Hindawi
Complexity
Volume 2020, Article ID 5686413, 13 pages
https://doi.org/10.1155/2020/5686413

Research Article

Differential Games of Rechargeable Wireless Sensor Networks against Malicious Programs Based on SILRD Propagation Model

Guiyun Liu, Baihao Peng, Xiaojing Zhong, and Xuejing Lan

School of Mechanical and Electric Engineering, Guangzhou University, Guangzhou 510006, China

Correspondence should be addressed to Baihao Peng; 2111807063@e.gzhu.edu.cn

Received 2 May 2020; Revised 4 June 2020; Accepted 10 June 2020; Published 3 July 2020

Academic Editor: Shuping He

Based on the traditional propagation model, this paper innovatively divides nodes into high- and low-energy states through introducing Low-energy (L) state and presents a whole new propagation model which is more suitable for WSNs (wireless sensor networks) against malicious programs, namely, SILRD (Susceptible, Infected, Low-energy, Recovered, Dead) model. In this paper, nodes are divided into five states according to the residual energy and infection level, and the differential equations are constructed to describe the evolution of nodes. At the same time, aiming at the exhaustion of WSNs' energy, this paper introduces charging as a method to supplement the energy. Furthermore, we regard the confrontation between WSNs and malicious programs as a kind of game and find the optimal strategies by using the Pontryagin Maximum Principle. It is found that charging as a defense mechanism can inhibit the spread of malicious programs and reduce overall costs. Meanwhile, the superiority of bang-bang control on the SILRD model is highlighted by comparing with square control.

1. Introduction

WSNs consist of a series of energy-limited nodes with monitoring, receiving, transmitting, and other functions that act as connections between surrounding environment and control centers or computers for further process. As WSNs have gradually penetrated into every aspect of our daily life, they have become an indispensable part of us, including environmental monitoring, medical care, and vehicle tracking [1].

However, the shortcomings of WSNs are increasingly exposed, such as vulnerability to malicious programs and limited battery capacity. Due to the similarity of transmission mechanism, the propagation of malicious programs in WSNs can be modeled by imitating the theory of epidemiology. After decades of research studies of the initial SIR (Susceptible, Infected, Removed) model proposed by Kephart and White [2], the epidemiological model has been fully developed [3–6].

Many scholars are also devoted to the study of malicious programs' propagation mechanism in WSNs. In order to better protect against worm theft of security-critical information, Haixia Peng et al. proposed a reliability-oriented local-area model, which considers the topology of WSNs [7]. Based on the actual scenario, Akansha Singh et al. proposed a mathematical model that considered the influence of node distribution density and different communication radius on worm propagation [8]. Mohammad Sayad Haghighi et al. proposed a dynamic propagation model with the consideration of geospatial limitation [9]. Shakya [10] and Bahi et al. [11] have even considered the spatial correlations in WSNs. Bo Qu and Wang added nodal degree into the model as a factor affecting the infection rates [12]. The sleep and work interleaving policy was incorporated in a multiworm propagation model proposed by [13]. Tang also introduced sleep pattern to enhance the defense of WSNs [14]. In mobile WSNs, the operations of providing pulse immunization to susceptible nodes can well resist the propagation of malware [15]. Compared with static defensive measures, mobile patching is more effective in suppressing the spread of mobile sensor worms [16]. Nicola Roberto Zema et al. also

used a mobile approach to repair WSNs [17]. By adding time delay to the propagation model, Neha Keshri et al. found it could reduce the damage to nodes [18]. Many scholars have considered the energy problem of WSNs, for example, Lei Mo et al. introduced a mobile charger to add energy to the networks [19]. However, it is not difficult to find that the nodal energy is basically not taken into account in the classification criteria of different states of nodes. One of the highlights of this paper is that the energy of nodes has been put forward and divided into high- and low-energy state further. At the same time, the SILRD (Susceptible, Infected, Low-energy, Recovered, Dead) model is proposed in this paper according to the nodal states.

As it is a problem of antagonism against malicious programs, some of the scholars also used game theory to get the optimal strategy in the nonlinear system. By reducing the transmission range to suppress the spread of malicious programs, M. H. R. Khouza-ni et al. obtained the optimal transmission range by constructing the optimal control model [20] and also considered bandwidth consumption and invasion risk as an optimal problem [21]. Mohamed S. Abdalzaher and Osamu Muta proposed a Stackelberg game approach to improve the defense mechanisms of WSNs against the spectrum sensing data falsification attack [22]. As a study of nonlinear systems, Chenglong Wang et al. studied the problem of online adaptive optimal controller with input time delays [23]. Shuping He et al. proposed a scheme of online $H\infty$ control laws for nonlinear systems [24]. Chengcheng Ren et al. designed a suitable distributed controller [25] and a suitable finite-time stabilizable controller [26] to guarantee the positiveness and stabilization of the closed-loop systems. As an inseparable part of game theory, differential game has advantages in dealing with dynamic problems. Miao and Li exploited differential game to construct the optimal problem between network systems and attackers [27]. Miao figured out the optimum between throughput and energy efficiency [28]. Dong HAO and Kouichi SAKURAI defined a game called PUE attack game between attackers and secondary users [29]. Ding et al. constructed a differential game between two types of nodes in WSNs [30]. In addition to various game theories, Shuping He et al. also used reinforcement learning [31] and policy iteration algorithm [32] to solve the problem of optimal control. Differential game can also solve different kinds of problems: multiagent collision prevention [33], multipath routing optimization [34], optimal storage capacities [35], and minimization of transmission cost [36]. At the same time, linear programming can also be used to find the optimal solution [37]. In this paper, the optimal dynamic game strategies between the malicious programs and WSNs are obtained by using Pontryagin's Maximum Principle.

Our contributions are summarized below.

First, an improvement on the basic epidemiological model has been proposed. Considering the energy storage of WSNs, the low-energy state to further satisfy the feature of WSNs has been introduced. In the actual situation, nodes will consume their energy as a result of daily work, and they will definitely undergo a process from full energy to low energy. Meanwhile, since the attack of some malicious programs will be embodied in the faster consumption of energy, the introduction of low-energy state can reflect the attack degree to some extent.

Second, the effect of rechargeable factor on WSNs has been considered. In order to maintain the normal function of WSNs, the rechargeable factor is introduced. As one of the main defects of WSNs, limited energy has been restricted the lifetime of WSNs, for nodes, which are infected by a certain kind of malicious programs, can consume energy quickly. Thus, the influence of malicious programs can be suppressed by charging. As the number of low-energy nodes decreases, the cost of WSNs' operation increases by deploying UAVs. Therefore, this paper will reveal the balance between the two. At the same time, the validity of the control method in the SILRD model is further explained.

The rest of our paper is organized as follows. In Section 2, SILRD model with low-energy state has been proposed. At the same time, the influence of rechargeable factors on WSNs is considered and the corresponding differential equations are formulated. In Section 3, differential game has been used to figure out optimal strategies applied by WSNs and malicious programs. In Section 4, the evolution of nodal states, the flow of nodal energy, and the games between WSNs and malicious programs will be revealed by simulation. In Section 5, a conclusion of the full paper is presented here.

2. SILRD Model with WSNs

In WSNs, the total number of identical and static nodes is N and they are distributed randomly in a flat area with S (m^2). Each node is equipped with an antenna for messaging and a receiver for wireless charging. The maximum radius of node's transmission is r (m). In this section, the SILRD model will be proposed, and the differential equations will dynamically reflect the transition of nodal states.

2.1. Nodal States in WSNs. At the same time, charging is happening all the time in WSNs. This model assumes the attack from only one type of malicious program, that is, the recovered nodes will not be repeatedly infected. Each node transmits information to their surrounding nodes, which will relay the information to remote computer or control center step by step. Malicious programs propagate through information transmission between nodes. Once infected with malicious programs, the nodes will consume their energy at a faster rate.

Based on the traditional model, the SILRD model further considers energy level of each nodes and classifies nodes into the following five states:

Susceptible (S): a node in the Susceptible state is extremely vulnerable to malicious programs because of its lack of defenses. Energy consumption level of these nodes is normal.

Infected (I): a node in the Infected state has a rapid increase in energy consumption due to the successful infection of malicious programs. If infected nodes are not patched or charged in time, they will die of exhaustion.

Low-energy (L): nodes in the Low-power state are those that are infected with malicious programs or that consume energy normally. These nodes are characterized by low-energy level so that they cannot maintain normal work, including data transmission between nodes.

Recovered (R): a node in the Recovered state is immune to malicious programs. Particularly, charging and patching occur at the same time. In other words, nodes in recovered state are possessing not only immunity but also a high-energy level.

