotheses, a novel dynamical system is obtained in (1)–(6):

$$\dot{S(t)} = \Lambda - (\alpha_1 I(t) + \beta_1 + \mu)S(t) + \gamma LS(t), \tag{1}$$

$$\dot{I(t)} = \alpha_1 S(t)I(t) - (\alpha_2 + \beta_3 + \mu + a)I(t) + \gamma LI(t), \tag{2}$$

$$\dot{A(t)} = -(\beta_2 + \mu)A(t) + \alpha_2 I(t), \tag{3}$$

$$\dot{LI(t)} = -(\gamma + \mu)LI(t) + \beta_3 I(t), \tag{4}$$

$$\dot{LS(t)} = -(\gamma + \mu)LS(t) + \beta_1 S(t) + \beta_2 A(t), \tag{5}$$

and

$$\dot{D(t)} = \mu N(t) + aI(t), \tag{6}$$

where $N(t) = S(t) + I(t) + A(t) + LS(t) + LI(t)$ and

$$\dot{N(t)} = \Lambda - \mu N(t) - aI(t). \tag{7}$$

2.2. *Computation of the Steady States and the Basic Reproductive Number*

Considering $LS(t) = N(t) - S(t) - I(t) - A(t) - LI(t)$, (1) can be rewritten as

$$\dot{S(t)} = \Lambda - (\alpha_1 I(t) + \beta_1 + \mu)S(t) + \gamma(N - S(t) - I(t) - A(t) - LI(t)), \tag{8}$$

where $N(t) = N(\infty) = \dfrac{\Lambda - aI(t)}{\mu}$.

Then, the solutions of the limit system (8) and (2)–(4) are the steady states of the system (1)–(5).

The first solution is the disease-free steady state: $E_0 = (S_0, I_0, A_0, LI_0)$, where $I_0 = 0$, $A_0 = 0$, $LI_0 = 0$, and

$$S_0 = \frac{\Lambda(\mu + \gamma)}{(\mu + \gamma)(\mu + \beta_1) - \gamma\beta_1}. \tag{9}$$

The second solution is the epidemic steady state $E^* = (S^*, I^*, A^*, LI^*)$, and

$$S^* = \frac{(\alpha_2 + \beta_3 + \mu + a)(\gamma + \mu) - \gamma\beta_3}{\alpha_1(\gamma + \mu)}, \tag{10}$$

$$I^* = \frac{\Delta_1 + \gamma\Lambda(\beta_2 + \mu)(\gamma + \mu)}{\Delta_2 + \Delta_3}, \tag{11}$$

$$A^{*} = \frac{\alpha_2\Delta_1 + \alpha_2\gamma\Lambda(\beta_2+\mu)(\gamma+\mu)}{(\beta_2+\mu)(\Delta_2+\Delta_3)}, \tag{12}$$

and

$$LI^{*} = \frac{\beta_3\Delta_1 + \beta_3\gamma\Lambda(\beta_2+\mu)(\gamma+\mu)}{(\gamma+\mu)(\Delta_2+\Delta_3)}, \tag{13}$$

where

$$\Delta_1 = [\Lambda - (\beta_1+\mu+\gamma)S^{*}][\mu(\beta_2+\mu)(\gamma+\mu)], \tag{14}$$

$$\Delta_2 = \mu(\beta_2+\mu)(\gamma+\mu)[\gamma+\alpha_1 S^{*}], \tag{15}$$

and

$$\Delta_3 = \gamma[a(\beta_2+\mu)(\gamma+\mu) + \alpha_2\mu(\gamma+\mu) + \beta_3\mu(\beta_2+\mu)]. \tag{16}$$

Consequently, considering the next generation matrix method, the basic reproductive number R_0 is its spectral radius.

Set

$$F = \begin{pmatrix} \alpha_1 S(t) & 0 \\ 0 & 0 \end{pmatrix} \tag{17}$$

and

$$V = \begin{pmatrix} \alpha_2+\beta_3+\mu+a & -\gamma \\ -\beta_3 & \gamma+\mu \end{pmatrix}. \tag{18}$$

Thus,

$$\begin{aligned} R_0 = F\cdot V^{-1} =& \frac{\alpha_1 S_0(\gamma+\mu)}{(\alpha_2+\beta_3+\mu+a)(\gamma+\mu)-\gamma\beta_3} \\ =& \frac{\alpha_1\Lambda(\gamma+\mu)^2}{[(\beta_1+\mu)(\gamma+\mu)-\gamma\beta_1][(\alpha_2+\beta_3+\mu+a)(\gamma+\mu)-\gamma\beta_3]}. \end{aligned} \tag{19}$$

3. Dynamic Analysis and Optimal Strategy

In this section, the stability and the optimal strategy in the SIALS model are discussed. In Section 3.1, the local and global stabilities of the disease-free point are proved by using the eigenvalues and the Lyaponov function. In Section 3.2, the local and global stabilities of the epidemic point are proved by using the Routh criterion and Bendixson-Dulac criterion. In Section 3.3, a five-tuple attack–defense game is proposed and the optimal strategies of malware and WRSNs are obtained by applying the Pontryagin Maximum Principle.

3.1. Analysis of Disease-Free Equilibrium Point

Theorem 1. *The disease-free equilibrium point, E_0, is locally asymptotically stable if $R_0 < 1$.*

Proof. Here, we use matrix eigenvalues to verify the validity of the theorem. In general, if the eigenvalues of the system matrix are negative, then the system must be stable.

Consider the follow matrix

$$F - V = \begin{pmatrix} \alpha_1 S_0 - (\alpha_2+\beta_3+\mu+a) & \gamma \\ \beta_3 & -\gamma-\mu \end{pmatrix} \tag{20}$$

The eigenvalues of (20) are

$$\lambda_1 = 0.5(-B_1 + \sqrt{B_1^2 + 4B_2}) \tag{21}$$

and

$$\lambda_2 = 0.5(-B_1 - \sqrt{B_1^2 + 4B_2}), \tag{22}$$

where $B_1 = (\gamma + \mu) - [\alpha_1 S_0 - (\alpha_2 + \mu + \beta_3 + a)]$ and $B_2 = [(\mu + \gamma)(\alpha_2 + \beta_3 + \mu + a) - \gamma\beta_3](R_0 - 1)$. The real parts of the two eigenvalues are negative if $R_0 < 1$. Besides,

$$\frac{\partial(\Lambda - (\beta_1 + \mu)S(t) + \gamma(N - S))}{\partial S} = -\beta_1 - \mu - \gamma < 0. \tag{23}$$

Thus, E_0 is locally asymptotically stable [42] when $R_0 < 1$. Conversely, E_0 is unstable if $R_0 > 1$. □

Theorem 2. *The disease-free equilibrium point, E_0, is globally asymptotically stable if $R_0 \leq 1$.*

Proof. Here, Lyapunov stability method is applied. In general, a positive definite Lyaponov function with negative definite first derivative needs to be established to test the stability of the system [43]. Considering a Lyaponov function $V(t) = (\gamma + \mu)I(t) + \gamma LI(t) > 0$, we have:

$$\begin{aligned}
V\dot{(t)} &= (\gamma + \mu)I\dot{(t)} + \gamma LI\dot{(t)} \\
&\leq I(t)[(\gamma + \mu)\alpha_1 S_0 - (\gamma + \mu)(\alpha_2 + \beta_3 + \mu + a) + \gamma\beta_3] \\
&= (\gamma + \mu)[\alpha_1 S_0 I(t) - (\alpha_2 + \beta_3 + \mu + a)I(t)] + \gamma\beta_3 I(t) \\
&= I(t)[(\gamma + \mu)\alpha_1 S_0 - (\gamma + \mu)(\alpha_2 + \beta_3 + \mu + a) + \gamma\beta_3] \\
&\leq I(t)(R_0 - 1)
\end{aligned} \tag{24}$$

In addition, $\dfrac{dV}{dt} = 0$ if and only if $R_0 = 1$ and $I(t) = 0$. Moreover, (S, I, A, LI) tends to E_0 when t tends to infinity, and the maximum invariant set in $\{(S, I, A, LI) \in \Omega : \dfrac{dV}{dt} = 0\}$ is E_0. Thus, Theorem 2 is proved, after considering the La-Salle Invariance Principle [44]. □

3.2. Analysis of Epidemic Equilibrium Point

Theorem 3. *The epidemic equilibrium point, E^*, is locally asymptotically stable if $R_0 > 1$.*

Proof. Here, the Routh criterion is applied to prove the theorem. Firstly, the Jacobian matrix of the limit system is:

$$\begin{pmatrix}
-(\alpha_1 I(t) + \beta_1 + \mu) - \gamma & -\alpha_1 S(t) - \gamma - \dfrac{a\gamma}{\mu} & -\gamma & -\gamma \\
\alpha_1 I(t) & \alpha_1 S(t) - (\alpha_2 + \beta_3 + \mu + a) & 0 & \gamma \\
0 & \alpha_2 & -(\beta_2 + \mu) & 0 \\
0 & \beta_3 & 0 & -(\gamma + \mu)
\end{pmatrix} \tag{25}$$

Then, the characteristic polynomial of (25) in E^* is

$$P(\lambda) = P_1\lambda^4 + P_2\lambda^3 + P_3\lambda^2 + P_4\lambda^1 + P_5, \tag{26}$$

where

$$P_1 = 1 > 0, \tag{27}$$

$$P_2 = a + \beta_1 + \alpha_2 + \beta_2 + \beta_3 + 2\gamma + 4\mu + \alpha_1\theta_3(R_0 - 1) + \frac{\gamma\beta_3}{\gamma + \mu} > 0, \tag{28}$$

$$P_3 = (\beta_2 + \mu)\frac{\gamma\beta_3}{\gamma + \mu} + \alpha_1(\alpha_1 S^* + \gamma)\theta_3(R_0 - 1) + (\gamma + \mu)(\beta_2 + \mu + \frac{\gamma\beta_3}{\gamma + \mu}) + \theta_1(\theta_2 + \frac{\gamma\beta_3}{\gamma + \mu}) > 0, \tag{29}$$

$$P_4 = (\gamma+\mu)(\beta_2+\mu)\frac{\gamma\beta_2}{\gamma+\mu} + \alpha_1\theta_3(R_0-1)(\alpha_1 S^* + \gamma)(\beta_2+\mu)\theta_2 + \theta_1[(\gamma+\mu)(\beta_2+\mu) + \theta_2\frac{\gamma\beta_3}{\gamma+\mu}] > 0, \tag{30}$$

and

$$P_5 = \alpha_1\theta_3(R_0-1)(\alpha_1 S^*+\gamma)(\gamma+\mu)(\beta_2+\mu) > 0, \tag{31}$$

where

$$\theta_1 = \alpha_1 I^* + \beta_1 + \mu + \gamma, \tag{32}$$

$$\theta_2 = \gamma + 2\mu + \beta_2, \tag{33}$$

and

$$\theta_3 = \frac{\beta_2+\mu}{\alpha_1(\gamma+\mu)[(\alpha_2+\beta_3+\mu+a) + \gamma\mu(\beta_2+\mu) + a\gamma(\beta_2+\mu) + \alpha_2\gamma\mu]} \tag{34}$$

