Hindawi
Complexity
Volume 2020, Article ID 3680518, 19 pages
https://doi.org/10.1155/2020/3680518

Research Article

Attack-Defense Game between Malicious Programs and Energy-Harvesting Wireless Sensor Networks Based on Epidemic Modeling

Guiyun Liu, Baihao Peng, Xiaojing Zhong, Lefeng Cheng, and Zhifu Li

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

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

Received 15 July 2020; Revised 19 August 2020; Accepted 27 August 2020; Published 14 September 2020

Academic Editor: Ning Cai

As energy-harvesting wireless sensor networks (EHWSNs) are increasingly integrated with all walks of life, their security problems have gradually become hot issues. As an attack means, malicious programs often attack sensor nodes in critical locations in the networks to cause paralysis and information leakage of the networks, resulting in security risks. Based on the previous works and the introduction of solar charging, we proposed a novel model, namely, Susceptible-Infected-Low (energy)-Recovered-Dead (SILRD) with solar energy harvesters. Meanwhile, this paper takes Logistic Growth as the drop rate of sensor nodes and the infection rate of multitype malicious programs under nonlinear condition into consideration. Finally, an Λ-Susceptible-Infected-Low (energy)-Recovered-Dead (ΛSILRD) model is proposed. Based on the Pontryagin Maximum Principle, this paper proposes the optimal strategies based on the SILRD with solar energy harvesters and the ΛSILRD. The effectiveness of SILRD with solar energy harvesters was demonstrated by comparison with the general epidemic model. At the same time, by analyzing different charging strategies, we conclude that solar charging is highly efficient. Moreover, we further analyze the influence of controllable and uncontrollable input and various node degrees on ΛSILRD model.

1. Introduction

With the rapid development of wireless sensor networks (WSNs) in the past few years, the unique characteristics of WSNs have enabled them to play a key role in many fields, such as military strike, agricultural production, intelligent transportation, medical and health systems, and industrial fields. Typical WSNs consist of a series of sensor nodes with different functions of gathering environment information and transmitting processed information, which is either fixed or randomly distributed. Generally, the coverage area of the networks is much larger than the maximum transmission distance of each sensor node. Therefore, transmission between sensor nodes and terminal computers or control centers is normally conducted in multihop. However, the limited energy vastly confines the lifetime of the networks. Renewable natural resources, such as wind, solar, and tidal energy, can be transferred to electricity by certain energy harvesters, which can greatly mitigate the impact of energy shortage on the lifetime of energy-harvesting wireless sensor networks (EHWSNs) which is equipped with energy harvesters on each sensor node.

However, the structure of WSNs provides a hotbed for the propagation of malicious programs. Furthermore, low defense capabilities render sensor nodes more vulnerable to malicious programs. With the booming of WSNs in all walks of life, paralysis and information leakage owing to malicious programs will cause unpredictable economic losses. Along with the ceaseless invasion of malicious programs, many scholars have studied the behavior characteristics of malicious programs and develop corresponding countermeasures. Due to the similarity of propagation mechanisms between malicious programs and infectious disease, epidemic models which are suitable for WSNs have been further developed after decades of study based on the initial Susceptible-Infected-Recovered (SIR) model proposed by

Kermack and McKendrick in 1927 [1]. Unlike computer viruses, the spread of malicious programs in WSNs is affected by node distribution density and communication radius [2]. Also, geospatial limitation [3], spatial correlation [4], coupling degree [5], and transmission delay [6] have effects on it. In addition to a series of removal methods, predicting the risk of infection of sensor nodes is also one of the current research hotspots [7]. Furthermore, a two-level bidirectional data prediction model proposed by Wang et al. can effectively reduce the data collection cost of the underwater acoustic sensor network and improve the utilization rate of bandwidth [8]. Li et al. applied machine learning methods to improve the efficiency of malware detection [9]. Han et al. proposed a DMPPR scheme to protect users' privacy of WSNs [10]. Zhao et al. proposed a method to detect an undetectable false data-injection attack in cyber-physical systems [11]. In the prevention of malicious programs, Li et al. [12] and Liu et al. [13], respectively, proposed a LightLRFMS algorithm and TPE-FTED algorithm to screen false data caused by malicious attacks and system failures. Dynamic defenses are also valid methods [14, 15] compared with static approaches. Wu et al. proposed a novel model and defense mechanism to effectively protect big data in the networks owing to its vulnerability to virus attacks [16].

Although few scholars discuss the issue of energy in the sensor network attacked by malicious programs, effectively, the increase in the energy of WSNs is always a hot topic. For example, Mo et al. used multiple mobile chargers to supplement the energy of WSNs [17, 18]. It is worth mentioning that the control of multiagent is one of the research hotspots in recent years [19, 20]. In this paper, sensor nodes have been divided into five states based on the remaining energy, and the energy-harvesting technology is introduced to supplement the energy of sensor nodes to extend the lifespan of the EHWSNs. On the basis of [21], this paper changes the charging method to solar charging and constructs a new model, namely, Susceptible-Infected-Low (energy)-Recovered-Dead (SILRD) with solar energy harvesters. At the same time, considering networks input and multitypes of malicious programs attacks with nonlinear infection rates, a novel model named Λ-Susceptible-Infected-Low (energy)-Recovered-Dead (ΛSILRD) is proposed.

Similar to conflict of interest in a game, game theory can be applied to get optimal solutions, like optimal Dissemination of Security Patches [22], optimal power control [23], optimal detection rate [24], optimal data transmission strategy [25], optimal hardware deployment cost in EHWSNs [26], optimal delay and transmission times in the networks [27], suitable game strategy and price adjustment principle in cyber-physical-social systems (CPSS) [28], maximization of energy efficiency [29], and optimal multipath routing [30]. As an essential part of game theory, the differential game can describe the dynamic process with differential equations. Mylvaganam et al. find the optimal control in multiagent collision avoidance [31]. Miao and Li [32] derive the optimal strategies for the attackers and the intrusion prevention systems. Miao et al. [33] find an optimal solution based on tradeoff between network throughput and energy efficiency. In this paper, the differential game will be applied to solve the confrontation problem between malicious programs and EHWSNs, and the optimal attack-defense strategies for both parties have been proposed.