Dead (D): a node in the Dead state is completely dysfunctional. Even charging such a node cannot restore it. Meanwhile, this part of nodes due to total loss of energy is unable to infect its neighbors.

In this paper, $S(t)$, $I(t)$, $R(t)$, $L(t)$, and $D(t)$ are the ratio of susceptible, infected, recovered, low-energy, and dead nodes at time t, respectively. The sum of these five ratios is equal to 1. Thus, the following equation must be satisfied:

$$S(t) + I(t) + R(t) + D(t) + L(t) = 1. \quad (1)$$

2.2. Transitions between Nodal States in SILRD Model. Before the game started, only susceptible nodes and infected nodes existed in WSNs, and their sum is equal to N. Furthermore, the death of nodes because of hardware damage or environmental factors have not been considered in this paper.

The transmission range of each node is πr^2 (m^2). The density of susceptible nodes in WSNs is $(S(t)/S)$. For an infected node, the number of susceptible nodes around which it can infect is $(\pi r^2 S(t)/S)$. Therefore, in whole WSNs, the number of susceptible nodes infected by malicious programs is $\pi r^2 I(t) S(t)/S$.

In this model, the number of sensor nodes does not increase. Before WSNs were not infected by malicious programs, nodes in WSNs normally collect different kinds of environmental information and transmit the processed messages to their surrounding nodes. Malicious programs are artificially implanted into WSNs. Besides destroying the functionality of nodes, malicious programs can eavesdrop on information through transmission between nodes. In the absence of rechargeable devices, nodes will eventually shut down as the power runs out.

It is necessary to charge WSNs because of the consumption of electricity caused by normal work and the attack by malicious programs. Infected nodes spread malicious programs to neighbors with a certain probability. Susceptible nodes which receive malicious programs and get infectivity will become infected nodes. Some susceptible nodes have not been infected by malicious programs during their lifetime and remain in the normal working state. This part of the nodes will be transferred directly from the susceptible state to low-energy state without recharging by UAVs (Unmanned Aerial Vehicles) or the other MCs (Moving Chargers). Some susceptible nodes will gain immunity to this type of malicious programs in time by receiving and installing patches from the UAVs. The rest of susceptible nodes will keep staying into the normal state. Specifically, two simple schematic diagrams of the scene of the SILRD model have also been portrayed, and the states evolutions of nodes covered during the UAV movement are clearly visible, as depicted in Figure 1.

The transmission capacity of malicious programs directly determines the number of nodes transmit from the susceptible state to infected state. Infected nodes dissipate their own energy by enhancing the frequency of information acquisition and the strength of communication with surrounding nodes. With the increasing damage degree of malicious programs, nodes will enter into the dead state at a faster speed. At the same time, malicious programs can also choose not to continue to attack the infected nodes, and these infected nodes are only infectious but not destructive. However, if the patches carried by UAVs are timely and successfully installed early, the nodes will safely convert to the recovered state.

Nodes in the recovered state are not only immune to the malicious programs but also in a high-energy level. Nodes that move from susceptible and infected states to recovered states are in high-energy level, and UAVs only need to transmit patches without charging them. On the contrary, nodes in the low-energy state need to be charged and patched at the same time to transform to the recovered state, even if the nodes in the recovered state shift to the low-energy state without energy replenishment due to normal consumption.

Some of the nodes in the low-energy state are immune, while others are not. Nodes in the low-energy state will exhaust quickly, and the effect of malicious programs on nodes transmitting from the low-energy state to dead state has been ignored. The flow diagram of the SILRD propagation model is shown in Figure 2.

The transition probability from the susceptible state to infected state due to being infected by malicious programs is P_{SI}. The probability of the susceptible nodes moves from the high-energy level to low-energy level due to normal operation is P_{SL}. Probability of susceptible nodes being patched by UAVs is P_{SR}. The probability that infected nodes will be repaired while still at high-energy level is P_{IR}. The probability that infected nodes are destroyed by malicious programs and squander energy until exhaustion is P_{ID}. Malicious programs in some infected nodes stop destroying, at this time, these infected nodes can work normally with probability P_{IL} at the low-energy state. The probability of nodes at the low-energy level being successfully charged and patched by UAVs before they run out of energy is P_{LR}. The probability of immune nodes entering the low-energy level due to daily collection and transmission is P_{RL}. Finally, the probability of death due to exhaustion at the low-energy level is P_{LD}. The rate of change in each state is formulated from

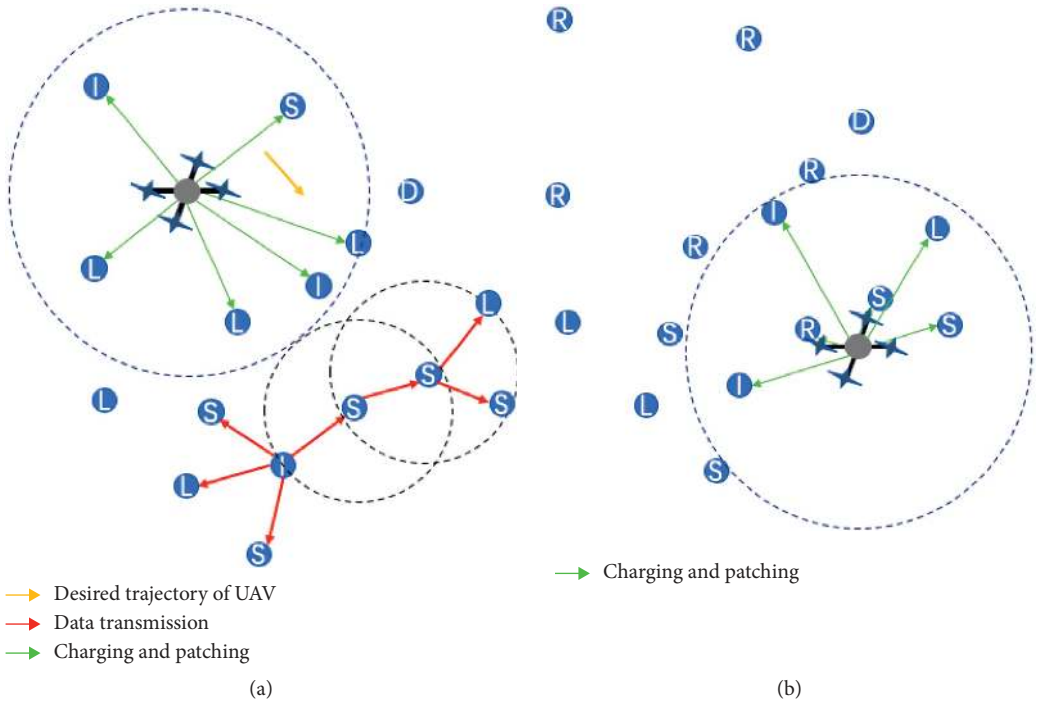

Figure 1: Evolution of nodal states in UAV coverage area. (a) The location of the UAV at a certain moment and the nodal states before UAV moves. (b) The evolution of Nodal states as a result of the UAV moving with the desired trajectory from the original position.

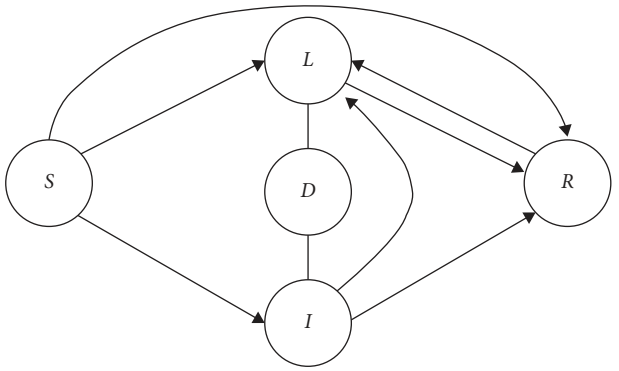

Figure 2: The flow diagram of the propagation model. The letters in the circle represent the corresponding state of the node. Arrows indicate the direction of transition between node states.

$$\frac{dS(t)}{dt} = -P_{SI}\pi r^2 \frac{S(t)I(t)}{S} - P_{SR}S(t) - P_{SL}S(t), \tag{2}$$

$$\frac{dI(t)}{dt} = P_{SI}\pi r^2 \frac{S(t)I(t)}{S} - P_{IR}I(t) - P_{IL}I(t) - P_{ID}I(t), \tag{3}$$

$$\frac{dL(t)}{dt} = P_{IL}I(t) + P_{SL}S(t) - P_{LR}L(t) - P_{LD}L(t) + P_{RL}R(t), \tag{4}$$

$$\frac{dR(t)}{dt} = P_{IR}I(t) + P_{SR}S(t) + P_{LR}L(t) - P_{RL}R(t), \tag{5}$$

$$\frac{dD(t)}{dt} = P_{LD}L(t) + P_{ID}I(t). \tag{6}$$

2.3. The Introduction of Control Variables. In this paper, the damage caused by malicious programs to WSNs is mainly reflected in the conversion process from the infected state to dead state. At the same time, the propagation ability of malicious programs depends not only on the transmission frequency between nodes but also on themselves. Therefore, attack modes of malicious programs include the destruction of WSNs and their propagation.