Moreover, a simple calculation shows $P_2P_3 - P_1P_4 > 0$ and $P_2P_3P_4 - P_1P_4^2 - P_2^2P_5 > 0$. Thus, if $R_0 > 1$, applying the Routh criterion [45], the local asymptotically stability of E^* is tenable. □

Theorem 4. *The epidemic equilibrium point, E^*, is globally asymptotically stable if $R_0 \geq 1$.*

Proof. Set

$$\mathbf{D}(I, LI) = \frac{1}{ILI}, \tag{35}$$

$$\mathbf{P} = \alpha_1 S(t)I(t) - (\alpha_2+\beta_2+\mu+a)I(t) + \gamma LI(t), \tag{36}$$

and

$$\mathbf{Q} = -(\gamma+\mu)LI(t) + \beta_3 I(t). \tag{37}$$

Considering the following formulation:

$$\frac{\partial(\mathbf{DP})}{\partial I} + \frac{\partial(\mathbf{DQ})}{\partial LI} = -\gamma I^{-2} - \beta_3 LI^{-2} < 0 \tag{38}$$

By applying the Bendixson–Dulac criterion [46], the system admits no periodic orbits in the interior of Ω.

Let (I, LI) be a smooth point on the boundary of Ω. Along the boundary, there exists two possibilities:

(a) $0 \leq I < 1$, $LI = 0$. Then, $\frac{d\mathbf{P}(t)}{dt} = \beta_3 I(t) \geq 0$. The value 0 occurs if and only if $I = 0$.

(b) $0 \leq LI < 1$, $I = 0$. Then, $\frac{d\mathbf{Q}(t)}{dt} = \gamma LI(t) \geq 0$. The value 0 occurs if and only if $LI = 0$.

Thus, there is no periodic solutions that pass through the boundary.

In view of Theorem 3, the claim follows from the generalized Poincare–Bendixson theorem [46]. □

3.3. Optimal Strategies

Based on the evolution of node state during the confrontation between malware and WRSNs, an attack–defense game model is constructed as follows.

The attack–defense game based on the SIALS model can be expressed as a five-tuple $\mathbf{G} = \{\mathcal{P}, \boldsymbol{\nu}, \boldsymbol{\mu}, \mathcal{X}, \boldsymbol{\Lambda}\}$, where

- $\mathcal{P} = \{P_A, P_D\}$ is the set of plays in the attack–defense game. P_A is the attacker and P_D is the defender.

- $\boldsymbol{\nu} = \{A_{SI}(t), A_{LII}(t), A_{ID}(t)\}$ is a set of strategies implemented by the malware. $A_{SI}(t)$ represents the spreading capability of the malware, $A_{LII}(t)$ represents the strength of the attacks on the charging process, and $A_{ID}(t)$ represents the strength of the hardware attack. In particular, the three control strategies are all constrained by the upper and lower bounds.
- $\boldsymbol{\mu} = \{D_{IA}(t), D_{LSS}(t)\}$ is a set of strategies implemented by the WRSNs. $D_{IA}(t)$ represents the strength of activation of the anti-malware program and $D_{LSS}(t)$ represents the control of the charging process by WRSNs. Similarly, the two strategies have upper and lower bounds.
- $\mathcal{X} = \{\mathcal{X}(t)|S(t), I(t), A(t), LS(t), LI(t), D(t)\}$ is a set of the state variables on the SIALS model. The denotations of the state variables are the same as the statement in Section 2.1.
- $\boldsymbol{\Lambda} = \{\boldsymbol{\Lambda}(t)|\lambda_S(t), \lambda_I(t), \lambda_A(t), \lambda_{LS}(t), \lambda_{LI}(t), \lambda_D(t)\}$ is a set of the adjoint variables of the games

Considering the controlled process stated above, (1)–(6) transform to

$$\dot{S}(t) = \Lambda - (\alpha_1 A_{SI}(t)I(t) + \beta_1 + \mu)S(t) + \gamma D_{LSS}(t)LS(t), \tag{39}$$

$$\dot{I}(t) = \alpha_1 A_{SI}(t)S(t)I(t) - (\alpha_2 D_{IA}(t) + \beta_3 + \mu + aA_{ID}(t))I(t) + \gamma A_{LII}(t)LI(t), \tag{40}$$

$$A\dot{(}t) = -(\beta_2 + \mu)A(t) + \alpha_2 D_{IA}(t)I(t), \tag{41}$$

$$L\dot{S}(t) = -(\gamma D_{LSS}(t) + \mu)LS(t) + \beta_1 S(t) + \beta_2 A(t), \tag{42}$$

$$L\dot{I}(t) = -(\gamma A_{LII}(t) + \mu)LI(t) + \beta_3 I(t), \tag{43}$$

and

$$D\dot{(}t) = \mu N(t) + aA_{ID}(t)I(t). \tag{44}$$

In this paper, we mainly focus on how to effectively suppress the growth of malware. Furthermore, in the purpose of maintaining the operation of the networks, the phenomenon of network interruption and paralysis caused by the dysfunctionality of the sensor nodes need to be minimized. Therefore, the number of the infected and dysfunctional sensor nodes is used to measure the overall cost in the attack–defense game. Set $\mathcal{J}(\cdot)$ as the overall cost of the game and

$$\mathcal{J}(\mathcal{X}(t), \boldsymbol{\mu}(t), \boldsymbol{\nu}(t)) = \int_{t_0}^{t_f} \{C_I I(t) + C_D D(t)\} dt. \tag{45}$$

The above description of the cost index is a classic Lagrange problem in differential games. In (6), t_0 and t_f, respectively, represent the initial and terminal moment of the game. Specifically, $C_I I(t)$ is the instantaneous cost determined by the damage capability and the number of I nodes at time t, where $C_I > 0$. $C_D D(t)$ is the instantaneous cost determined by the impact of network interruption and paralysis at time t, where $C_D > 0$.

In this game, the goal of both parties is to influence changes in the cost $\mathcal{J}(\cdot)$ to make it more beneficial to their own development. Malware aims to maximize $\mathcal{J}(\cdot)$, while WRSNs aim to minimize $\mathcal{J}(\cdot)$. Therefore, malware needs to apply the dynamic strategies in $\boldsymbol{\nu}(t)$ to maximize $\mathcal{J}(\cdot)$ and WRSNs need to use the dynamic strategies in $\boldsymbol{\mu}(t)$ to minimize the $\mathcal{J}(\cdot)$. To achieve the purpose of both parties, Theorem 5 is given by applying the Pontryagin Maximum Principle.

Theorem 5. *Based on the state functions (39)–(44), there exist an optimal strategy set* $\{\mu^*(t), \nu^*(t)\} = \{(D^*_{IA}(t), D^*_{LSS}(t)), (A^*_{SI}(t), A^*_{ID}(t), A^*_{LII}(t))\}$ *in the attack–defense game such that*

$$J(\mathbf{X}(t), \mu^*(t), \nu^*(t)) = max_\nu min_\mu J(\mathbf{X}(t), \mu(t), \nu(t)) = min_\mu max_\nu J(\mathbf{X}(t), \mu(t), \nu(t)). \tag{46}$$

The expressions of the optimal strategies are

$$A^*_{SI}(t) = \begin{cases} maxA_{SI}, & (\lambda_I(t) - \lambda_S(t))\alpha_1 S(t)I(t) > 0 \\ minA_{SI}, & (\lambda_I(t) - \lambda_S(t))\alpha_1 S(t)I(t) < 0, \end{cases} \tag{47}$$

$$A^*_{ID}(t) = \begin{cases} maxA_{ID}, & (\lambda_D(t) - \lambda_I(t))aI(t) > 0 \\ minA_{ID}, & (\lambda_D(t) - \lambda_I(t))aI(t) < 0, \end{cases} \tag{48}$$

$$A^*_{LII}(t) = \begin{cases} maxA_{LII}, & (\lambda_I(t) - \lambda_{LI}(t))\gamma LI(t) + C_C\gamma LI(t) > 0 \\ minA_{LII}, & (\lambda_I(t) - \lambda_{LI}(t))\gamma LI(t) + C_C\gamma LI(t) < 0, \end{cases} \tag{49}$$

$$D^*_{IA}(t) = \begin{cases} minD_{IA}, & (\lambda_A(t) - \lambda_I(t))\alpha_2 I(t) > 0 \\ maxD_{IA}, & (\lambda_A(t) - \lambda_I(t))\alpha_2 I(t) < 0, \end{cases} \tag{50}$$

and

$$D^*_{LSS}(t) = \begin{cases} minD_{LSS}, & (\lambda_S(t) - \lambda_{LS}(t))\gamma LS(t) + C_C\gamma LS(t) > 0 \\ maxD_{LSS}, & (\lambda_S(t) - \lambda_{LS}(t))\gamma LS(t) + +C_C\gamma LS(t) < 0. \end{cases} \tag{51}$$

Proof. First, there exists a saddle-point in the game according to [41].