Our contributions are summarized in the following paragraphs.

The low-energy state is introduced into the basic epidemic model considering the limited energy of sensor nodes. To suppress the spread of malicious programs, the method of charging by solar energy harvesters is put forward which is helpful to alleviate the security problems and maintenance of the networks. Thus, a model named SILRD with solar energy harvesters which better fits EHWSNs has been proposed. The effectiveness of SILRD with solar energy harvesters is obtained by comparison with existing epidemic models. The efficiency of solar charging is demonstrated by comparing with different charging strategies.

Three nonlinear factors will be considered in this paper, including Logistic Growth, nonlinear infection rate, and charging power provided by solar energy harvesters. At the same time, this paper takes the impact of multitypes of malicious programs into consideration. Finally, a novel attack-defense game model named ΛSILRD is proposed in this paper. Meanwhile, the influence of controllable input, uncontrollable input, and various node degree on ΛSILRD model and EHWSNs has been discussed.

Based on the ΛSILRD model, the optimal dynamic control strategies for EHWSNs and malicious programs under various node degrees are proposed by applying Pontryagin Maximum Principle.

The rest of the paper is organized as follows. In Section 2, the nonlinear factors involved in ΛSILRD model will be proposed first, and then ΛSILRD model will be introduced in detail. In Section 3, the Pontryagin Maximum Principle will be used to find the optimal dynamic control strategies and the optimality will be proved briefly after the introduction of the expressions of control variables and game cost. In Section 4, the effectiveness of SILRD with solar energy harvesters and solar charging, the influence of controllable and uncontrollable input, and node degree on ΛSILRD will be demonstrated through simulations. Section 5 is the conclusion and prospect of this paper.

2. ΛSILRD Model in EHWSNs

This section explains the nonlinear factors at first, including Logistic Growth, nonlinear infection rate, and solar charging power. Then, on the premise of considering multiple types of malicious programs' attacks, the ΛSILRD model is proposed.

2.1. Nonlinear Factors in ΛSILRD Model. In this paper, EHWSNs consist of identical sensor nodes equipped with solar energy harvesters, which are distributed statically. The solar energy harvesters energize sensor nodes according to the duration of sunlight. In the case of the diurnal period, the charging power generally goes through a process of increasing firstly and then decreasing. Specifically, the

charging power increases slowly at first since the sunlight intensity is weak at dawn. With the arrival of noon, sunlight intensity increasingly reaches the maximum value of the day, while charging power at this time is also at a maximum. However, the charging power will show a downward trend when night falls. In this paper, 24 hours is assumed as a period and the case of fine days is only considered. In particular, (1) is used to describe the trend of solar charging power over a day [34]:

$$P(t) = \frac{A}{\sqrt{2\pi n}} e^{-\left((t-m)^2/2n^2\right)}, \tag{1}$$

where A is the intensity of solar charging power and m and n are the mean value and variance value of the power distribution, respectively.

To maintain the functioning of EHWSNs, it is indispensable to deploy new nodes when conditions permit. This paper considers Logistic Growth as input rate of new nodes. Logistic Growth is formulated by

$$\Lambda(t) = rS(t)\left[1 - \frac{S(t)}{k}\right], \tag{2}$$

where r represents the node degree, k represents the capacity of EHWSNs, and $S(t)$ represents the quantity of susceptible nodes at time t.

Compared with the linear infection rate, the nonlinear infection rate can better describe the ability of malicious programs to propagate in a limited area. Models with linear infection rates, where the quantity of infected nodes grows linearly, are impractical. Actually, the quantity of infections is bound to increase exponentially at first. As time progresses, the quantity grows steadily until it eventually infects the entire networks. According to the above description of infection process, (3) is applied to express it:

$$Y(t) = \left[1 - \left(1 - P_{SI}\right)^{nI(t)}\right], \tag{3}$$

where P_{SI} is the probability of infection, $I(t)$ is the quantity of infected nodes at time t, and n represents the connectivity of nodes.

2.2. Model with Solar Energy Harvester. There exist two-time intervals without sunlight in one day. Specifically, one is from 0 am to 5 am and the other is from 8 pm to 12 pm [34]. In these two intervals, solar energy harvesters knock off and sensor nodes may be dysfunctional since electricity drains out. According to the energy levels and the infection status, sensor nodes have been divided into five states.

Susceptible (S) State. Sensor nodes in the susceptible state are with high-energy level and can complete assignment normally. Without defense measures, susceptible sensor nodes are vulnerable to malicious programs.

Infected (I) State. Sensor nodes in the infected state are transformed from susceptible, recovered, or low-energy sensor nodes by running malicious programs. In the early stage of infection or after charging, infected sensor nodes are still at a high-energy level because the extent of damage has not yet been reached.

Low-Energy (L) State. Sensor nodes in the low-energy state are with energy which are too insufficient to function properly, including information transmission. Therefore, malicious programs attached to low-energy sensor nodes do not have the ability to continue infecting. Similarly, low-energy sensor nodes will not be patched.

Recovered (R) State. Sensor nodes in the recovered state have installed the patches successfully. Also, recovered sensor nodes are all in high-energy level. The patches are only applicable to relevant malicious programs. In the face of attacks by inhomogeneous malicious programs, these sensor nodes will also be helpless and transform to infected state.

Dead (D) State. Sensor nodes in the dead state are absolute dysfunction compared with low-energy sensor nodes. Dead sensor nodes no longer own the ability to collect, process, and transmit information.