The defense measures of WSNs are embodied in charging and patching various nodes. Charging nodes in different types of states by UAVs can not only prolong the lifespan of WSNs but also mitigate the damage from malicious programs to some degree. Patching a node can make it immune to the corresponding malicious programs. Thus, the defense patterns of WSNs are manifested in the supplement of node electricity and the provision of relevant patches.

According to the effects of the attack and defense measures on nodal states, two hypotheses have been proposed. One is that P_{SI} and P_{ID} are controlled by malicious programs to some degree. The higher the attack level of the malicious programs, the higher these two probabilities. The other is that P_{SR}, P_{IR}, and P_{LR} are controlled by WSNs to some degree. Similarly, the higher the defense level of WSNs, the higher the probability of all three.

To further formulate this five transition probabilities, equation (7) has been put forward:

$$\begin{cases} P_{\mathrm{SI}} = \dfrac{A_{\mathrm{SI}} L_{\mathrm{SI}}}{A_{\mathrm{SImax}} + A_{\mathrm{SImin}}}, \\ P_{\mathrm{ID}} = \dfrac{A_{\mathrm{ID}} L_{\mathrm{ID}}}{A_{\mathrm{IDmax}} + A_{\mathrm{IDmin}}}, \\ P_{\mathrm{SR}} = \dfrac{D_{\mathrm{SR}} L_{\mathrm{SR}}}{D_{\mathrm{SRmax}} + D_{\mathrm{SRmin}}}, \\ P_{\mathrm{IR}} = \dfrac{D_{\mathrm{IR}} L_{\mathrm{IR}}}{D_{\mathrm{IRmax}} + D_{\mathrm{IRmin}}}, \\ P_{\mathrm{LR}} = \dfrac{D_{\mathrm{LR}} L_{\mathrm{LR}}}{D_{\mathrm{LRmax}} + D_{\mathrm{LRmin}}}, \end{cases} \tag{7}$$

where A_{SI} and A_{ID} represent the control levels of malicious programs, while L_{SI} and L_{IL} represent the probability of successful attack by malicious programs. In the same way, D_{SR}, D_{LR}, and D_{IR} represent the control level of WSNs, while L_{SR}, L_{IR}, and L_{LR} represent the probability of successful defense. A_{SImin} and A_{SImax} represent the minimum and maximum values of malicious program's control level, respectively, so do the other counterparts in equation (7).

The success rates of infection and suppression are all on a scale of 0 to 1, as shown below:

$$L_{\mathrm{SI}}, L_{\mathrm{ID}}, L_{\mathrm{SR}}, L_{\mathrm{IR}}, L_{\mathrm{LR}} \in [0, 1]. \tag{8}$$

3. Optimal Dynamic Game Strategies for the Malicious Programs and WSNs

As an important branch of game theory, differential game is the theory which both parties can make decisions freely proposed by Isaac in solving the pursuit evasion problem in 1965 [38]. Differential game refers to the game played by multiple players in a continuous time system. At the same time, players in the system try to optimize their independent and ambivalent goals and finally obtain the optimal strategies of the players over time. Generally speaking, differential game is a theory to study the decision-making process of two or more players when their controls are applied to a dynamical system described by differential equations. In the differential game, figuring out a saddle point is the same thing as finding out Nash equilibrium. In this section, the cost of the game is formulated by further description of the flow diagram, and the optimal dynamic strategies of both sides of the game are constructed according to Pontryagin's Maximum Principle.

3.1. Payoff Function in the Attack-Defense Game. In this paper, the zero-sum noncooperative differential game between malicious programs and WSNs has been discussed. The goal of malicious programs is to maximize the payoff while the networks want to minimize it. After analysis by Pontriagin's Maximum Principle, the optimal attack strategy for malicious programs has been obtained, and WSNs also have the corresponding optimal countermeasures.

Definition 1. Given a fixed duration T, $\nu(t) = (A_{\mathrm{SI}}(t), A_{\mathrm{ID}}(t))$ is a strategy set of malicious programs at time t. Identically, $\mu(t) = (D_{\mathrm{SR}}(t), D_{\mathrm{IR}}(t), D_{\mathrm{LR}}(t))$ is a strategy set of WSNs at time t.

In addition to the costs cause by malicious programs' attack, WSNs themselves will generate a variety of costs with time.

Nodes in the infected state, by destroying the transmission mechanism between nodes, lose plenty of their own energy and bring to a certain cost. Moreover, such nodes also cause unexpected losses through eavesdropping on WSNs. Although nodes in the low-energy state do not have the ability to propagate malicious programs, they cannot work normally due to the low-energy level, which will definitely engender much losses. As a result of complete loss of function of the dead node, topological structure of WSNs will be disrupted. In the reconstruction of the new transmission mechanism, it is bound to incur additional costs. Multiple UAVs charge or patch corresponding nodes by carrying patches and energy to some area of WSNs. During the flight of the UAVs, a part of electricity will be consumed, and it will be consumed in the process of SWIPT (simultaneous wireless information and power transfer) of UAVs.

While malicious programs create networks' losses, WSNs' own defense measures will make up for this losses. The purpose of malicious programs is to make them as greater as possible, whereas WSNs do the opposite, thus forming two sides of the game.

By patching susceptible nodes, they will be immune to some malicious programs, which ensures normal operation of WSNs in the future. The infected node returns to the normal state, which not only reduces the loss that should have occurred but also guarantees the normal operation for a period of time. In addition to the low-energy levels, nodes in the low-energy state are likely to contain more malicious programs. Therefore, it should not only be replenished with energy but also be patched to make it immune.

The risk posed by infected nodes spreading malicious programs is $C_I I(t)$ at time t, where C_I is a cost coefficient and $C_I \geq 0$. The consumption caused by using UAVs to repair nodes while replenishing the node energy is $C_{\mathrm{LR}} P_{\mathrm{LR}} L(t)$ at time t, where $C_{\mathrm{LR}} \geq 0$. The cost of losing some functions due to nodes at low-energy levels is $C_L L(t)$ at time t, where $C_L \geq 0$. Loss of WSNs' failure due to nodes death is $C_D D(t)$ at time t, where $C_D \geq 0$. Nodes have positive benefits $C_R R(t)$ at time t due to having immunity, where $C_R \geq 0$. The costs of patching susceptible and infected nodes are $C_{\mathrm{SR}} P_{\mathrm{SR}} S(t)$ and $C_{\mathrm{IR}} P_{\mathrm{IR}} I(t)$ at time t, respectively, where $C_{\mathrm{SR}} \geq 0$ and $C_{\mathrm{IR}} \geq 0$. Nodes in the susceptible state have $C_S S(t)$ benefit from working normally at time t, where $C_S \geq 0$. At the terminal moment, susceptible and recovered nodes will bring future benefits, so $C_{S_f} S(t_f)$ and $C_{R_f} R(t_f)$ will be used to measure these benefits, where $C_{S_f} \leq 0$ and $C_{R_f} \leq 0$. Conversely, nodes in the infected, low-energy, and dead states will continue to affect the networks. $C_{I_f} I(t_f)$,

$C_{L_f}L(t_f)$, and $C_{D_f}D(t_f)$ will be used to describe these costs, where $C_{I_f} \geq 0$, $C_{L_f} \geq 0$, and $C_{D_f} \geq 0$.