Then, in view of (39)–(44) and (45), the Hamiltonian function constructs as:

$$\begin{aligned}\mathcal{H}(\mathbf{X}(t), \boldsymbol{\lambda}(t), \mu(t), \nu(t), t) =& \lambda_S(t)\dot{S(t)} + \lambda_I(t)\dot{I(t)} + \lambda_A(t)\dot{A(t)} + \lambda_{LS}(t)\dot{LS(t)} \\ &+ \lambda_{LI}(t)\dot{LI(t)} + \lambda_D(t)\dot{D(t)} + C_I I(t) + C_D D(t)\end{aligned} \tag{52}$$

Note that the constraints of the adjoint variables are given by the following formulas [44]:

$$\dot{\lambda_S(t)} = (\lambda_S(t) - \lambda_I(t))\alpha_1 A_{SI}(t)I(t) + (\lambda_S(t) - \lambda_{LS}(t))\beta_1 + (\lambda_S(t) - \lambda_D(t))\mu, \tag{53}$$

$$\begin{aligned}\dot{\lambda_I(t)} =& (\lambda_S(t) - \lambda_I(t))\alpha_1 A_{SI}(t)S(t) + (\lambda_I(t) - \lambda_A(t))\alpha_2 D_{IA}(t) \\ &+ (\lambda_I(t) - \lambda_{LI}(t))\beta_3 + (\lambda_I(t) - \lambda_D(t))(\mu + aA_{ID}(t)) - C_I,\end{aligned} \tag{54}$$

$$\dot{\lambda_A(t)} = (\lambda_A(t) - \lambda_{LS}(t))\beta_2 + (\lambda_A(t) - \lambda_D(t))\mu, \tag{55}$$

$$\dot{\lambda_{LS}(t)} = (\lambda_{LS}(t) - \lambda_S(t))\gamma D_{LSS}(t) + (\lambda_{LS}(t) - \lambda_D(t))\mu, \tag{56}$$

$$\dot{\lambda_{LI}(t)} = (\lambda_{LI}(t) - \lambda_I(t))\gamma A_{LII}(t) + (\lambda_{LI}(t) - \lambda_D(t))\mu, \tag{57}$$

and

$$\dot{\lambda_D(t)} = -C_D. \tag{58}$$

Furthermore, the end values of the adjoint variables all equal to 0, i.e.,

$$\lambda_{S_{t_f}} = \lambda_{I_{t_f}} = \lambda_{A_{t_f}} = \lambda_{LS_{t_f}} = \lambda_{LI_{t_f}} = 0. \tag{59}$$

Finally, according to the Pontryagin Maximum Principle, the optimal strategies are obtained by

$$\mathcal{H}(t, \mathbf{X}^*(t), \boldsymbol{\lambda}(t), \mu^*(t), \nu(t)) \leq \mathcal{H}(t, \mathbf{X}^*(t), \boldsymbol{\lambda}(t), \mu^*(t), \nu^*(t)) \leq \mathcal{H}(t, \mathbf{X}^*(t), \boldsymbol{\lambda}(t), \mu(t), \nu^*(t)). \tag{60}$$

□

As a consequence, in the optimal case, when $(\lambda_I(t) - \lambda_S(t))\alpha_1 S(t)I(t) > 0$, the malware exerts the maximum effort to infect vulnerable sensor nodes; otherwise, it does not propagate. When $(\lambda_D(t) - \lambda_I(t))aI(t) > 0$, the malware exerts the maximum effort to launch the hardware attack; otherwise, it does nothing in hardware equipped in sensor nodes. When $(\lambda_I(t) - \lambda_{LI}(t))\gamma LI(t) + C_C\gamma LI(t) < 0$, the malware exerts the minimum effort to influence the charging process to LI nodes; otherwise, the LI nodes accept the charging requests. Moreover, when $(\lambda_A(t) - \lambda_I(t))\alpha_2 I(t) < 0$, WRSNs exist the maximum effort to clear the malware; otherwise, the networks do nothing in activating anti-malware program. When $(\lambda_S(t) - \lambda_{LS}(t))\gamma LS(t) + C_C\gamma LS(t) < 0$, WRSNs exist the maximum effort to charge the LS nodes; otherwise, LS nodes do not be charged.

4. Simulation

The purpose of this section is to further verify and develop the theorems stated in Section 3. In detail, the first three subsections focus on the stability of the system (1)–(6) and the last three subsections focus on the optimal control of the system (39)–(44).

The parameters used in the simulations were set as: $\Lambda = 0.2$, $\alpha_1 = 0.0001$, $\alpha_2 = 0.001$, $\beta_1 = 0.005$, $\beta_2 = 0.005$, $\beta_3 = 0.008$, $\mu = 0.004$, $a = 0.005$, and $\gamma = 0.05$. All simulations were run on MacOS Catalina (Intel Core i5, 8GB, 1.8GHz) and MATLAB 2017b.

4.1. Stable Analysis When $R_0 < 1$

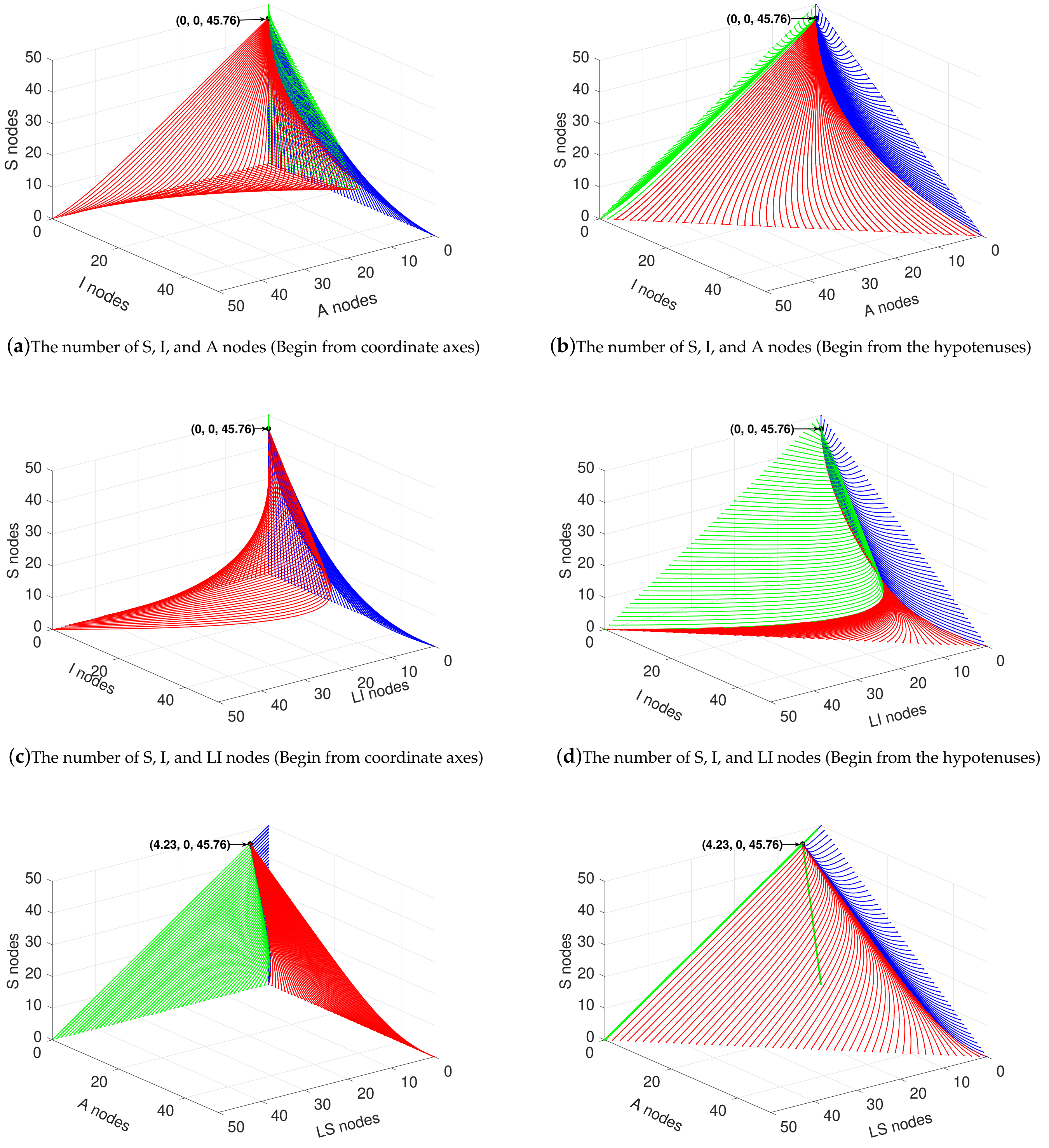
In this subsection, the stability of the system (1)–(6) is verified when $R_0 < 1$. Substituting the parameters into (19), we obtained $R_0 = 0.432 < 1$. Thus, there must exist a disease-free equilibrium point $(S_0, I_0, A_0, LS_0, LI_0)$ in the system. According to (10), $S_0 = 45.76$, $I_0 = 0$, $A_0 = 0$, $LS_0 = 4.23$, and $LI_0 = 0$. The simulation results are illustrated in Figure 3.

For the purpose of showing the changing trend of the system in a more three-dimensional and comprehensive way, we consider to verify the stability of the system in the form of three dimensions. We set $N(t) \leq 50$ (i.e., $S(t) + I(t) + A(t) + LS(t) + LI(t) \leq 50$). Therefore, in the case of three dimensions, the feasible region is a regular triangular pyramid with an equilateral triangle at its base and a right-angled isosceles triangle (Waist = 50) at its three sides.

The curves in Figure 3a,c,e all begin from the axes and the curves in Figure 3b,d,f all start at the boundary on the hypotenuses.

As shown in Figure 3a,b, in the three-dimensional area formed by the number of A nodes as the x-axis, the number of I nodes as the y-axis, and the number of S nodes as the z-axis, the curves eventually converge to $(0, 0, 45.67)$ from the six boundaries. In detail, in Figure 3a, when the curves start from x-axis, it is assumed that that there exists only A and LI nodes in the networks at the initial moment; when the curve starts from the z-axis, it is assumed that that only S and LI nodes in the network at the initial moment; and when the curve starts from y-axis, it is assumed that that only I and LS nodes in the network at the initial moment. The purpose of these assumptions is to ensure that malware exists in the network at the beginning, otherwise it would be meaningless. In Figure 3b, in the S-A plane, we set the sum of S nodes and A nodes as 49, and the number of LI nodes as 1 at the beginning. In the S-I plane, we set the sum of the number of S and I nodes as 50 at the beginning. In the A-I plane, we set that the sum of the number of A and I nodes is 50 at the beginning.

Similarly, in the three-dimensional area formed by the number of LI nodes as the x-axis, the number of I nodes as the y-axis, and the number of S nodes as the z-axis, the curves eventually converge to $(0, 0, 45.67)$, as shown in Figure 3c,d. Here, the principle of assumption is the same as above. The curves start from y-axis contain only I and LS nodes at the beginning. The curves start from the x-axis initially contain only LI and LS nodes at the beginning. It is worth noting that, in Figure 3c, the curve starts from the z-axis is reunited with the z-axis because it does not contain malware at the beginning. In Figure 3d, the curves start from the *S*-*LI* plane initially contain only *S* and *LI* nodes; the curves start from the *S*-*I* plane initially contain only *S* and *I* nodes; and the curves start from the *I*-*LI* plane initially contain only *I* and *LI* nodes.



(**a**)The number of S, I, and A nodes (Begin from coordinate axes)

(**b**)The number of S, I, and A nodes (Begin from the hypotenuses)

(**c**)The number of S, I, and LI nodes (Begin from coordinate axes)

(**d**)The number of S, I, and LI nodes (Begin from the hypotenuses)

(**e**)The number of S, A, and LS nodes (Begin from coordinate axes)

(**f**)The number of S, A, and LS nodes (Begin from the hypotenuses)

Figure 3. Variation of state variables in the case of $R_0 < 1$.