At time t, the proportion of the number of sensor nodes in susceptible, infected, recovered, low-energy, and dead states is $S(t)$, $I(t)$, $L(t)$, $R(t)$, and $D(t)$, respectively. And the following equation must be met:

$$S(t) + I(t) + L(t) + R(t) + D(t) = 1. \tag{4}$$

In the absence of sunlight, the networks rely on the residual energy to maintain functioning. New sensor nodes are cast randomly to keep the connectivity of EHWSNs. Susceptible nodes still consume electricity at night to continue data acquisition, processing, and transmission. Under the attack of malicious programs, susceptible sensor nodes are transformed into infected sensor nodes with probability P_{SI}. Some susceptible sensor nodes are fortunately enough to be patched to possess immunity with probability P_{SR}. The rest stick at their daily tasks normally with probability P_{SL}.

Infected sensor nodes transmit data to neighbors at higher frequencies to spread malicious programs rapidly and disrupt the transmission mechanism. Therefore, infected sensor nodes will consume the remaining electricity at a faster rate and transform to low-energy or dead state with probability P_{IL} and P_{ID} according to the attack power of malicious programs. While malicious programs are spreading arbitrarily, patches carried by unmanned aerial vehicles (UAVs) transmitted to the infected sensor nodes located at the corresponding district with probability P_{IR}.

The existence of multiple types of malicious programs is considered and the common feature of these malicious programs is that their attack mechanisms are embodied in the accelerated consumption of sensor nodes' energy. For this reason, even recovered sensor nodes will be infected again with probability P_{RI}. Similarly, few recovered sensor nodes work normally until low-energy level with probability P_{RL}.

Sensor nodes at high-energy levels include sensor nodes in susceptible, infected, and recovered state. Energy consumption owing to damage or normal operation will eventually convert sensor nodes in high-energy state to low-energy state. Sensor nodes at low-energy levels suspend some functions, including data transmission, for their own subsistence. Therefore, low-energy sensor nodes will not receive and transmit malicious programs. Even if the consumption is lower, the energy will eventually run out with probability P_{LD}. With the use of solar energy harvesters, the probabilities of sensor nodes in low-energy state converting into susceptible, infected, and recovered states are $P_{LS}P(t)$, $P_{LI}P(t)$, and $P_{LR}P(t)$, respectively. Among them, P_{LS} is related to the number of sensor nodes that transformed from susceptible state to low-energy state at the previous moment, P_{LI} is related to the number of sensor nodes that transformed from infected state to low-energy state at the previous moment, and P_{LR} is related to the number of nodes that switched from an infected state to a low-energy state at the previous moment. In particular, Figure 1 is used to visualize the evolution of sensor nodes. Figure 1 shows a part of sensor nodes in EHWSNs. Among them, the letter in the circle represents the node state. Specifically, Figure 1(a) shows the initial node state when the patch-carrying UAV has not yet passed the sensor nodes and the solar energy harvesters have started working. Figure 1(b) shows the evolution of sensor nodes after the UAV drives over a part of sensor nodes and the solar energy harvesters charge sensor nodes.

Considering the Logistic Growth (2) and the nonlinear incidence rate (3), the above dynamic processes are formulated in (5)–(9), and the flow diagram of propagation is shown in Figure 2:

$$\frac{\mathrm{d}S(t)}{\mathrm{d}t} = \Lambda(t) - Y(t)S(t) - P_{SR}S(t) - P_{SL}S(t) + P_{LS}P(t)L(t), \tag{5}$$

$$\frac{\mathrm{d}I(t)}{\mathrm{d}t} = Y(t)S(t) - P_{IR}I(t) - P_{IL}I(t) + P_{RI}R(t) - P_{ID}I(t) + P_{LI}P(t)L(t), \tag{6}$$

$$\frac{\mathrm{d}L(t)}{\mathrm{d}t} = P_{IL}I(t) + P_{SL}S(t) - P_{LD}L(t) + P_{RL}R(t) - P_{LS}P(t)L(t) - P_{LI}P(t)L(t) - P_{LR}P(t)L(t), \tag{7}$$

$$\frac{\mathrm{d}R(t)}{\mathrm{d}t} = P_{IR}I(t) + P_{SR}S(t) - P_{RI}R(t) - P_{RL}R(t) + P_{R}(t)L(t), \tag{8}$$

$$\frac{\mathrm{d}D(t)}{\mathrm{d}t} = P_{LD}L(t) + P_{ID}I(t). \tag{9}$$

3. Optimal Controls in Attack-Defense Game

In this section, control variables between malicious programs and EHWSNs are introduced at first. Then, the process of attack-defense game has been analyzed and the overall cost has been formulated. Finally, the Hamiltonian function has been built and constructed and the optimal strategies of both sides are obtained on the basis of proving the existence and the uniqueness.

3.1. Control Variables in the ΛSILRD Model. The attacks of malicious programs are mainly reflected in the propagation performance and the damage capacity. The more contagious malicious programs are, the more sensor nodes they can infect. Infected sensor nodes can spread malicious programs by increasing communication frequency. The damage capacity is incarnated in the consumption of energy and the destruction of hardware. Some malicious programs can overload sensor nodes so that they can become dysfunctional quickly, and other malicious programs cannot directly destroy sensor nodes because damage capacities are not powerful enough [35].

The defense measures applied by EHWSNs are the deployment of patch-carrying UAVs and the installing and running of solar energy harvesters. Because of the periodicity of sunlight, patching is the only countermeasure at night. By identifying and analyzing multitype malicious programs, UAVs will download corresponding patches from the base station. Energy supplements do not cure infected sensor nodes but only alleviate their severe consumption.