The payoff function of this game is shown in

$$J(\mu(t), \nu(t)) = \int_{t_0}^{t_f} \{-C_S S(t) + [C_I + C_{\mathrm{IL}}P_{\mathrm{IL}} + C_{\mathrm{PATCH}}P_{\mathrm{IR}}]I(t) - C_R R(t) + C_D D(t) + [C_{\mathrm{LR}}P_{\mathrm{LR}} + C_L]L(t) + C_{\mathrm{PATCH}}P_{\mathrm{SR}}S(t)\}\mathrm{d}t + C_{S_f}S(t_f) + C_{I_f}I(t_f) + C_{\mathrm{PATCH}}P_{\mathrm{SR}}S(t)\mathrm{d}t + C_{S_f}S(t_f) + C_{I_f}I(t_f). \tag{9}$$

According to the payoff function, we have ϕ to determine terminal constraint of the game, as depicted in the following equation:

$$\phi = C_{S_f}S(t_f) + C_{I_f}I(t_f) + C_{L_f}L(t_f) + C_{R_f}R(t_f) + C_{D_f}D(t_f). \tag{10}$$

3.2. Optimal Dynamic Strategies in the Attack-Defense Game

Theorem 1. *In the Attack-Defense game in the SILRD model, the optimal dynamic strategies of malicious programs and WSNs are*

$$A_{SI}^* = \begin{cases} A_{\mathrm{SImax}}, & \beta_{SI} > 0, \\ \text{unknown}, & \beta_{SI} = 0, \\ A_{\mathrm{SImin}}, & \beta_{\mathrm{SI}} < 0, \end{cases}$$

$$A_{\mathrm{ID}}^* = \begin{cases} A_{\mathrm{IDmax}}, & \beta_{\mathrm{ID}} > 0, \\ \text{unknown}, & \beta_{\mathrm{ID}} = 0, \\ A_{\mathrm{IDmin}}, & \beta_{\mathrm{ID}} < 0, \end{cases}$$

$$D_{\mathrm{SR}}^* = \begin{cases} D_{\mathrm{SRmin}}, & \beta_{\mathrm{SR}} > 0 \\ \text{unknown}, & \beta_{\mathrm{SR}} = 0, \\ D_{\mathrm{SRmax}}, & \beta_{\mathrm{SR}} < 0, \end{cases} \tag{11}$$

$$D_{\mathrm{IR}}^* = \begin{cases} D_{\mathrm{IRmin}}, & \beta_{\mathrm{IR}} > 0, \\ \text{unknown}, & \beta_{\mathrm{IR}} = 0, \\ D_{\mathrm{IRmax}}, & \beta_{\mathrm{IR}} < 0, \end{cases}$$

$$D_{\mathrm{LR}}^* = \begin{cases} D_{\mathrm{LRmin}}, & \beta_{\mathrm{LR}} > 0, \\ \text{unknown}, & \beta_{\mathrm{LR}} = 0, \\ D_{\mathrm{LRmax}}, & \beta_{\mathrm{LR}} < 0, \end{cases}$$

where β_{SI}, β_{ID}, β_{SR}, β_{IR}, and β_{LR} satisfy the following equation:

$$\beta_{\mathrm{SI}} = \frac{[\lambda_I(t) - \lambda_S(t)]\pi r^2 L_{\mathrm{SI}}(S(t)I(t)/S)}{A_{\mathrm{SImax}} + A_{\mathrm{SImin}}},$$

$$\beta_{\mathrm{ID}} = \frac{[\lambda_D(t) - \lambda_I(t)]L_{\mathrm{ID}}I(t)}{A_{\mathrm{IDmax}} + A_{\mathrm{IDmin}}},$$

$$\beta_{\mathrm{SR}} = \frac{[\lambda_R(t) - \lambda_S(t) + C_{\mathrm{PATCH}}]L_{\mathrm{SR}}S(t)}{D_{\mathrm{SRmax}} + D_{\mathrm{SRmin}}}, \tag{12}$$

$$\beta_{\mathrm{IR}} = \frac{[\lambda_R(t) - \lambda_I(t) + C_{\mathrm{PATCH}}]L_{\mathrm{IR}}I(t)}{D_{\mathrm{IRmax}} + D_{\mathrm{IRmin}}},$$

$$\beta_{\mathrm{LR}} = \frac{[\lambda_R(t) - \lambda_L(t) + C_{\mathrm{LR}}]L_{\mathrm{LR}}L(t)}{D_{\mathrm{LRmax}} + D_{\mathrm{LRmin}}}.$$

Proof. According to (2)–(6) and (8), we can construct the Hamiltonian function as shown below:

$$H = \lambda_S(t)\frac{S(t)}{\mathrm{d}t} + \lambda_I(t)\frac{I(t)}{\mathrm{d}t} + \lambda_L(t)\frac{L(t)}{\mathrm{d}t} + \lambda_R(t)\frac{R(t)}{\mathrm{d}t} + \lambda_D(t)\frac{D(t)}{\mathrm{d}t} - C_S S(t) + C_I I(t) - C_R R(t) + C_L L(t) + C_D D(t) - C_{\mathrm{LR}}P_{\mathrm{LR}}L(t) - C_{\mathrm{IR}}P_{\mathrm{IR}}I(t) + C_{\mathrm{SR}}P_{\mathrm{SR}}S(t). \tag{13}$$

From state functions (2)–(6) and payoff function (8), the following characteristics have been found out:

1 The five state functions and the payoff function are all continuous in time

2 The control variables are all bounded and continuous in the state functions and payoff function

Thus, there must exist a saddle point $(\mu^*(t), \nu^*(t))$ that meets (14) according to [39]:

$$J(\mu^*(t), \nu(t)) \leq J(\mu^*(t), \nu^*(t)) \leq J(\mu^*(t), \nu^*(t)), \tag{14}$$

where $J(\mu^*(t), \nu(t))$ represents the cost incurred when only the optimal strategy is selected by WSNs. $J(\mu^*(t), \nu(t))$ also

denotes that only malicious programs choose the optimal strategy. $J(\mu^*(t), \nu(t))$ indicates that not only the networks choose the optimal strategy but also malicious programs choose the optimal strategy.

According to [40] and the characteristics of this model, there must be a V satisfying

$$V = \max_{\nu(t)}\min_{\mu(t)} J(\mu(t), \nu(t)) = \min_{\mu(t)}\max_{\nu(t)} J(\mu(t), \nu(t)) = J(\mu^*(t), \nu^*(t)), \tag{15}$$

where $\max_{\nu(t)}\min_{\mu(t)} J(\mu(t), \nu(t))$ represents the cost incurred by WSNs in selecting the optimal strategy after the malicious programs makes optimal decision, while $\min_{\mu(t)}\max_{\nu(t)} J(\mu(t), \nu(t))$ denotes the cost incurred when the order of two sides is switched.

The following co-state differential equations (16)–(20) determine the co-state variables $\lambda_S(t)$, $\lambda_I(t)$, $\lambda_R(t)$, $\lambda_L(t)$, and $\lambda_D(t)$, which are all time dependent:

$$\frac{d\lambda_S(t)}{dt} = -\frac{dH}{dS(t)} = \frac{[\lambda_S(t) - \lambda_I(t)]\pi r^2 I^*(t) A_{SI}^* L_{SI}}{(A_{SImax} + A_{SImin})S} + C_S - \frac{C_{PATCH} D_{SR}^* L_{SR}}{D_{SRmax} + D_{SRmin}} + [\lambda_S(t) - \lambda_L(t)]P_{SL} + \frac{[\lambda_S(t) - \lambda_R(t)]D_{SR}^* L_{SR}}{D_{SRmax} + D_{SRmin}}, \tag{16}$$

$$\frac{d\lambda_S(t)}{dt} = -\frac{dH}{dI(t)} = \frac{[\lambda_S(t) - \lambda_I(t)]\pi r^2 S^*(t) A_{SI}^* L_{SI}}{(A_{SImax} + A_{SImin})S} - C_I + \frac{[\lambda_I(t) - \lambda_R(t)]D_{IR}^* L_{IR}}{D_{IRmax} + D_{IRmin}} - \frac{C_{PATCH} D_{IR}^* L_{IR}}{D_{IRmax} + D_{IRmin}} + [\lambda_I(t) - \lambda_L(t)]P_{IL} + (\lambda_I(t) - \lambda_D(t))A_{ID}^* L_{ID}, \tag{17}$$

$$\frac{d\lambda_L^*(t)}{dt} = -\frac{dH}{dL(t)} = \frac{[\lambda_L(t) - \lambda_R(t)]D_{LR}^* L_{LR}}{D_{LRmax} + D_{LRmin}} + [\lambda_L(t) - \lambda_D(t)]P_{LD} - C_L - \frac{C_{LR} D_{LR}^* L_{LR}}{D_{LRmax} + D_{LRmin}}, \tag{18}$$

$$\frac{d\lambda_R^*(t)}{dt} = -\frac{dH}{dR(t)} = [\lambda_L(t) - \lambda_R(t)]P_{RL} + C_R, \tag{19}$$

$$\frac{d\lambda_D^*(t)}{dt} = -\frac{dH}{dD(t)} = -C_D. \tag{20}$$

Meanwhile, the terminal value of the co-state variables satisfies

$$\begin{cases} \lambda_S(t_f) = \dfrac{d\phi}{dS(t)} = C_{S_f}, \\ \lambda_I(t_f) = \dfrac{d\phi}{dI(t)} = C_{I_f}, \\ \lambda_L(t_f) = \dfrac{d\phi}{dL(t)} = C_{L_f}, \\ \lambda_R(t_f) = \dfrac{d\phi}{dR(t)} = C_{R_f}, \\ \lambda_D(t_f) = \dfrac{d\phi}{dD(t)} = C_{D_f}. \end{cases} \tag{21}$$