In the three-dimensional area formed by the number of LS nodes as the x-axis, the number of A nods as the y-axis, and the number of S nodes as the z-axis, the curves eventually converge to $(4.23, 0, 45.76)$, as shown in Figure 3e,f. Similarly, in Figure 3e, the curves begin from the z-axis initially contain S and I nodes; the curves begin from the x-axis initially contain LS and I nodes; and the curves begin from the y-axis initially contain A and I nodes. In Figure 3f, the curves begin from S-A plane initially contain S, A, and I nodes, and the sum of the number of S and A nodes are 49 and the number of I nodes is 1; the curves begin from S-LS plane initially contain S, LS, and I nodes, and the sum of the number of S and LS nodes are 49 and the number of I nodes is 1; and the curves begin from A-LS plane initially contain A, LS, and I nodes, and the sum of the number of A and LS nodes are 49 and the number of I nodes is 1.

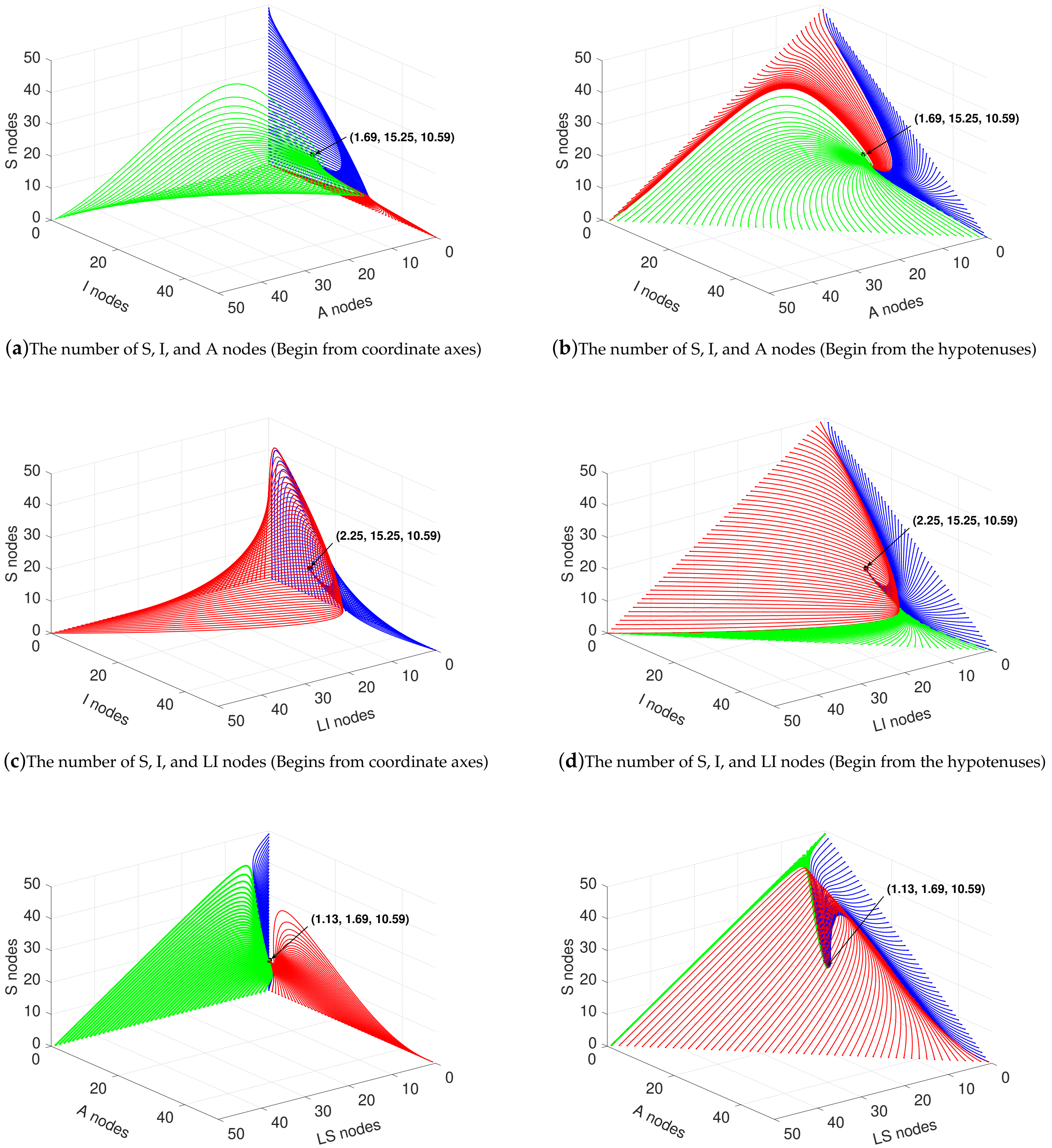
In Figure 3a–d, when the initial number of I nodes is less than a threshold, the number of I nodes has a peak value and decreases after that, and finally reaches 0. When the number of I nodes is greater than this threshold, the number of I nodes decreases continuously because the number of newly infected nodes is smaller than the number of newly recovered nodes. All these results confirm Theorems 1 and 2.

4.2. Stable Analysis when $R_0 > 1$

In this subsection, the situation under $R_0 > 1$ is discussed. Except for $\alpha_1 = 0.001$, the parameters remain the same as above. In this simulation, $R_0 = 4.320 > 1$, $S^* = 10.59$, $I^* = 15.25$, $A^* = 1.69$, $LS^* = 1.13$, $LI^* = 2.25$ and $N(\infty) = 30.9375$ based on (10)–(13) and (19). As in the Section 4.2, suppose $N(t) \leq 50$. The simulation results are shown in Figure 4.

The assumptions at the initial moment of the curve in this subsection are the same as in Section 4.1. As shown in Figure 4a,b, in the three-dimensional area formed by the number of A nodes as the x-axis, the number of I nodes as the y-axis, and the number of S nodes as the z-axis, the curves eventually converge to $(1.69, 15.25, 10.59)$ from the boundaries at the axes and the hypotenuses. In the three-dimensional area formed by the number of LI nodes as the x-axis, the number of I nodes as the y-axis, and the number of S nodes as the z-axis, the curves eventually converge to $(2.25, 15.25, 10.59)$ from the boundaries, as shown in Figure 4c,d. In the three-dimensional area formed by the number of LS nodes as the x-axis, the number of A nodes as the y-axis, and the number of S nodes as the z-axis, the curves eventually converge to $(1.13, 1.69, 10.59)$ from the boundaries, as shown in Figure 4e,f. All these results confirm Theorems 3 and 4.

Compared with the case of $R_0 < 1$, more peaks exist in the process of quantity change when $R_0 > 1$, but the general trend is similar. For I nodes, when the initial number is less than a certain threshold, it peaks and then eventually stabilize at the steady state value. When the initial number is greater than this threshold, the number of I nodes continues to decline until the steady state value. It is worth noting that the trend of the number of nodes is affected by the initial value. The trend changes if the initial values are set differently. However, if the model parameters do not change, the final value of the number of nodes does not change.



(**a**)The number of S, I, and A nodes (Begin from coordinate axes)

(**b**)The number of S, I, and A nodes (Begin from the hypotenuses)

(**c**)The number of S, I, and LI nodes (Begins from coordinate axes)

(**d**)The number of S, I, and LI nodes (Begin from the hypotenuses)

(**e**)The number of S, A, and LS nodes (Begins from coordinate axes)

(**f**)The number of S, A, and LS nodes (Begin from the hypotenuses)

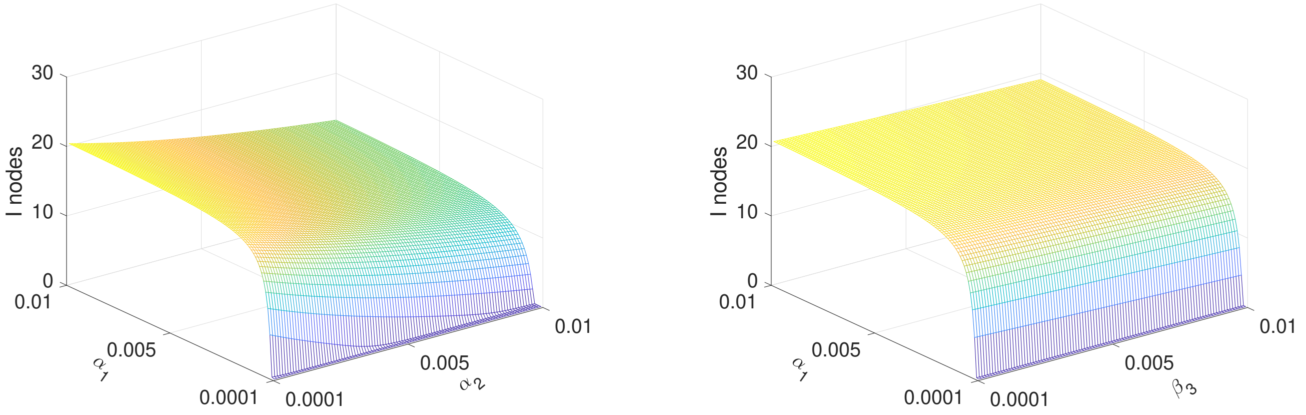
Figure 4. Variation of state variables in the case of $R_0 > 1$.

4.3. Influence of Parameters under Stable State

In this subsection, the influence of parameters on the spread of malware is analyzed. In detail, we analyzed the influence of α_1, α_2, β_3, and γ on the number of I nodes. The values of α_1, α_2, and β_3 range from 0.0001 to 0.01, and the value of γ ranges from 0.01 to 1.

Figure 5a shows the relationship between α_1 and α_2 and the number of I nodes when $t \to \infty$. Figure 5a shows that, by reducing the transmission rate α_1, malware can eventually be cleared. At the same time, increasing the removal rate α_2 of malware can effectively suppress the increasing of malware; Figure 5b shows the relationship between α_1 and β_3 and the number of I nodes when $t \to \infty$. As shown in Figure 5b, the behavior of malware to drops nodes to LI state by increasing the frequency or intensity of exhaustion attacks cannot be too effective to increase the number of I nodes in the steady state. Figure 5c shows the relationship between γ and α_2 and the number of I nodes in steady state. Figure 5c clearly shows that controlling the frequency or power of charging γ can restrain the spread of malware to a certain extent. Figure 5d shows the relationship between γ and β_3 and the number of I nodes in the steady state. As shown in Figure 5d, increasing the intensity of software attacks has little effect on the eventual prevalence of malware. On the contrary, when the charging rate γ drops to a certain extent, the amount of malware is greatly reduced. This suggests that we can control the charging rate γ to suppress the spread of malware. Figure 5e shows the relationship between β_3 and α_2 and the number of I nodes in the steady state. In Figure 5e, the influence of β_3 on the eventual prevalence of malware is verified again. At the same time, the effect of increasing the rate of activating anti-malware programs on the prevalence of malware is more obvious. Figure 5f shows the relationship between α_1 and γ and the number of I nodes in the steady state. As shown in Figure 5f, the method of reducing the number of I nodes by reducing the charging rate and transmission rate is verified again.