It is not hard to find that the propagation performance of malicious programs is the process of transformation from susceptible or recovered state to infected state. The attacks on the above transformations are defined as $A_{SI}(t)$ and $A_{RI}(t)$. At the same time, the damage capacities are reflected in the process of transformation from infected state to low-energy or dead state. Thus, the attacks are defined as $A_{IL}(t)$ and $A_{ID}(t)$. The defenses of EHWSNs are embodied in all sensor nodes that are transformed into recovered state. Therefore, the defense measures are defined as $D_{SR}(t)$ and $D_{IR}(t)$.

According to the above statement, the corresponding probability can be replaced by the equations containing the control variables. Specifically, P_{IL} can be replaced by $(A_{IL}(t)S_{IL}/(A_{IL\max} + A_{IL\min}))$, P_{ID} can be replaced by

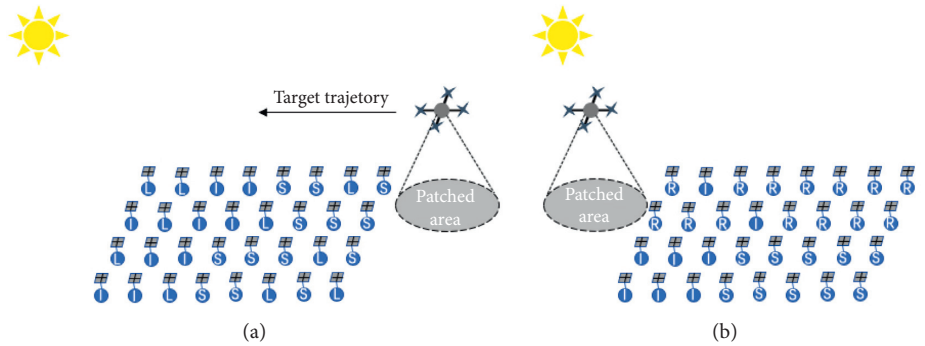

Figure 1: Schematic of ΛSILRD model. (a) The initial state of sensor nodes; (b) the current state of sensor nodes after solar charging and UAVs' patching.

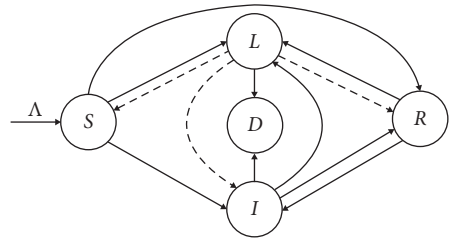

Figure 2: The flow diagram of ΛSILRD model.

$(A_{ID}(t)S_{ID}/(A_{ID\max}+A_{ID\min}))$, P_{RI} can be replaced by $(A_{RI}(t)S_{RI}/(A_{RI\max}+A_{RI\min}))$, P_{SR} can be replaced by $(D_{SR}(t)S_{SR}/(D_{SR\max}+D_{SR\min}))$, and P_{IR} can be replaced by $(D_{IR}(t)S_{IR}/(D_{IR\max}+D_{IR\min}))$. In particular, for the convenience of calculation, $(A_{SI}(t)S_{SI}/(A_{SI\max}+A_{SI\min}))$ will be directly multiplied by the term corresponding to the nonlinear incidence rate. The subscripts max and min, respectively, represent the maximum and the minimum values of the attacks or defenses, and the letter S represents the probability of the successful attacks or defenses and its subscript represents relevant state transition relationship.

3.2. Cost Function in ΛSILRD Model. The continuous confrontation between malicious programs and EHWSNs constitutes the attack-defense game. The purposes of malicious programs as attacker are to infect and destroy as many nodes as possible, while EHWSNs as defender aim to keep as many nodes immune and alive as possible. Both sides achieve their goals through the control means mentioned in the previous part. The cost function is applied to indicate the consequence of attack-defense game.

Deployment costs include production costs and human costs. Cost factor C_N times the drop rate formulated in (2) is used to represent the deployment costs at time t, where C_N is greater than 0. By completing daily assignments, sensor nodes in susceptible state which send involved information to clients to meet their requirements will generate positive benefits.

Although the unstoppable spread of malicious programs causes more sensor nodes to be infected, infected sensor nodes do not initially incur additional costs until malicious programs begin to run. $C_I I(t)$ is used to describe the costs incurred after malicious programs run at time t, where C_I is greater than 0.

As a defense means for EHWSNs, the transmission of patches to susceptible and infected sensor nodes will incur costs. $C_{SR}P_{SR}S(t)$ is used to describe the cost of transmitting patches to susceptible sensor nodes at time t, and $C_{IR}P_{IR}I(t)$ is used to describe the cost of transmitting patches to infected sensor nodes at time t, where C_{SR} and C_{IR} are greater than 0.

Recovered sensor nodes are similar to susceptible nodes. Because they have immunity to certain types of malicious programs, the revenue generated by recovered nodes at time t will be higher than that of the susceptible sensor nodes.

Low-energy sensor nodes cannot operate normally compared with the high-energy sensor nodes, so that they can incur the cost $C_L L(t)$ at time t, where C_L is greater than 0. The generation of dead sensor nodes will lead to the interruption of the connection of sensor nodes, or even the paralysis of the networks, and $C_D D(t)$ is used to describe the cost at time t, where C_D is greater than 0. It is worth noting that since solar energy harvesters capture natural resources, the cost of energy harvesting and transformation is not considered.

At the end of the game, each type of sensor nodes will incur a series of termination payoff. Among them, susceptible sensor nodes and recovered sensor nodes will still generate revenue in the future, so their terminal costs should be less than 0; that is, C_{S_f} and C_{R_f} are both less than 0. Conversely, sensor nodes at infected, low-energy, and dead states will still cause loss in the future; that is, C_{I_f}, C_{L_f}, and C_{D_f} are greater than 0.