According to Pontryagin's Maximum Principle, when $([\lambda_I(t) - \lambda_S(t)]\pi r^2 L_{SI}(S(t)I(t)/S)/A_{SImax} + A_{SImin})$ is greater than 0, the malicious programs will choose the maximum control A_{SImax} in order to make the cost as large as possible. On the contrary, supposing $([\lambda_I(t) - \lambda_S(t)]\pi r^2 L_{SI}(S(t)I(t)/S)/A_{SImax} + A_{SImin})$ is less than 0, the malicious programs will choose the minimum control A_{SImax} to maximize the cost. Similarly, when $[\lambda_D(t) - \lambda_I(t)]L_{ID}I(t)/(A_{IDmax} + A_{IDmin})$ is greater than 0, the malicious programs will choose A_{IDmax}, and the malicious programs will choose A_{IDmin} if $[\lambda_D(t) - \lambda_I(t)]L_{ID}I(t)/(A_{IDmax} + A_{IDmin})$ is less than 0.

For WSNs, in case $[\lambda_R(t) - \lambda_S(t) + C_{PATCH}]L_{SR}S(t)/(D_{SRmax} + D_{SRmin})$is greater than 0, it will adopt the minimum control D_{SRmin} to make the cost as small as possible. Maximum control D_{SRmax} is taken to minimize the cost, when $[\lambda_R(t) - \lambda_S(t) + C_{PATCH}]L_{SR}S(t)/(D_{SRmax} + D_{SRmin})$is less than 0. In terms of restoration measures for infected nodes, if $[\lambda_R(t) - \lambda_I(t) + C_{PATCH}]L_{IR}I(t)/(D_{IRmax} + D_{IRmin})$is greater than 0, WSNs will choose the minimum control D_{IRmin}, while WSNs will choose the maximum control D_{IRmax} when $[\lambda_R(t) - \lambda_I(t) + C_{PATCH}]L_{IR}I(t)/(D_{IRmax} + D_{IRmin})$ is less than 0. WSNs also takes similar measures to nodes moving from the low-energy state to recovered state. The node will take the maximum control D_{LRmax} supposing $[\lambda_R(t) - \lambda_L(t) + C_{LR}]L_{LR}L(t)/(D_{LRmax} + D_{LRmin})$is less than 0, while the node will take the minimum control D_{LRmin} if $[\lambda_R(t) - \lambda_L(t) + C_{LR}]L_{LR}L(t)/(D_{LRmax} + D_{LRmin})$is greater than 0. □

4. Simulation

In this chapter, two parts are discussed. In the first part, based on the dynamic strategy, charging factor is further analyzed to illustrate its advantages. The second part will compare and analyze with other control combinations to highlight the points of bang-bang control. In these two parts, simulations are verified on MATLAB R2017 B and the memory specification of the computer is 8 GB 1600 MHz DDR3.

In our assumptions, nodes are distributed at random in a two-dimensional region with an area of 10,000 m^2. The maximum transmission radius of a node is 10 m, and the neighbor nodes must exist within the maximum transmission range of the nodes. UAVs will perform nodes' patching and wireless charging operations together. At the beginning of the game, most of the nodes are in the susceptible state, and the rest are in the infected state. The maximum value of all control levels is assumed to be 1, and the minimum value is assumed to be 0. The parameters are set as shown in Table 1. According to the Pontriagin Maximum Principle, the algorithm of the Attack-Defense Game based on the SILRD model will be briefly explained in the form of pseudocode in Algorithm 1.

4.1. Dynamic Strategies in the Game between WSNs and Malicious Programs. This section will focus on the evolution on different nodes, control rules, and overall costs. At the same time, it is worth noting that this section will compare the case of no energy input.

4.1.1. The Variation Trend of Nodal States. Here, the variation trend of each state quantity over time under two cases will be compared. In particular, similar state quantities are contrasted in one simulation diagram for further analysis. Each state quantity curve is constructed from 100 sample points. The number of each type of nodes is evolved based on (2)–(6). The difference between Figures 2 and 3 is whether or not charging involved.

It can be seen from the comparison between Figure 3(a) and Figure 3(b) that, in the SILRD model proposed in this paper, energy input, namely, charging, has little influence on the number of susceptible nodes and infected nodes because charging does not directly affect such high-energy nodes.

Although the curves of the same type of nodes are similar in both cases, there exist numerical difference. The number of recovered nodes increased to 17.1% with energy input, up by 6% compared with the case of no energy input, and low-energy and death nodes decreased by 1.8% and 4.1%.

4.1.2. Comparison of Dynamic Optimal Control. Here, the reason for the evolution of states' quantities will be investigated, that is, the change of control levels of both sides in the game. When $T = 0$, the initial value of each controls is assumed to be 1. The malicious programs select the strategy according to (9) and (10), and WSNs choose according to (11)–(13).

Malicious programs stopped propagation on the third day because the peak of infection has been arrived. Even so, the damage from malicious programs continued until the end of the game, that is, the malicious programs have not been cleaned up.

Similarly, WSNs stopped patching infected and susceptible nodes on the second day of the game, as depicted in Figures 4 and 5. Because malicious programs are no longer spreading, patching vulnerable nodes is not cost effective. The same applies to infected nodes. Even if the malicious programs still exist, it costs more to patch them, so it stops.

The difference between Figures 4 and 5 is that the former adds control over energy input to the networks. As can be seen from Figures 3(a) and 4, after the number of recovered nodes reaches a peak, WSNs stop the repair of low-energy nodes to suspend the cost of charging and patching.

4.1.3. Cost Comparison. The costs of four cases will be compared over here. Due to the impact of the dynamic strategies' end-values, only the cost simulation diagram when $T < 100$ will be shown and will explain in detail. The costs are all constructed according to equation (8).As can be seen from Figure 6, without taking the terminal cost ($T = 100$) into account, strategies with energy inputs can actually reduce cost than strategies without them. Therefore, it is not always good to charge, and sometimes it is more cost effective to use the networks' residual energy. In the first ten days, the difference between charging and noncharging strategies is nonsignificant. However, with the development of the iteration, the gap continues to expand. From the comparison of costs, the strategies with charging are cost-saving than those without charging. Thus, the benefits of charging can cover the costs of it. It is worth noting that when the charging power is slightly reduced to about 50%, the cost will decrease rapidly. And then as the power continues to drop to about 10%, the cost, at 43 days, exceeds the cost at full power.

However, the ranking of costs will change after the end values are taken into account. At this point, the cost order from high to low is strategies with 10% power charging (-5.9344×10^4), strategies with full-power charging (-9.9543×10^4), strategies without charging (-1.7139×10^5), and strategies with 50% power charging (-1.7772×10^5). Therefore, the maximum charging power is not necessary when WSNs are evenly replenished. Because larger power means more nodes are converted to the high-energy state, but costs are also rising. There must exist a number of tradeoffs that are lower than both full-power operation and no energy input, such as the 50% power in this paper.

4.2. Comparison of Differential Hybrid Control Strategies. In this section, four combination control strategies are discussed. In the above, both the control of patching and charging belong to bang-bang control. In order to highlight the advantages of bang-bang control in the SILRD model, this paper compares it with another common control method which only needs to expand the corresponding

Table 1: Experimental parameters.