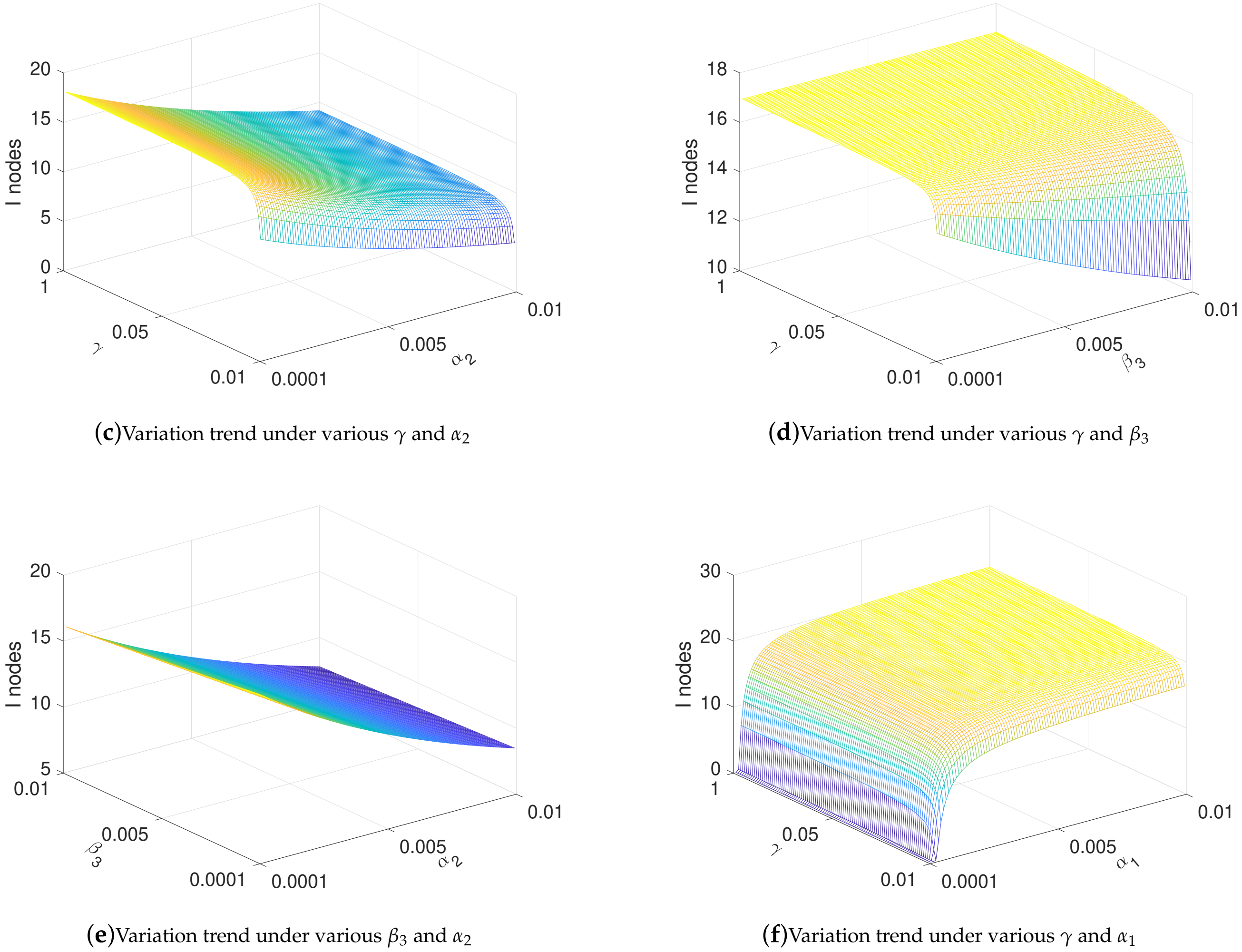
Among them, the most effective suppression method is to reduce the transmission rate α_1. By increasing removal rate α_2 and reducing the charging rate γ, the number of malware can be reduced to a certain extent when $t \to \infty$. In detail, although the method of reducing the transmission rate has a good effect, the effect is obvious when it is reduced to a certain extent, which is impractical in real life. The most direct method is to activate the anti-malware program to remove its own malware. The method of charging control is similar to the method of adjusting the transmission rate, which needs to be reduced to a certain threshold before the effect becomes obvious. Therefore, the method of suppressing malware by adjusting the transmission rate and charging rate is effective but requires much more consideration than activating the ant-malware program.



(**a**)Variation trend under various α_1 and α_2

(**b**)Variation trend under various α_1 and β_3

Figure 5. *Cont.*



(**c**)Variation trend under various γ and α_2

(**d**)Variation trend under various γ and β_3

(**e**)Variation trend under various β_3 and α_2

(**f**)Variation trend under various γ and α_1

Figure 5. Change of infection under various parameters when $t \to \infty$.

4.4. Variation of State Variables when $R_0 < 1$

Here, the evolution of state variables under optimal control is discussed. To verify the optimality, a non-optimal control group is set to compare with the optimal one. In detail, the situation under $R_0 < 1$ is stated first.

To satisfy (53)–(59), a Forward–Backward Sweep (FBS) method is applied. The flow diagram of the method is illustrated in Figure 6. First, the supposed values of model parameters are given. Then, by applying the finite difference method, the numerical solutions of the state variables are calculated in order and adjoint variables in reversed order. Furthermore, the values of controls are obtained at the same time. Finally, if and only if the difference between the two iterations is less than an error value δ multiplied by the iteration value at the current moment, then the optimality conditions stated in Theorem 5 are considered to be satisfied. Here, we set $\delta = 0.001$. It is worth noting that, when the system has low computational complexity, the FBS method can achieve better convergence of the adjoint variables. However, with the increasing complexity of the system, the method has difficulty achieving convergence, and it needs to update, which is also one of the directions of our future work.

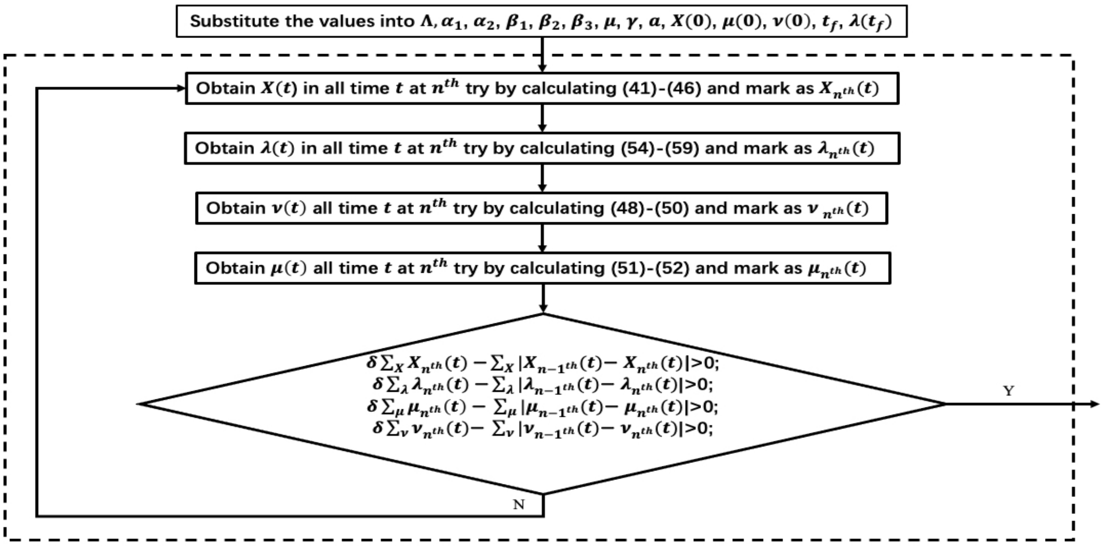

Substitute the values into Λ, α_1, α_2, β_1, β_2, β_3, μ, γ, a, $X(0)$, $\mu(0)$, $\nu(0)$, t_f, $\lambda(t_f)$
Obtain $X(t)$ in all time t at n^{th} try by calculating (41)-(46) and mark as $X_{n^{th}}(t)$
Obtain $\lambda(t)$ in all time t at n^{th} try by calculating (54)-(59) and mark as $\lambda_{n^{th}}(t)$
Obtain $\nu(t)$ all time t at n^{th} try by calculating (48)-(50) and mark as $\nu_{n^{th}}(t)$
Obtain $\mu(t)$ all time t at n^{th} try by calculating (51)-(52) and mark as $\mu_{n^{th}}(t)$
$\delta\sum_X X_{n^{th}}(t) - \sum_X |X_{n-1^{th}}(t) - X_{n^{th}}(t)| > 0$;
$\delta\sum_\lambda \lambda_{n^{th}}(t) - \sum_\lambda |\lambda_{n-1^{th}}(t) - \lambda_{n^{th}}(t)| > 0$;
$\delta\sum_\mu \mu_{n^{th}}(t) - \sum_\mu |\mu_{n-1^{th}}(t) - \mu_{n^{th}}(t)| > 0$;
$\delta\sum_\nu \nu_{n^{th}}(t) - \sum_\nu |\nu_{n-1^{th}}(t) - \nu_{n^{th}}(t)| > 0$;
Y
N

Figure 6. Flow diagram of Forward–Backward Sweep (FBS) method.

Figure 7 shows the comparison of evolution of state variables under optimal control and non-optimal control. Here, the blue lines represent the evolution under optimal control and the red lines represent the evolution under non-optimal control. In Figure 7a, we set up 100 datasets, in which cases of the optimal control and the non-optimal control are equally divided. In the sets under optimal control, we assume that the sum of the initial number of nodes S and I of the networks is 50. For example, when the initial number of S nodes is 24, the initial number of I nodes is 26. Figure 7a shows the comparison of the number of S nodes in the two cases. Figure 7a shows that the number of S nodes under optimal control reach the equilibrium point more quickly, and the number is less than that under non-optimal control. Furthermore, the number of S nodes under optimal control is lower than that under non-optimal control when the number stay steady.