Based on the above statement, the cost function (10) is constructed as follows:

$$J(t) = \int_{t_0}^{t_f} \left\{ C_I I(t) + rC_N S(t)\left[1 - \frac{S(t)}{k}\right] + C_L L(t) + C_D D(t) + C_{SR} P_{SR} S(t) + C_{IR} P_{IR} I(t) \right\} \mathrm{d}t + C_{S_f} S\left(t_f\right) + C_{I_f} I\left(t_f\right) + C_{L_f} L\left(t_f\right) + C_{R_f} R\left(t_f\right) + C_{D_f} D\left(t_f\right). \tag{10}$$

3.3. Optimal Strategies in the ΛSILRD Model. Suppose the duration of the game is T. Within T, according to (5)–(9), it is not difficult to find that the state variables are continuous and uninterrupted. Meanwhile, the state variables are continuous in the cost function (10).

For the control variables, they are not only continuous in state functions (5)–(9) and cost function (10), but also linear. Specifically, according to the assumptions in Section 3.1, each control variable has a maximum value and a minimum value; that is, each control variable is bounded. Furthermore, we define $\nu(t)$ as a set of control strategies of attacker (malicious programs), that is, $\nu(t) = \{A_{SI}(t), A_{IL}(t), A_{ID}(t), A_{RI}(t)\}$, and $\mu(t)$ as a set of control strategies of defender (EHWSNs), that is, $\mu = \{D_{SR}(t), D_{IR}(t)\}$.

Thus, according to the conditions put forward by [36], there must exist a saddle point in (10), which satisfies

$$J\left(\mu^*(t), \nu(t)\right) \le J\left(\mu^*(t), \nu^*(t)\right) \le J\left(\mu(t), \nu^*(t)\right), \tag{11}$$

where $J(\mu^*(t), \nu(t))$ represents the cost incurred when only the optimal strategy is selected by EHWSNs, $J(\mu(t), \nu^*(t))$ denotes that only malicious programs choose the optimal strategy and $J(\mu^*(t), \nu^*(t))$ indicates that both EHWSNs and malicious programs choose the optimal strategies.

Specifically, the inequality on the left indicates that when strategy chosen by EHWSNs is unchanged, the cost will be maximized when the malicious programs choose the optimal strategy; the inequality on the right indicates the cost will be minimized when EHWSNs select the optimal strategy, while the strategy chosen by malicious programs remains unchanged. When both parties choose the optimal strategies, an equilibrium point, the saddle point, will be formed between the maximum cost generated by the malicious programs and the minimum cost generated by EHWSNs.

According to [37] and the characteristics of this model, we can further know that there must be V satisfying the following equation:

$$\begin{aligned} V &= \max_{\nu(t)} \min_{\mu(t)} J(\mu(t), \nu(t)) \\ &= \min_{\mu(t)} \max_{\nu(t)} J(\mu(t), \nu(t)) \\ &= J\left(\mu^*(t), \nu^*(t)\right), \end{aligned} \tag{12}$$

where $\max_{\nu(t)} \min_{\mu(t)} J(\mu(t), \nu(t))$ represents the cost incurred by EHWSNs in selecting the optimal strategy after the malicious programs make an 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.

Theorem 1. *In the attack-defense game based on the ΛSILRD model, the optimal dynamic strategies of EHWSNs and malicious programs are*

$$A_{SI}^*(t) = \begin{cases} A_{SI\max}; & \beta_{A_{SI}} > 0, \\ \text{unknown}; & \beta_{A_{SI}} = 0, \\ A_{SI\min}; & \beta_{A_{SI}} < 0, \end{cases} \tag{13}$$

$$A_{IL}^*(t) = \begin{cases} A_{IL\max}; & \beta_{A_{IL}} > 0, \\ \text{unknown}; & \beta_{A_{IL}} = 0, \\ A_{IL\min}; & \beta_{A_{IL}} < 0, \end{cases} \tag{14}$$

$$A_{ID}^*(t) = \begin{cases} A_{ID\max}; & \beta_{A_{ID}} > 0, \\ \text{unknown}; & \beta_{A_{ID}} = 0, \\ A_{ID\min}; & \beta_{A_{ID}} < 0, \end{cases} \tag{15}$$

$$A_{RI}^*(t) = \begin{cases} A_{RI\max}; & \beta_{A_{RI}} > 0, \\ \text{unknown}; & \beta_{A_{RI}} = 0, \\ A_{RI\min}; & \beta_{A_{RI}} < 0, \end{cases} \tag{16}$$

$$D_{SR}^*(t) = \begin{cases} D_{SR\max}; & \beta_{D_{SR}} > 0, \\ \text{unknown}; & \beta_{D_{SR}} = 0, \\ D_{SR\min}; & \beta_{D_{SR}} < 0, \end{cases} \tag{17}$$

$$D_{IR}^*(t) = \begin{cases} D_{IR\max}; & \beta_{D_{IR}} > 0, \\ \text{unknown}; & \beta_{D_{IR}} = 0, \\ D_{IR\min}; & \beta_{D_{IR}} < 0, \end{cases} \tag{18}$$

where discriminant parameters are shown in Table 1.

Proof. Define $x(t) = \{S(t), I(t), L(t), R(t), D(t)\}$ in the ΛSILRD model. For all t which belongs to T, if $H(x(t), \mu^*(t), \nu(t), t) \le H(x(t), \mu^*(t), \nu^*(t), t) \le H(x(t), \mu(t), \nu^*(t), t)$ is satisfied, there must be an optimal set of strategies $(\mu^*(t), \nu^*(t))$ according to [38].

First, the generalization of the cost function in the game will be described as follows:

$$J(\mu(t), \nu(t)) = \varphi\left(x(t_1), t_1\right) + \int_{t_0}^{t_f} L(x(t), \mu(t), \nu(t), t)\mathrm{d}t + \upsilon\psi\left(x(t_1), t_1\right). \tag{19}$$

Define a new function ϕ as follows:

Table 1: Table of parameters in optimal strategies.