Parameter	Description	Value
L_{SI}	Probability of nodes converting from the susceptible state to infected state	0.1
L_{ID}	Probability of nodes converting from the infected state to dead state	0.05
L_{SR}	Probability of nodes converting from the susceptible state to recovered state	0.2
P_{IL}	Probability of nodes converting from the infected state to low-energy state	0.005
L_{LR}	Probability of nodes converting from the low-energy state to recovered state	0.2
P_{SL}	Probability of nodes converting from the susceptible state to low-energy state	0.005
P_{LD}	Probability of nodes converting from the low-energy state to dead state	0.005
P_{RL}	Probability of nodes converting from the recovered state to low-energy state	0.005
C_{SR}	Cost of nodes converting from the susceptible state to recovered state	5
C_{IR}	Cost of nodes converting from the infected state to recovered state	7
C_S	Cost of nodes in the susceptible state	12
C_D	Cost of nodes in the dead state	20
C_I	Cost of nodes in the infected state	12
C_R	Cost of nodes in the recovered state	15
C_L	Cost of nodes in the low-energy state	15
C_{LR}	Cost of nodes converting from the low-energy state to recovered state	10
$S(0)$	The ratio of the initial number of susceptible nodes	95%
$I(0)$	The ratio of the initial number of infected nodes	5%
$L(0)$	The ratio of the initial number of low-energy nodes	0%
$R(0)$	The ratio of the initial number of recovered nodes	0%
$D(0)$	The ratio of the initial number of dead nodes	0%

(1) Initialize all coefficients;
(2) Define $\alpha(t) = \{S(t), I(t), L(t), R(t), D(t)\}$;
(3) Define $\beta(t) = \{\lambda_S(t), \lambda_I(t), \lambda_L(t), \lambda_R(t), \lambda_D(t)\}$;
(4) Define $\gamma(t) = \{\mu(t), \nu(t)\}$;
(5) **if** $t = 0$ **then**
(6) Substitute $\alpha(0)$ and $\gamma(0)$ into (2)–(6);
(7) Substitute $\alpha(0)$, $\beta(0)$ and $\gamma(0)$ into (17)–(21);
(8) end if
(9) **for** $t = 1$ to T **do**
(10) Substitute $\alpha(t)$ and $\gamma(t)$ into (2)–(6);
(11) Substitute $\alpha(t), \beta(t)$ and $\gamma(t)$ into (17)–(21);
(12) Substitute $\alpha(t+1)$ and $\beta(t+1)$ into (9)–(13);
(13) **end for**

Algorithm 1: Attack-Defense Game based on the SILRD Model.

control into second term, that is, replace D_{SR} with D_{SR}^2, D_{IR} with D_{IR}^2, and D_{LR} with D_{LR}^2. It is worth noting that the payoff function describing the game under square control does not change. According to the proof conditions of the Maximum Principle in [38], there still exist a pair of saddle points $(\mu^*(t), \nu^*(t))$ at this time, so the proofs will not be described here again.

For the convenience of the following description, this kind of control is named as square control in this paper. Bang-bang control and square control will alternate between charging process and patching process to form four different control combinations.

4.2.1. The Variation Trend of Nodal States. In particular, similar state quantities are contrasted in one simulation diagram for further analysis.

The trend of the number of susceptible nodes under four strategies is basically similar, as depicted in Figure 7(a). The number of susceptible nodes decayed most slowly when square control was only used to patch high-energy nodes. When the square control is used for charging low-energy nodes, the curves are fairly close. Therefore, if the aim of the network is to keep the number of susceptible nodes as high as possible, the bang-bang control can be applied to patching high-energy nodes and square control for charging and patching low-energy nodes.

As can be seen from Figure 7(b), if only the square control is used in WSNs, the number of infections will reach a very high peak at about 13%. Applying square control to patching high-energy nodes is more effective at suppressing the spread of malicious programs than just only using bang-bang control and its peak value is about 5.6%.

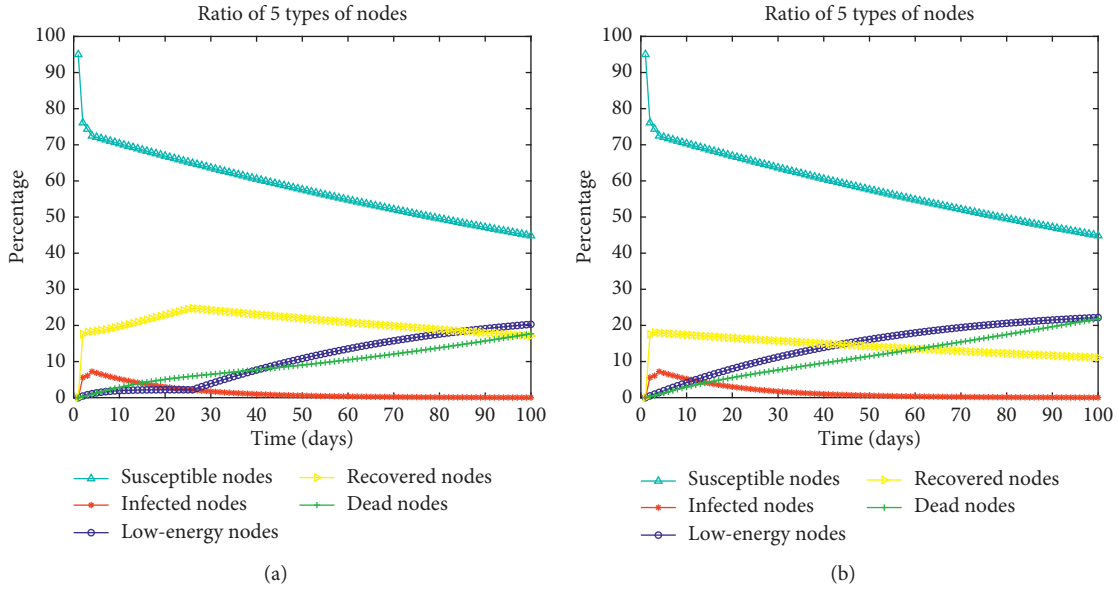

Figure 3: Evolution of five types of nodes. In order to emphasize the impact of charging, this experiment takes charging as a research factor. (a) The evolution of nodes under the condition of charging (i.e., with energy inputs). (b) The evolution of nodes under the condition of no charging (i.e., without energy input).

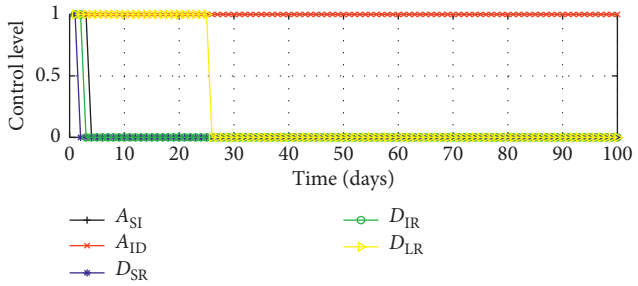

Figure 4: Optimal dynamic control with charging factors. This figure shows how the five control variables change over 100 days.

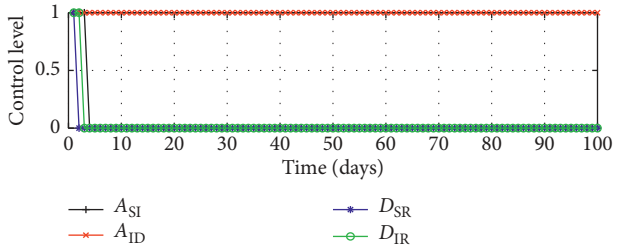

Figure 5: Optimal dynamic control without charging factors. The difference (Figure 4) is the change of the five control variables in the absence of UAVs within 100 days.

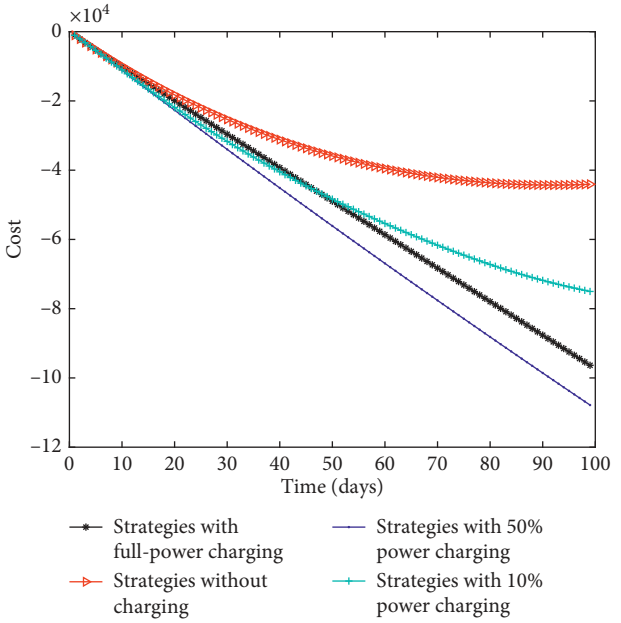

Figure 6: Cost comparison on four cases. The four cases differ in the level of charging power. The corresponding charging power levels of the curve from top to bottom are 0%, 10%, 100%, and 50%.