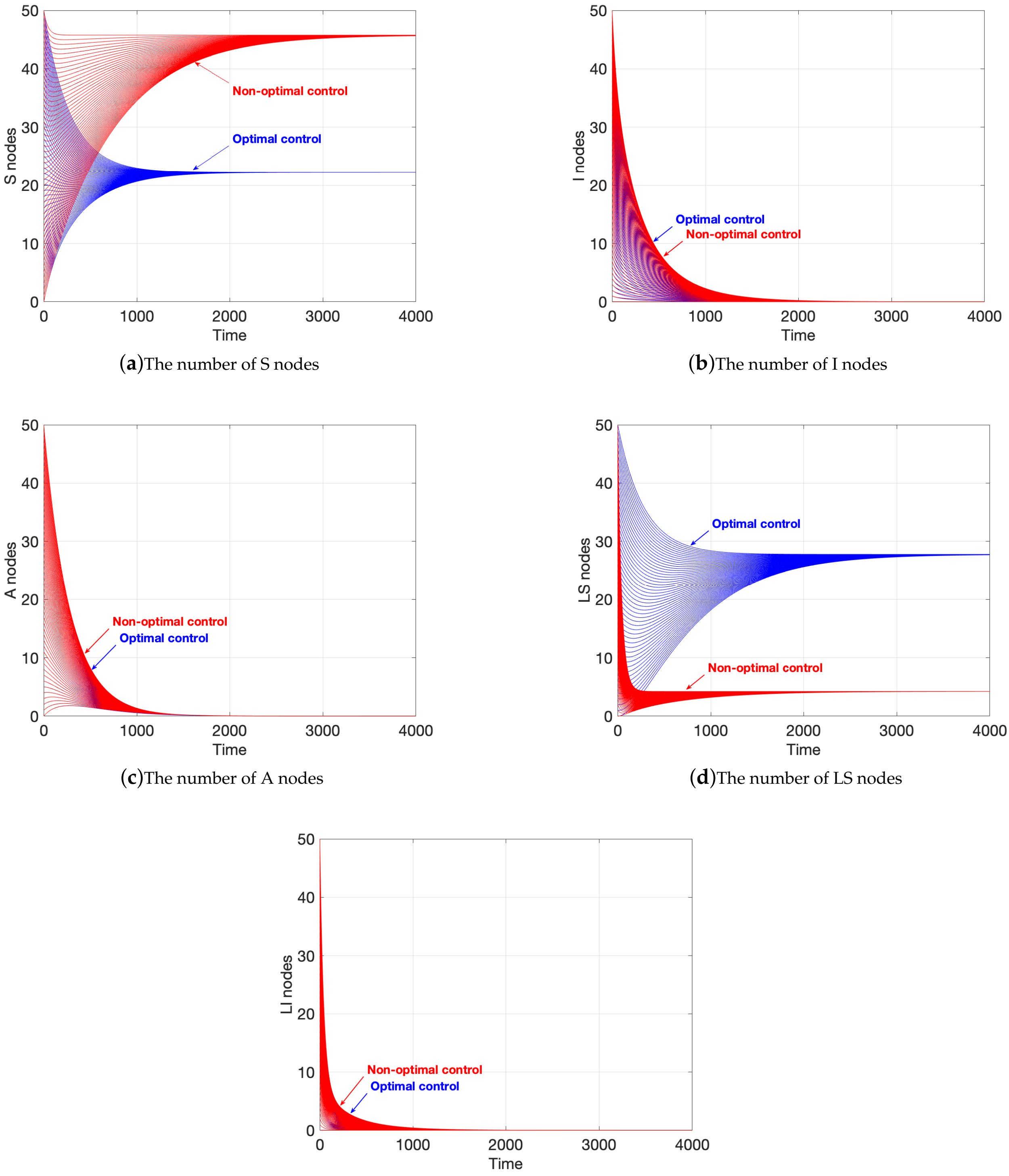
The data in Figure 7b follow those in Figure 7a. In the case of optimal control, as the number of S nodes decreases, the number of I nodes decreases more rapidly, as shown in Figure 7b. In other words, malware is eliminated faster under optimal control.

In the setting of the data of the two cases in Figure 7c, we assume that it contains A and I nodes at the beginning, and the sum is 50. As illustrated in Figure 7c, the difference in the number of A nodes is not evident in the two cases, which indicates the removal action never stops.

In Figure 7d, we assume that it contains only LS and LI nodes at the beginning, and their sum is 50. As illustrated in Figure 7d, the reason for the decrease in the number of S nodes is that WRSNs choose to stop charging the LS nodes, which leads to an increase to the number of LS nodes.

The data setting in Figure 7e follows that in Figure 7d. Similarly, the difference in the number of LI nodes is not significant in the two cases, as shown in Figure 7e, which indicates the software attacks never stop.

Therefore, although the spread of malicious programs can be suppressed under the optimal control, the performance of the system is sacrificed, that is, the existence of more low-energy sensor nodes leads to problems in network operation.



(**a**)The number of S nodes

(**b**)The number of I nodes

(**c**)The number of A nodes

(**d**)The number of LS nodes

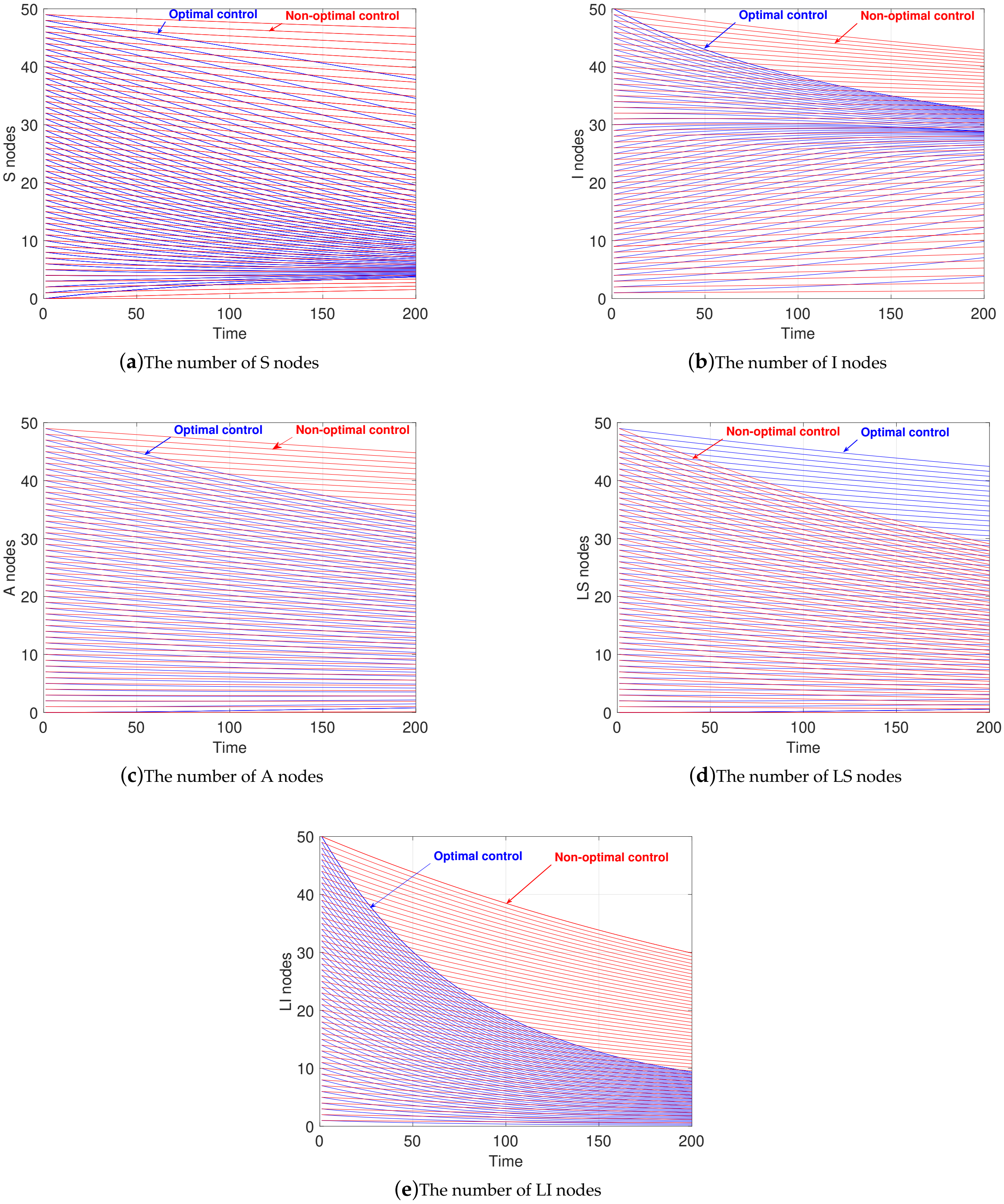
(**e**)The number of LI nodes

Figure 7. Evolution of state variables under various controls in the case of $R_0 < 1$.

4.5. Variation of State Variables when $R_0 > 1$

In this subsection, the situation under $R_0 > 1$ is discussed. Comparing with Section 4.4, if the value of T is too high, the adjoint variables do not converge finally under the FBS method, so we set the terminal time of the game to 200, i.e., $T = 200$. Meanwhile, the data setting is the same as in Section 4.5.

Figure 8 shows the comparison of the changes in the number of the state variables in the same two cases stated in Section 4.4. Similar to the statement in Section 4.4, the number of S nodes under optimal control always shows a faster decline, as shown in Figure 8a. In contrast, the number of S nodes with non-optimal control does not change much from time 0 to 200. Therefore, in the case of $R_0 > 1$, WRSNs can restrain the growth of I nodes by reducing the number of S nodes.



(**a**)The number of S nodes

(**b**)The number of I nodes

(**c**)The number of A nodes

(**d**)The number of LS nodes

(**e**)The number of LI nodes

Figure 8. Evolution of state variables under various controls in the case of $R_0 > 1$.

Compared with the case without optimal control, more LS nodes stay in the LS state at this time instead of returning to the S state, as shown in Figure 8d. For the case of non-optimal control, the number of LS nodes decreases rapidly since LS nodes constantly send charging requests and get fully charged. For the optimal control, LS nodes choose to stop charging in order to reduce the growth rate of S nodes' number.

As illustrated in Figure 8b,c,e, with the effective reduction of the number of S nodes, the numbers of I nodes, A nodes, and LI nodes all show a significant decrease, compared with the situation under non-optimal control.