Letter	Counterpart
$\beta_{A_{SI}}$	$(\lambda_{I(t)} - \lambda_{S(t)})[1 - (1 - P_{SI})^{nI^*(t)}]S^*(t)$
$\beta_{A_{IL}}$	$(\lambda_{L(t)} - \lambda_{I(t)})P_{IL}I^*(t)$
$\beta_{A_{ID}}$	$(\lambda_{D(t)} - \lambda_{I(t)})P_{ID}I^*(t)$
$\beta_{A_{RI}}$	$(\lambda_{I(t)} - \lambda_{R(t)})P_{RI}R^*(t)$
$\beta_{D_{SR}}$	$(\lambda_{R(t)} - \lambda_{S(t)})P_{SR}S^*(t) + C_{SR}P_{SR}S^*(t)$
$\beta_{D_{IR}}$	$(\lambda_{R(t)} - \lambda_{I(t)})P_{IR}I^*(t) + C_{IR}P_{IR}I^*(t)$

$$\phi = \varphi(x(t_1), t_1) + v\psi(x(t_1), t_1). \tag{20}$$

Then, the above general cost function will be simplified as follows:

$$J(\mu(t), \nu(t)) = \phi(x(t_1), t_1) + \int_{t_0}^{t_f} L(x(t), \mu(t), \nu(t), t)\mathrm{d}t, \tag{21}$$

where $L(x(t), \mu(t), \nu(t), t)$ corresponds to the integral term in (10) and $\phi(x(t_1), t_1)$ corresponds to the nonintegral term in (10).

According to the definition of Hamiltonian function in differential game, we have the following formula:

$$\begin{aligned} H(\lambda(t), x(t), \mu(t), \nu(t), t) &\triangleq \sum_{i=0}^{5} \lambda_i(t) f_i(x(t), \mu(t), \nu(t), t) \\ &= \sum_{i=1}^{5} \lambda_i(t) f_i(x(t), \mu(t), \nu(t), t) + L(x(t), \mu(t), \nu(t)), \end{aligned} \tag{22}$$

where $\lambda(t)$ is the set of costate variables; that is, $\lambda(t) = \{\lambda_S(t), \lambda_I(t), \lambda_L(t), \lambda_R(t), \lambda_D(t)\}$, and $f_i(x(t), \mu(t), \nu(t), t)$ is the differential equation of node state corresponding to (5)–(9).

Among them, when the costate functions satisfy the following equations, there exists an optimal strategy (μ^*, ν^*):

$$\begin{aligned} \frac{\partial \lambda_i}{\partial t} &= -\frac{\partial H}{\partial x_i}, \\ \lambda_i(t_1) &= -\frac{\partial \phi}{\partial x_i(t_1)}, \end{aligned} \tag{23}$$

where t_1 represents the terminal moment when the game ends.

Therefore, the Hamiltonian function, the differential equations, and the end-value constraints of costate variables in this paper can be formulated from (24) to (30):

$$\begin{aligned} H(\lambda(t), x(t), \mu(t), \nu(t), t) &= \lambda_S(t)\frac{\mathrm{d}S(t)}{\mathrm{d}t} + \lambda_I(t)\frac{\mathrm{d}I(t)}{\mathrm{d}t} + \lambda_R(t)\frac{\mathrm{d}R(t)}{\mathrm{d}t} + \lambda_L(t)\frac{\mathrm{d}L(t)}{\mathrm{d}t} + \lambda_D(t)\frac{\mathrm{d}D(t)}{\mathrm{d}t} \\ &\quad + rC_N S(t)\left[1 - \frac{S(t)}{k}\right] + C_I I(t) + C_{SR}S(t)\frac{D_{SR}S_{SR}}{D_{SR\max} + D_{SR\min}} + C_L L(t) \\ &\quad + C_{IR}I(t)\frac{D_{IR}S_{IR}}{D_{IR\max} + D_{IR\min}} + C_D D(t), \end{aligned} \tag{24}$$

$$\begin{aligned} \frac{\mathrm{d}\lambda_S(t)}{\mathrm{d}t} &= \frac{2\lambda_S(t)S(t)}{k} + (\lambda_S(t) - \lambda_I(t))A_{SI}(t)(1 - (1 - P_{SI}))^{nI(t)} - \lambda_S(t)r \\ &\quad + (\lambda_S(t) - \lambda_R(t))\frac{D_{SR}(t)S_{SR}}{D_{SR\max} + D_{SR\min}} + (\lambda_S(t) - \lambda_L(t))P_{SL} - rC_{N(t)} \\ &\quad + \frac{2rC_N S(t)}{k} - C_{SR}\frac{D_{SR}(t)S_{SR}}{D_{SR\max} + D_{SR\min}}, \end{aligned} \tag{25}$$

$$\begin{aligned} \frac{\mathrm{d}\lambda_I(t)}{\mathrm{d}t} &= nA_{SI}(\lambda_I(t) - \lambda_S(t))S(t)(1 - P_{SI})^{nI(t)}\ln(1 - P_{SI}) - C_I - C_{IR}\frac{D_{IR}(t)S_{IR}}{D_{IR\max} + D_{IR\min}} \\ &\quad + (\lambda_I(t) - \lambda_R(t))\frac{D_{IR}(t)S_{IR}}{D_{IR\max} + D_{IR\min}} + (\lambda_I(t) - \lambda_D(t))\frac{A_{ID}(t)S_{ID}}{A_{ID\max} + A_{ID\min}} \\ &\quad + (\lambda_I(t) - \lambda_L(t))\frac{A_{IL}(t)S_{IL}}{A_{IL\max} + A_{IL\min}}, \end{aligned} \tag{26}$$