As can be seen from the comparison between Figures 7(c) and 7(d), when bang-bang control is only applied in WSNs, the number of low-energy nodes and recovered nodes are significantly changed. In Figures 7(c) and 7(d), the other three control combinations' evolution areas similarly. In other words, applying bang-bang control to charging and patching is more effective in suppressing low-energy nodes and boosting the number of recovered nodes. In particular, when only bang-bang control is applied, the peak value of recovered nodes can reach 25%.

All control combinations had lower mortality rates, as depicted in Figure 7(e). In the first six days, there was little difference in mortality among the combinations. For the first 41 days, applying bang-bang control and square control, respectively, to patching and charging had the lowest

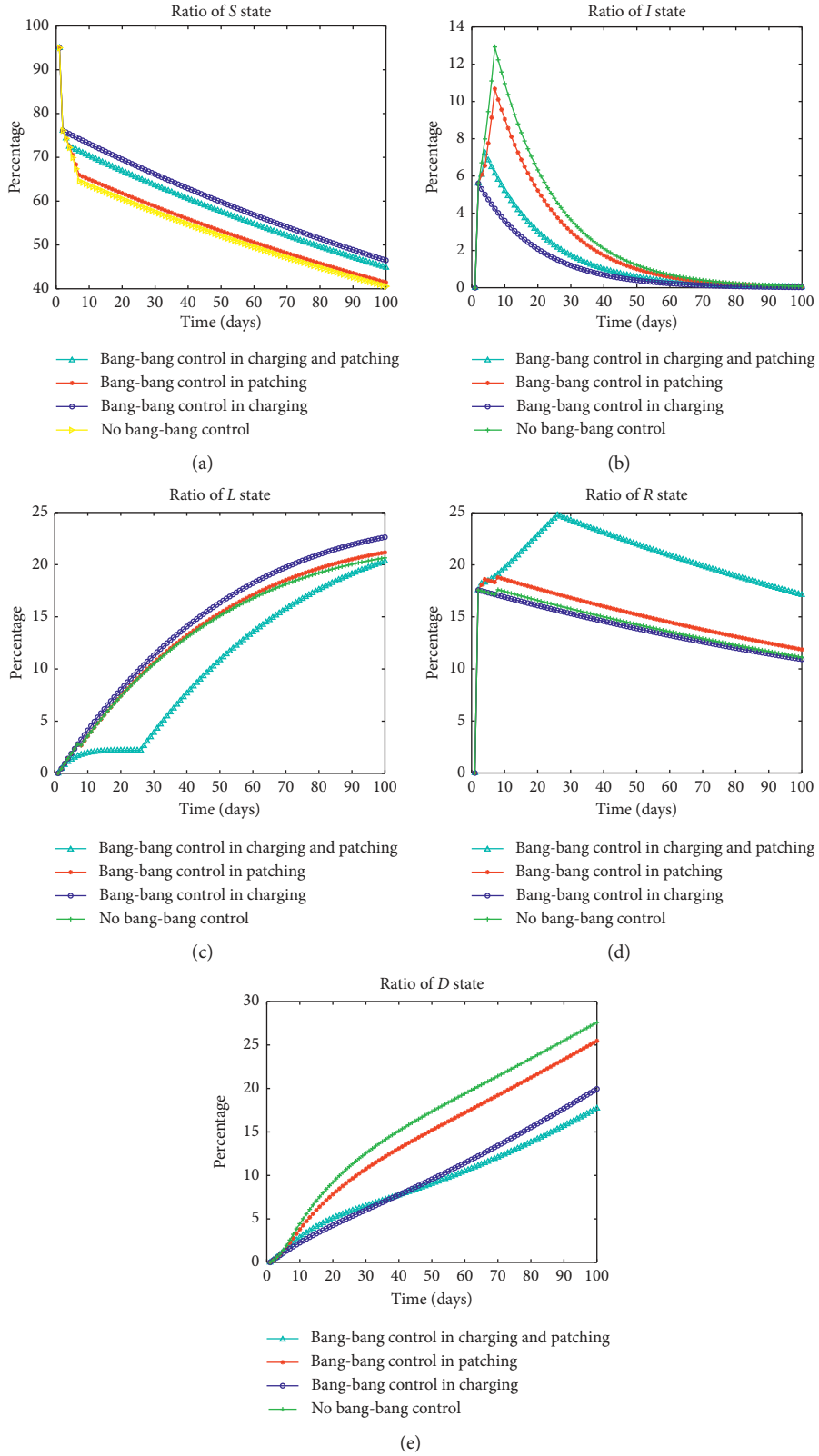

Figure 7: Evolution of five types of nodes under four control combinations. Unlike the previous section, the research factor considered in Section 4.2.1 is the control combination applied to charging and patching. This section considers the control combination of bang-bang control and square control. If bang-bang control is only applied to patching on high-energy nodes, then square control is applied to charging and patching on low-energy nodes. Similarly, if bang-bang control is used to low-energy nodes, then high-energy nodes use square control. If UAVs do not use bang-bang control, then they adopt square control. (a) The number of S-nodes. (b) The number of I-nodes. (c) The number of L-nodes. (d) The number of R-nodes. (e) The number of D-nodes.

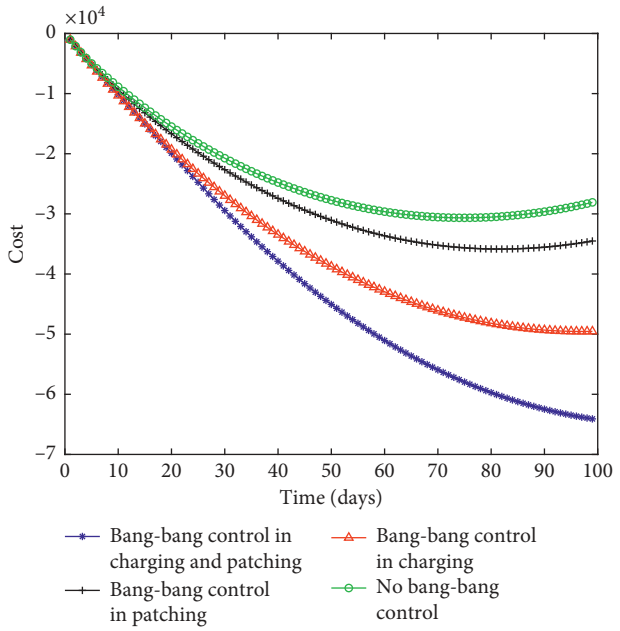

Figure 8: Cost comparison based on four control combinations. The four combinations are consistent with the four in Figure 7. The advantages of the combinations are further explained by comparing the costs incurred by them.

mortality. Starting at day 42, the combinations with bang-bang control only had a lower mortality.

4.2.2. Cost Comparison. In this part, the costs of the control combinations will be compared. The combination with the highest cost is the one with only the square control, as can be seen from Figure 8. The lowest-cost combination is the one with only the bang-bang control. At the same time, further analysis shows that bang-bang control can be applied to the charging process to reduce the cost effectively.

The reason bang-bang control produces lower costs is because of the jump property of the control. Specifically, when generating revenue, the jump from the minimum control level to the maximum level can quickly yield. Similarly, a jump from the maximum level to minimum can quickly reduce losses.

5. Conclusion

By using residual energy of nodes as one of the classification criteria, not only the flows of energy between nodes are revealed but also the attack patterns of malicious programs can be further described. The idea of charging, though just pro forma, can be used as a way to fend off malicious programs and reduce mortality of nodes. Meanwhile, the relationship between charging power and game cost has been further revealed in this paper. The advantages of bang-bang control in WSNs against malicious programs are demonstrated. When the cost of patching or charging becomes too high, the bang-bang control rule can quickly jump from maximum to minimum.

When considering the process of charging nodes, this paper assumes that charging and patching are carried out simultaneously. However, there may be a delay between the two process. Further analysis shows the way of charging may be affected by various random factors, such as light, wind speed, and human factors. The model would be more precise and practical if more practical conditions were considered. Incorporating more realistic elements into the model is a promising direction for future work.

Data Availability

The data used to support the findings of this study are included within the article, such as the cover area of the WSNs, the maximum transmission radius of nodes, the initial values of the number of sensor nodes, the transition probabilities among five nodal states, and the cost coefficients.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," *Computer Networks*, vol. 52, no. 12, pp. 2292–2330, 2008.

[2] W. O. Kermack and A. G. McKendrick, "Contribution to the mathematical theory of epidemics," *Proceedings of the Royal Society*, vol. 115, no. 772, pp. 700–721, 1927.