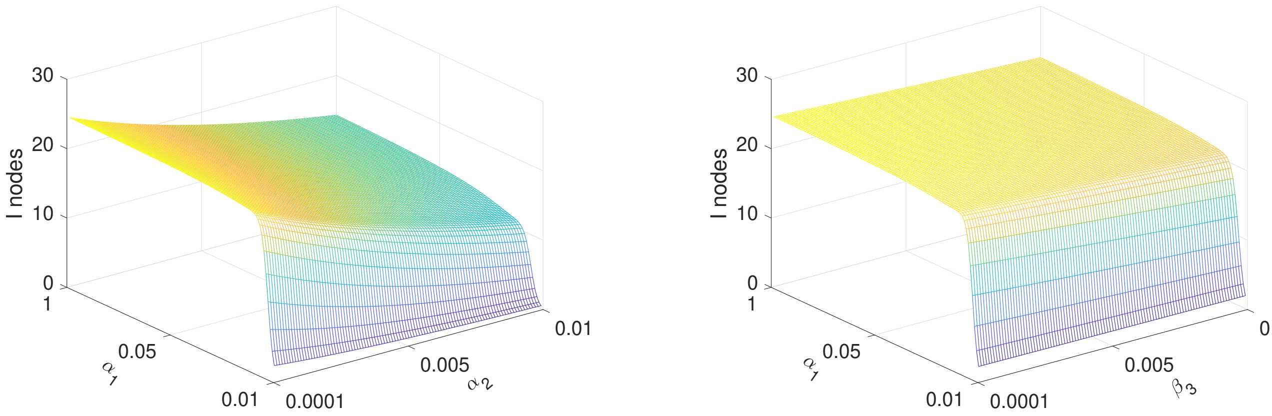
In the case of $R_0 > 1$, for malware, to make the cost as large as possible, the three means controlled by malware maintain the maximum degree of control; for WRSNs, in addition to removing malware in the maximum efforts, it also stops charging the LS nodes to further deter more vulnerable nodes from being attacked.

4.6. Influence of Parameters under Optimal Controls

As in Section 4.3, the influence of parameters on malware is developed here. It is easy to know from Section 4.4 that, when $R_0 < 1$, malware is completely eliminated eventually. Therefore, we only consider the case $R_0 > 1$. At the same time, to maintain the continuity with Section 4.3, suppose $T = 200$.

Figure 9 shows the influence of the parameters on the number of I nodes, and the range of the parameters is consistent with Section 4.3. It is worth mentioning that, at this time, since the time setting is much smaller than that in Section 4.3, the number of I nodes is larger. Comparing with Figure 5 in Section 4.3, it is not difficult to find that, under optimal control, the influence of parameters on the propagation of malware is very similar to that under non-optimal control. Similarly, the conclusion is similar to Section 4.3, and is not repeated here.

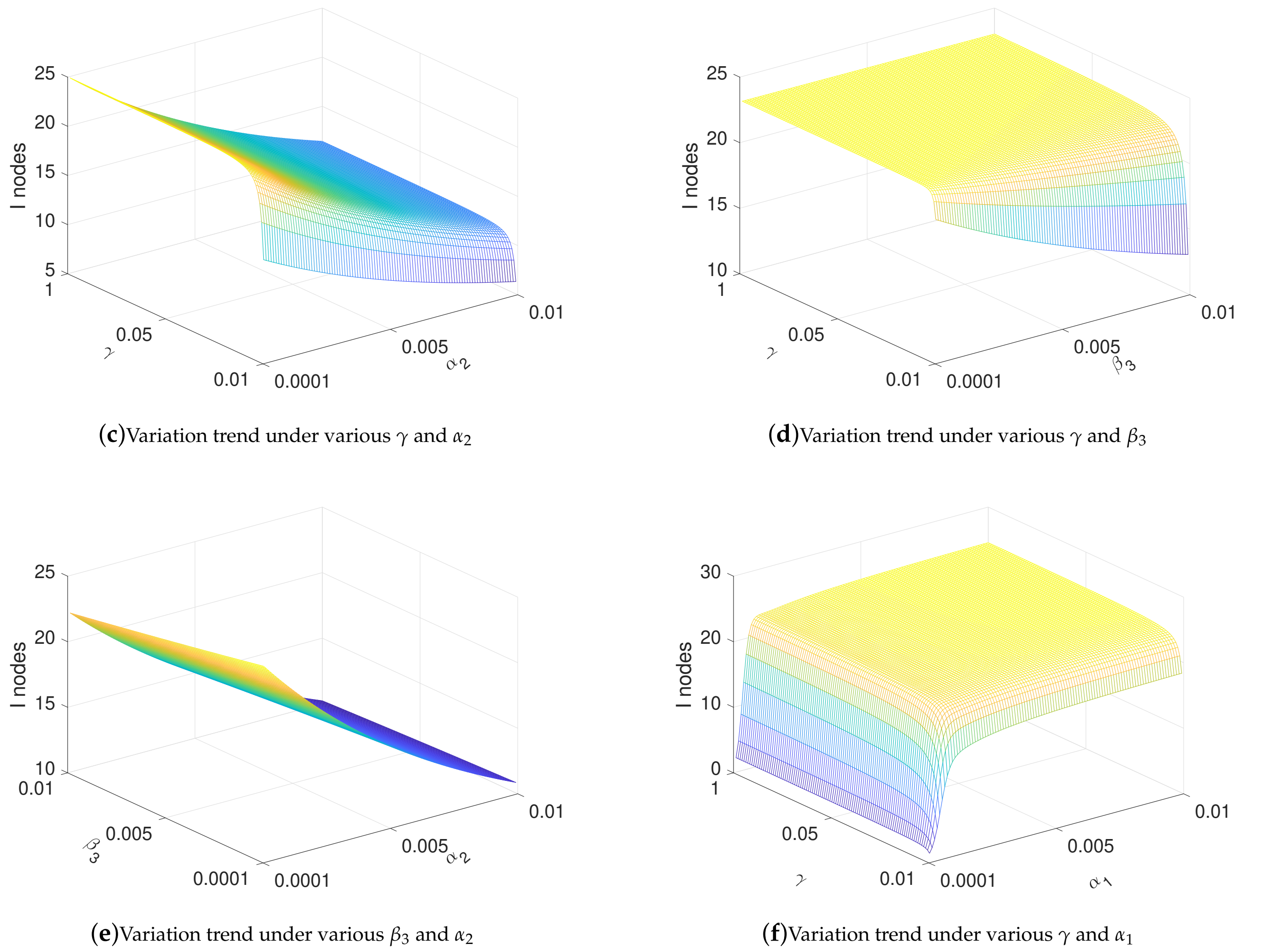
In the optimal dynamic game, the three control methods of malware, namely $A_{SI}(t)$, $A_{ID}(t)$, and $A_{LII}(t)$, are always present and undiminished. As WRSNs, it stops charging the LS nodes while exerting greatest effort to activate the anti-malware program. Therefore, in the game process, the overall architecture of SIALS model is not affected. In other words, stopping charging has little effect on the model. Meanwhile, this phenomenon also reveals that the influence of reduced charging rate on the spread of malware mainly occurs in the state transition of sensor nodes from LI state to I state.



(**a**)Variation trend under various α_1 and α_2

(**b**)Variation trend under various α_1 and β_3

Figure 9. *Cont.*



(**c**)Variation trend under various γ and α_2

(**d**)Variation trend under various γ and β_3

(**e**)Variation trend under various β_3 and α_2

(**f**)Variation trend under various γ and α_1

Figure 9. Change of infection in optimal controls under various parameters when t = 200.

5. Conclusions

In this paper, we use epidemiology to propose a dynamic model, namely SIALS, describing the propagation of malware in WRSNs. In this model, not only the remaining energy of the sensor nodes is revealed, but also the description of the recovered process is enriched by introducing the anti-malware (A) state. Meanwhile, through the stability analysis of the model, we proved the local and global stability of disease-free equilibrium point and the epidemic equilibrium point. Furthermore, based on the confrontational nature of malware and WRSNs, this paper proposes a five-tuple attack–defense game model. Specifically, after introducing the overall cost, by adopting the Pontryagin Maximum Principle, this paper introduces the dynamic optimal strategies for malware and WRSNs. We verified the validity of the theories through simulations in the form of three-dimensional figures and analyzed the influence of the parameters on the propagation of malware. Then, the evolution of the number of state variables based on optimal control in the two cases of $R_0 < 1$ and $R_0 > 1$ was also simulated and analyzed. Meanwhile, the influence of parameters on infection under optimal control was analyzed.

Simulation results show that the malware can be eliminated by adjusting the transmission rate, but it needs to be reduced to a certain threshold. Activating anti-malicious program is the most effective and direct way to suppress the spread of malware. Adjusting the charging rate can also suppress the spread of malware effectively, but, again, it needs to be below a certain threshold. In the dynamic game between malware and WRSNs, WRSNs effectively reduce the number of malware by refusing to charge. In particular, in the case of $R_0 < 1$, malware goes extinct more quickly. In the case of $R_0 > 1$, the spread of malware is suppressed obviously compared with the case with non-optimal control.

With the continuous development of the wireless power transfer and the intelligent mobile vehicles, the potential security risk of mobile charger cannot be ignored. In our future work, in view of the integrating of various devices, both the homogenous and heterogenous cases will be taken into consideration, and, if the ability permits, the stochastic modeling and the advanced mathematical theories will be applied. Consequently, we hope our works can give some inspirations to interested researchers.

Author Contributions: Conceptualization, G.L. and B.P.; methodology, G.L., B.P. and X.Z.; software, B.P.; validation, G.L., B.P. and X.Z.; formal analysis, B.P.; investigation, G.L. and B.P.; writing—original draft preparation, B.P.; and writing—review and editing, G.L., B.P. and X.Z. All authors have read and agreed to the published version of the manuscript.

Funding: The National Natural Science Foundation of China (61403089) and the 2020 Department of Education of Guangdong Province Innovative and Strong School Project (Natural Sciences) - Young Innovators Project (Natural Sciences) under Grant 2020KQNCX054.