$$\begin{aligned} \frac{\mathrm{d}\lambda_L(t)}{\mathrm{d}t} &= (\lambda_L(t) - \lambda_D(t))P_{LD} + (\lambda_L(t) - \lambda_R(t))P_{LR}P(t) \\ &\quad + (\lambda_L(t) - \lambda_S(t))P_{LS}P(t) + (\lambda_L(t) - \lambda_I(t))P_{LI}P(t) - C_L, \end{aligned} \tag{27}$$

$$\frac{d\lambda_R(t)}{dt} = (\lambda_R(t) - \lambda_I(t))\frac{A_{RI}(t)S_{RI}}{A_{RI\max} + A_{RI\min}} + (\lambda_R(t) - \lambda_L(t))P_{RL}, \tag{28}$$

$$\frac{d\lambda_D(t)}{dt} = -C_D, \tag{29}$$

$$\begin{cases} \lambda_S(t_f) = \dfrac{d\phi}{dS(t)} = C_{S_f}, \\ \lambda_I(t_f) = \dfrac{d\phi}{dI(t)} = C_{I_f}, \\ \lambda_L(t_f) = \dfrac{d\phi}{dL(t)} = C_{L_f}, \\ \lambda_R(t_f) = \dfrac{d\phi}{dR(t)} = C_{R_f}, \\ \lambda_D(t_f) = \dfrac{d\phi}{dD(t)} = C_{D_f}. \end{cases} \tag{30}$$

When $H(x(t), \mu^*(t), \nu(t), t) \le H(x(t), \mu^*(t), \nu^*(t), t)$ is satisfied, if $(\lambda_I(t) - \lambda_S(t))[1 - (1 - P_{SI})^{nI^*(t)}]S^*(t)$ is greater than 0, $A_{SI}(t)$ takes the maximum value, and if $(\lambda_I(t) - \lambda_S(t))[1 - (1 - P_{SI})^{nI^*(t)}]S^*(t)$ is less than 0, $A_{SI}(t)$ takes the minimum value; if $(S_{IL}(\lambda_L(t) - \lambda_I(t))I^*(t)/(A_{IL\max} + A_{IL\min}))$ is greater than 0, $A_{IL}(t)$ takes the maximum value, and if $(S_{IL}(\lambda_L(t) - \lambda_I(t))I^*(t)/(A_{IL\max} + A_{IL\min}))$ is less than 0, $A_{IL}(t)$ takes the minimum value; if $(S_{ID}(\lambda_D(t) - \lambda_I(t))I^*(t)/(A_{ID\max} + A_{ID\min}))$ is greater than 0, $A_{ID}(t)$ takes the maximum value, and if $(S_{ID}(\lambda_D(t) - \lambda_I(t))I^*(t)/(A_{ID\max} + A_{ID\min}))$ is less than 0, $A_{ID}(t)$ takes the minimum value; if $(S_{RI}(\lambda_I(t) - \lambda_R(t))R^*(t)/(A_{RI\max} + A_{RI\min}))$ is greater than 0, $A_{RI}(t)$ takes the maximum value, and if $(S_{RI}(\lambda_I(t) - \lambda_R(t))R^*(t)/(A_{RI\max} + A_{RI\min}))$ is less than 0, $A_{RI}(t)$ takes the minimum value. On the contrary, when $H(x(t), \mu^*(t), \nu^*(t), t) \le H(x(t), \mu, \nu^*(t), t)$ is to be satisfied, if $(S_{SR}(\lambda_R(t) - \lambda_S(t) + C_{SR})S^*(t)/(D_{SR\max} + D_{SR\min}))$ is greater than 0, $D_{SR}(t)$ chooses the minimum value, and if $(S_{SR}(\lambda_R(t) - \lambda_S(t) + C_{SR})S^*(t)/(D_{SR\max} + D_{SR\min}))$ is less than 0, $D_{SR}(t)$ chooses the maximum value; if $(S_{IR}(\lambda_R(t) - \lambda_I(t) + C_{IR})I^*(t)/(D_{IR\max} + D_{IR\min}))$ is greater than 0, $D_{IR}(t)$ chooses the minimum value, and if $(S_{IR}(\lambda_R(t) - \lambda_I(t) + C_{IR})I^*(t)/(D_{IR\max} + D_{IR\min}))$ is less than 0, $D_{IR}(t)$ chooses the maximum value.

4. Simulation

In this section, we will expand into three parts. The first part is to compare with the existing general epidemic models in turn. The second part is to analyze the impact of charging on the SILRD model. The third part is to discuss the impact of controllable and uncontrollable system input and node degree on the ΛSILRD model. In all three parts, the simulations are implemented in MATLAB R2017b. The abbreviations are applied in the section list in Table 2.

4.1. Comparison with General Epidemic Model. In this part, three general epidemic models will be compared, namely, Susceptible-Infected-Recovered (SIR) model [39], Susceptible-Exposed-Infected-Recovered (SEIR) model [40], and EiSIRS model [41]. Among the three models, SIR model is the basic, SEIR model extends the E state on the basis of the SIR model, and EiSIRS adds the corresponding sleeping state on the basis of the SIR model.

For the unification and reasonability of the analysis, we did not consider the multiple rounds of infection in the EiSIRS model, and EiSIRS model would be renamed as Susceptible-Susceptible & sleep-Infected-Infected & sleep-Recovered-Recovered & sleep-Dead (SsIiRrD) model to facilitate understanding, where lowercase letters represent the sleep state of the corresponding state.