[3] L. P. Feng, L. P. Song, Q. S. Zhao, and H. B. Wang, "Modeling and stability analysis of worm propagation in wireless sensor network," *Mathematical Problems in Engineering*, vol. 2015, Article ID 129598, 8 pages, 2015.

[4] R. P. Ojha, P. K. Srivastava, and G. Sanyal, "Improving wireless sensor networks performance through epidemic model," *International Journal of Electronics*, vol. 106, no. 6, pp. 862–879, 2019.

[5] O. A. Toutonji, S.-M. Yoo, and M. Park, "Stability analysis of VEISV propagation modeling for network worm attack," *Applied Mathematical Modelling*, vol. 36, no. 6, pp. 2751–2761, 2012.

[6] K. M. Bimal and N. Keshri, "Mathematical model on the transmission of worms in wireless sensor network," *Applied Mathematical Modelling*, vol. 37, no. 6, pp. 4103–4111, 2013.

[7] H. X. Peng, H. Zhao, Y. G. Bi, and S. Z. Si, "A reliability-oriented local-area model for large-scale wireless sensor networks," *Mathematical Problems in Engineering*, vol. 2015, Article ID 923692, 17 pages, 2015.

[8] A. Singh, A. K. Awasthi, K. Singh, and P. K. Srivastava, "Modeling and analysis of worm propagation in wireless sensor networks," *Wireless Personal Communications*, vol. 98, no. 3, pp. 2535–2551, 2018.

[9] M. S. Haghighi, S. Wen, Y. Xiang, B. Quinn, and W. L. Zhou, "On the race of worms and patches: modeling the spread of information in wireless sensor networks," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 12, pp. 2854–2865, 2016.

[10] R. K. Shakya, "Modified si epidemic model for combating virus spread in spatially correlated wireless sensor networks," http://arxiv.org/abs/1801.04744v1.

[11] J. M. Bahi, C. Guyeux, M. Hakem, and A. Makhoul, "Epidemiological approach for data survivability in unattended

wireless sensor networks," *Journal of Network and Computer Applications*, vol. 46, pp. 374–383, 2014.

[12] B. Qu and H. Wang, "SIS epidemic spreading with correlated heterogeneous infection rates," *Physica A: Statistical Mechanics and Its Applications*, vol. 472, pp. 13–24, 2017.

[13] X. Wang, Q. Li, and Y. Li, "EiSIRS: a formal model to analyze the dynamics of worm propagation in wireless sensor networks," *Journal of Combinatorial Optimization*, vol. 20, no. 1, pp. 47–62, 2010.

[14] S. Tang, "A modified SI epidemic model for combating virus spread in wireless sensor networks," *International Journal of Wireless Information Networks*, vol. 18, no. 4, pp. 319–326, 2011.

[15] S. Shen, H. Zhou, S. Feng, J. Liu, and Q. Cao, "SNIRD: disclosing rules of malware spread in heterogeneous wireless sensor networks," *IEEE Access*, vol. 7, pp. 92881–92892, 2019.

[16] T. Wang, Q. Wu, S. Wen et al., "Propagation modeling and defending of a mobile sensor worm in wireless sensor and actuator networks," *Sensors*, vol. 17, no. 1, pp. 1–17, 2017.

[17] N. R. Zema, E. Natalizio, G. Ruggeri, M. Poss, and A. Molinaro, "MeDrone: on the use of a medical drone to heal a sensor network infected by a malicious epidemic," *Ad Hoc Networks*, vol. 50, pp. 115–127, 2016.

[18] N. keshri and B. K. Mishra, "Two time-delay dynamic model on the transmission of malicious signals in wireless sensor network," *Chaos, Solitons & Fractals*, vol. 68, pp. 151–158, 2014.

[19] L. Mo, P. C. You, X. H. Cao, Y. Q. Song, and J. M. Chen, "Decentralized multi-charger coordination for wireless rechargeable sensor networks," in *Proceedings of the IEEE IEEE 20th International Conference on High Performance Computing and Communications*, pp. 1–8, Nanjing, China, 2015.

[20] M. H. R. Khouzani, E. Altman, and S. Sarkar, "Optimal quarantining of wireless malware through reception gain control," *IEEE Transactions on Automatic Control*, vol. 57, no. 1, pp. 49–61, 2012.

[21] M. H. R. Khouzani, S. Sarkar, and E. Altman, "Maximum damage malware attack in mobile wireless networks," *IEEE/ACM Transactions on Networking*, vol. 20, no. 5, pp. 1347–1360, 2012.

[22] M. S. Abdalzaher and O. Muta, "Employing game theory and tdma protocol to enhance security and manage power consumption in wsns-based cognitive radio," http://arxiv.org/abs/1908.06844.

[23] C. Wang, H. Fang, and S. He, "Adaptive optimal controller design for a class of LDI-based neural network systems with input time-delays," *Neurocomputing*, vol. 385, pp. 292–299, 2020.

[24] S. He, H. Fang, M. Zhang, F. Liu, X. Luan, and Z. Ding, "Online policy iterative-based H∞ optimization algorithm for a class of nonlinear systems," *Information Sciences*, vol. 495, no. 25, pp. 1–13, 2019.

[25] C. Ren, R. Nie, and S. He, "Finite-time positiveness and distributed control of lipschitz nonlinear multi-agent systems," *Journal of the Franklin Institute*, vol. 356, no. 15, pp. 8080–8092, 2019.

[26] C. C. Ren and S. P. He, "Finite-time stabilization for positive Markovian jumping neural networks," *Applied Mathematics and Computation*, vol. 365, Article ID 123631, 2020.

[27] M. Li and L. Shuai, "A differential game-theoretic approach for the intrusion prevention systems and attackers in wireless networks," *Wireless Personal Communications*, vol. 103, no. 3, pp. 1993–2003, 2018.

[28] X. N. Miao, X. W. Zhou, and H. Y. Wu, "A cooperative differential game model based on network throughput and energy efficiency in wireless networks," *Optimization Letters*, vol. 6, no. 1, pp. 65–68, 2012.

[29] H. Dong and K. SAKURAI, "A differential game approach to mitigating primary user emulation attacks in cognitive radio network," in *Proceedings of the 26th International Conference on Advanced Computing, Networking, and Informatics*, pp. 495–502, Fukuoka, Japan, 2012.

[30] Y. Ding, X.-w. Zhou, Z.-m. Cheng, and F.-h. Lin, "A security differential game model for sensor networks in context of the internet of things," *Wireless Personal Communications*, vol. 72, no. 1, pp. 375–388, 2013.

[31] S. He, M. Zhang, H. Fang, F. Liu, X. Luan, and Z. Ding, "Reinforcement learning and adaptive optimization of a class of markov jump systems with completely unknown dynamic information," *Neural Computing and Applications*, 2019.

[32] S. He, H. Fang, M. Zhang, F. Liu, and Z. Ding, "Adaptive optimal control for a class of nonlinear systems: the online policy iteration approach," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 31, no. 2, pp. 549–558, 2020.

[33] T. Mylvaganam, M. Sassano, and A. Astolfi, "A differential game approach to multi-agent collision avoidance," *IEEE Transactions on Automatic Control*, vol. 62, no. 8, pp. 4229–4235, 2017.

[34] J. Hu and Y. Xie, "A stochastic differential game theoretic study of multipath routing in heterogeneous wireless networks," *Wireless Personal Communications*, vol. 80, no. 3, pp. 971–991, 2015.

[35] B. Gao, X. Liu, C. Wu, and Y. Tang, "Game-theoretic energy management with storage capacity optimization in the smart grids," *Journal of Modern Power Systems and Clean Energy*, vol. 6, no. 4, pp. 656–667, 2018.

[36] J. Hu, Q. Qian, A. Fang, S. Wu, and Y. Xie, "Optimal data transmission strategy for healthcare-based wireless sensor networks: a stochastic differential game approach," *Wireless Personal Communications*, vol. 89, no. 4, pp. 1295–1313, 2016.

[37] L. Mo, A. Kritikakou, and S. He, "Energy-aware multiple mobile chargers coordination for wireless rechargeable sensor networks," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8202–8214, 2019.

[38] R. Isaacs, *Differential Game*, Wiley, New York, NY, USA, 1965.

[39] F. Avner, *"Differential Games," in Handbook of Game Theory*, Elsevier, Amsterdam, Netherlands, 1994.

[40] A. Bressan, "Noncooperative differential games," *Milan Journal of Mathematics*, vol. 79, no. 2, pp. 357–427, 2011.