Data Availability Statement: The data presented in this study is contained within the article.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Xie, H.M.; Yan, Z.; Yan, Z.; Atiquzzaman, M. Data Collection for Security Measurement in Wireless Sensor Networks: A Survey. *IEEE Internet Things J.* **2020**, *6*, 2205–2224. [CrossRef]
2. Han, G.J.; Jiang, J.F.; Zhang, C.Y.; Duong, T.Q.; Guizani, M.; Karagiannidis, G.K. A Survey on Mobile Anchor Node Assisted Localization in Wireless Sensor Networks. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 2220–2243. [CrossRef]
3. Butun, I.; Osterberg, P.; Song, H.B. Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 616–644. [CrossRef]
4. Rashid, B.; Rehmani, M.H. Applications of wireless sensor networks for urban areas: A survey. *J. Netw. Comput. Appl.* **2016**, *60*, 192–219. [CrossRef]
5. Yetgin, H.; Cheung, K.T.K.; El-Hajjar, M.; Hanzo, L. A Survey of Network Lifetime Maximization Techniques in Wireless Sensor Networks. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 828–854. [CrossRef]
6. Panatik, K.Z.; Kamardin, K.; Shariff, S.A.; Yuhaniz, S.S.; Ahmad, N.A.; Yusop, O.M.; Ismail, S. Energy Harvesting in Wireless Sensor Networks: A Survey. In Proceedings of the 2016 IEEE 3rd international symposium on Telecommunication Technologies (ISTT), Kuala Lumpur, Malaysia, 28–30 November 2016.
7. Shu, Y.C.; Yousefi, H.; Cheng, P.; Chen, J.M.; Gu, Y.; He, T.; Shin, K.G. Near-Optimal Velocity Control for Mobile Charging in Wireless Rechargeable Sensor Networks. *IEEE. Trans. Mob. Comput.* **2016**, *15*, 1699–1713. [CrossRef]
8. Wu, P.F.; Xiao, F.; Sha, C.; Huang, H.P.; Sun, L.J. Trajectory Optimization for UAVs' Efficient Charging in Wireless Rechargeable Sensor Networks. *IEEE Trans. Veh. Technol.* **2020**, *69*, 4207–4220. [CrossRef]
9. Mo, L.; Kritikakou, A.; He, S.B. Energy-Aware Multiple Mobile Chargers Coordination for Wireless Rechargeable Sensor Networks. *IEEE Internet Things J.* **2019**, *6*, 8202–8214. [CrossRef]
10. Lin, C.; Shang, Z.; Du, W.; Ren, J.K.; Wang, L.; Wu, G.W. CoDoC: A Novel Attack for Wireless Rechargeable Sensor Networks through Denial of Charge. In Proceedings of the IEEE INFOCOM 2019-IEEE Conference on Computer Communications, Paris, France, 29 April–2 May 2019.
11. Lin, C.; Zhou, J.Z.; Guo, C.Y.; Song, H.B.; Wu, G.W.; Mohammad, S.O. TSCA: A temporal-spatial real-time charging scheduling algorithm for on-demand architecture in wireless rechargeable sensor networks. *IEEE. Trans. Mob. Comput.* **2018**, *17*, 211–224. [CrossRef]
12. Nguyen, A.N.; Vo, V.N.; So-ln, C.; Ha, D.B.; Sanguanpong, S.; Baig, Z.A. On Secure Wireless Sensor Networks With Cooperative Energy Harvesting Relaying. *IEEE Access* **2019**, *7*, 139212–139225. [CrossRef]
13. Jung, J.; Kang, M.; Yoon, I.; Noh, D.K. Adaptive Forward Error Correction Scheme to Improve Data Reliability in Solar-powered Wireless Sensor Networks. In Proceedings of the 2016 International Conference on Information Science and Security (ICISS), Pattaya, Thailand, 19–22 December 2016.
14. Vo, V.N.; Nguyen, T.G.; So-ln, C.; Ha, D.B. Secrecy Performance Analysis of Energy Harvesting Wireless Sensor Networks with a Friendly Jammer. *IEEE Access* **2017**, *5*, 25196–25206. [CrossRef]
15. Shafie, A.E.I.; Niyato, D.; Al-Dhahir, N. Security of Rechargeable Energy-Harvesting Transmitters in Wireless Networks. *IEEE Wirel. Commun. Lett.* **2016**, *5*, 384–387. [CrossRef]

16. Bhushan, B.; Sahoo, G. E2SR2: An acknowledgement-based mobile sink routing protocol with rechargeable sensors for wireless sensor networks. *Wirel. Netw.* **2019**, *25*, 2697–2721. [CrossRef]
17. Lim, S.; Huie, L. Hop-by-Hop Cooperative Detection of Selective Forwarding Attacks in Energy Harvesting Wireless Sensor Networks. In Proceedings of the 2015 International Conference on Computing, Networking and Communications, Anaheim, CA, USA, 16–19 February 2015.
18. Kommuru, K.J.S.R.; Kadari, K.K.Y.; Alluri, B.K.S.P.K.R. A novel approach to balance the trade-off between security and energy consumption in WSN. In Proceedings of the 2018 2nd International Conference on Micro-Electronics and Telecommunication Engineering, Ghaziabad, India, 20–21 September 2018.
19. Mauro, A.D.; Fafoutis, X.; Dragoni, N. Adaptive Security in ODMAC for Multihop Energy Harvesting Wireless Sensor Networks. *Int. J. Distrib. Sens. Netw.* **2015**, *11*, 760302. [CrossRef]
20. Hu, X.; Huang, K.Z.; Chen, Y.J.; Xu, X.M.; Liang, X.H. Secrecy Analysis of UL Transmission for SWIPT in WSNs with Densely Clustered Eavesdroppers. In Proceedings of the 2017 9th International Conference on Wireless Communications and Signal Processing (WCSP 2017), Nanjing, China, 11–13 October 2017.
21. Bouachir, O.; Mnaouer, A.B.; Touati, F.; Crescini, D. Opportunistic Routing and Data Dissemination Protocol for Energy Harvesting Wireless Sensor Networks. In Proceedings of the 2016 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS 2016), Larnaca, Cyprus, 21–23 November 2016.
22. Huang, S.Y.; Chen, F.D.; Chen, L.J. Global dynamics of a network-based SIQRS epidemic model with demographics and vaccination. *Commun. Nonlinear Sci. Numer. Simul.* **2017**, *43*, 296–310. [CrossRef]
23. Srivastava, P.K.; Pandey, S.P.; Gupta, N.; Singh, S.P.; Ojha, R.P. Modeling and Analysis of Antimalware Effect on Wireless Sensor Network. In Proceedings of the 2019 IEEE 4th International Conference on Computer and Communication Systems (ICCCS), Singapore, 23–25 February 2019.
24. Zhu, L.H.; Guan, G. Dynamical analysis of a rumor spreading model with self-discrimination and time delay in complex networks. *Physics A* **2019**, *533*, 121953. [CrossRef]
25. Liu, G.Y.; Peng, B.H.; Zhong, X.J. A Novel Epidemic Model for Wireless Rechargeable Sensor Network Security. *Sensors* **2020**, *21*, 123. [CrossRef]
26. Hosseini, S.; Azgomi, M.A. The dynamics of an SEIRS-QV malware propagation model in heterogeneous networks. *Physics A* **2018**, *512*, 803–817. [CrossRef]
27. Ojha, R.P.; Srivastava, P.K.; Sanyal, G.; Gupta, N. Improved Model for the Stability Analysis of Wireless Sensor Network Against Malware Attacks. *Wirel. Pers. Commun.* **2020**, 1–24. [CrossRef]
28. Huang, D.W.; Yang, L.X.; Yang, X.F.; Wu, Y.B.; Tang, Y.Y. Towards understanding the effectiveness of patch injection. *Physics A* **2019**, *526*, 120956. [CrossRef]
29. Zhu, L.H.; Zhou, M.T.; Zhang, Z.D. Dynamical Analysis and Control Strategies of Rumor Spreading Models in Both Homogeneous and Heterogeneous Networks. *J. Nonlinear Sci.* **2020**, *30*, 2545–2576. [CrossRef]
30. Guillén, J.D.H.; del Rey, A.M. A mathematical model for malware spread on WSNs with population dynamics. *Physics A* **2020**, *545*, 123609.
31. Shen, S.G.; Zhou, H.P.; Feng, S.; Liu, J.H.; Zhang, H.; Cao, Q.Y. An Epidemiology-Based Model for Disclosing Dynamics of Malware Propagation in Heterogeneous and Mobile WSNs. *IEEE Access* **2020**, *8*, 43876–43887. [CrossRef]
32. Eshghi, S.; Khouzani, M.H.R.; Sarkar, S. Optimal Patching in Clustered Malware Epidemics. *IEEE-ACM Trans. Netw.* **2016**, *24*, 283–298. [CrossRef]
33. Khouzani, M.H.R.; Sarkar, S.; Altman, E. Optimal Dissemination of Security Patches in Mobile Wireless Networks. *IEEE Trans. Inf. Theory* **2012**, *58*, 4714–4732. [CrossRef]
34. Zhang, L.T.; Xu, J. Differential Security Game in Heterogeneous Device-to-Device Offloading Network under Epidemic Risks. *IEEE Trans. Netw. Sci. Eng.* **2020**, *7*, 1852–1861. [CrossRef]
35. Al-Tous, H.; Barhumi, I. Differential Game for Resource Allocation in Energy Harvesting Sensor Networks. In Proceedings of the 2018 IEEE International Conference on Communications (ICC), Kansas City, MO, USA, 20–24 May 2018.
36. Huang, Y.H.; Zhu, Q.Y. A Differential Game Approach to Decentralized Virus-Resistant Weight Adaptation Policy over Complex Networks. *IEEE Trans. Control Netw. Syst.* **2020**, *7*, 944–955. [CrossRef]
37. Sun, Y.; Li, Y.B.; Chen, X.H.; Li, J. Optimal defense strategy model based on differential game in edge computing. *J. Intell. Fuzzy Syst.* **2020**, *39*, 1449–1459. [CrossRef]
38. Shen, S.G.; Li, H.J.; Han, R.S.; Vasilakos, A.V.; Wang, Y.H.; Cao, Q.Y. Differential Game-Based Strategies for Preventing Malware Propagation in Wireless Sensor Networks. *IEEE Trans. Inf. Forensics Secur.* **2014**, *9*, 1962–1973. [CrossRef]
39. Hu, J.H.; Qian, Q.; Fang, A.; Fang, S.Z.; Xie, Y. Optimal Data Transmission Strategy for Healthcare-Based Wireless Sensor Networks: A Stochastic Differential Game Approach. *Wirel. Pers. Commun.* **2016**, *89*, 1295–1313. [CrossRef]
40. Sarkar, S.; Khouzani, M.H.R.; Kar, K. Optimal Routing and Scheduling in Multihop Wireless Renewable Energy Networks. *IEEE Trans. Autom. Control* **2013**, *58*, 1792–1798. [CrossRef]
41. Liu, G.Y.; Peng, B.H.; Zhong, X.J.; Cheng, L.F.; Li, Z.F. Attack-Defense Game between Malicious Programs and Energy-Harvesting Wireless Sensor Networks Based on Epidemic Modeling. *Complexity* **2020**, *2020*, 3680518. [CrossRef]
42. Van den Diressche, P.; Watmough, J. Further notes on the basic reproduction number. In *Mathematical Epidemiology*; Brauer, F., van den Driessche, P., Wu, J., Eds.; Springer: Berlin, Germany, 2008; pp. 159–178.

43. Lyapunov, A.M. The general problem of the stability of motion. *Int. J. Control* **1992**, *55*, 531–534. [CrossRef]
44. Lasalle, J.P. *The Stability of Dynamical Systems*; SIAM: Philadelphia, PA, USA, 1976.
45. Merkin, D.R. *Introduction to the Theory of the Stability*; Springer: New York, NY, USA, 2012; Volume 24.
46. Robinson, R.C. *An Introduction to Dynamical Systems: Continous and Discrete*; Pearson Education; Prentice Hall: Upper Saddle River, NJ, USA, 2004.