Experimental parameters are set as follows: $P_{SI} = 0.1$, $P_{SR} = 0.4$, $P_{SD} = 0.0008$, $P_{ID} = 0.005$, $P_{IR} = 0.21$, $P_{RD} = 0.008$, $P_{EI} = 0.005$, $P_{ER} = 0.21$, $P_{ED} = 0.005$, $P_{Ss} = 0.006$, $P_{sS} = 0.006$, $P_{Ii} = 0.006$, $P_{iI} = 0.009$, $P_{Rr} = 0.006$, $P_{rR} = 0.006$, $P_{SL} = 0.0008$, $P_{IL} = 0.001$, $P_{RL} = 0.0008$, $P_{LD} = 0.3$, $P_{LR} = 0.6$.

Three general epidemic models have the same parameter settings except for their own defensive measures. Similarly, the SILRD with UAVs and the SILRD with solar energy harvesters have the same parameter settings except for the introduction of the L state and the corresponding defensive measures. In particular, the difference between the two SILRD models lies in the different charging methods. The first method is to use energy harvesters to capture solar energy and convert light energy into electrical energy to

Table 2: Table of abbreviations.

Abbreviation	Full name
EHWSNs	Energy-harvesting wireless sensor networks
WSNs	Wireless sensor networks
SILRD	Susceptible-Infected-Low (energy)-Recovered-Dead
ΛSILRD	Λ-Susceptible-Infected-Low (energy)-Recovered-Dead
UAVs	Unmanned aerial vehicles
SIR	Susceptible-Infected-Recovered
SEIR	Susceptible-Exposed-Infected-Recovered
SsIiRrD	Susceptible-Susceptible & sleep-Infected-Infected & sleep-Recovered-Recovered & sleep-Dead

supplement the energy of sensor nodes. The second method is to deploy UAVs to charge sensor nodes [21].

It is worth noting that the purpose of this part is to highlight the characteristics of the two SILRD model by comparing with other general epidemic models, so the system input, multiple types of malicious programs, and the nonlinear infection rate will be ignored. Figure 3 shows the evolution of sensor node under five epidemic models.

It can be seen from Figure 3(a) that the changes in the quantity of susceptible sensor nodes in the five models are very close. Except for SEIR, the other models had a high infection rate in the first few days, as depicted in Figure 3(b). Because the SEIR model exists an exposed state between the susceptibility and infection state, some infected sensor nodes were cleared during the exposure period. For recovered sensor nodes, the decline was more pronounced in SsIiRrD, followed by SEIR and SIR, as depicted in Figure 3(c). Among them, the quantity of recovered sensor nodes in SIRLD model decreased the most slowly and stay around 96% after 20 days. As shown in Figure 3(d), the order of increasing quantity of dead sensor nodes from fast to slow is SIR, SEIR, SsIiRrD, SILRD with UAVs, and SILRD with solar energy harvesters.

It can be seen from the comparison with other general epidemic models that the SILRD model can more effectively increase the quantity of recovered sensor nodes and reduce the quantity of dead sensor nodes. The phenomenon is more obvious in SILRD with solar energy harvesters. At the same time, the two SILRD model directly charges low-energy sensor nodes, which will effectively reduce the energy depletion of sensor nodes due to infections or daily work.

4.2. Effect of Charging on SILRD Model. Charging factors as one of the features of SILRD model will be discussed here. In this part, variations in the quantity of five node states, control variables and the quantity of high- and low-energy nodes, and the overall costs will be applied as indicators to explain the impact of charging.

Three scenarios will be discussed here, namely, SILRD model with solar energy harvesters, SILRD model with UAVs [21], and SILRD model without charging capability. In order to facilitate the analysis of the impact of charging, this part will ignore the impact of system input but will consider multiple types of malicious programs' attacks and nonlinear infection rates.

Unlike the previous section, the simulation here only considers one day, so the relevant simulation parameters have also been modified. Experimental parameters are set as follows: $S_{SI} = 0.005, S_{SR} = 0.05$, $S_{IR} = 0.05, S_{IL} = 0.001$, $S_{ID} = 0.005, S_{RI} = 0.005$, $P_{SL} = 0.0008, P_{LD} = 0.0016$, $P_{RL} = 0.0008, C_{SR} = 5$, $C_{IR} = 7, C_I = 10$, $C_L = 12, C_D = 20$, $A = 8, a = 0.5$, $b = 0.5, m = 12$, $n = 3$, and $C_N = 50$.

4.2.1. Evolution of Sensor Node under Various Charging Strategies. The solar charging power is formulated in (1). It is worth noting that SILRD with UAVs considers the situation of patching and charging at the same time, so low-energy sensor nodes will be transformed to recovered state directly. Figure 4 shows the evolution of sensor nodes under three charging strategies.

As can be seen from Figure 4(a), SILRD with solar energy harvesters can effectively increase the quantity of susceptible sensor nodes. However, under the attack of multiple types of malicious programs, the SILRD model with charging strategy cannot effectively restrain the growth of malicious programs, among which the case with solar charging is the most serious, as shown in Figure 4(b). Nevertheless, charging can effectively reduce the quantity of low-energy sensor nodes, as shown in Figure 4(c). Similarly, the quantity of recovered sensor nodes also increased due to the charging strategies, as depicted in Figure 4(d). The situation of energy depletion is very close as shown in Figure 4(e). Among them, the more accurate sorting from high to low should be SILRD with UAVs, followed by SILRD without charging and SILRD with solar energy harvesters.

Under the attack of multitype of malicious programs, the strategies with charging cannot inhibit the increase of the quantity of infected sensor nodes effectively, but it can greatly reduce the quantity of low-energy sensor nodes so as to increase the quantity of recovered sensor nodes. The strategy with solar charging is more widely distributed, so it can increase the quantity of recovered sensor nodes in highly efficient to keep the networks running well.

4.2.2. Variation on Dynamic Control Level. The variation of dynamic control will further reveal the cause of the evolution of node state, as depicted in Figure 5. Specifically, Figure 5(a) shows the changes in control variables in SILRD with solar energy harvesters, Figure 5(b) shows the changes in control

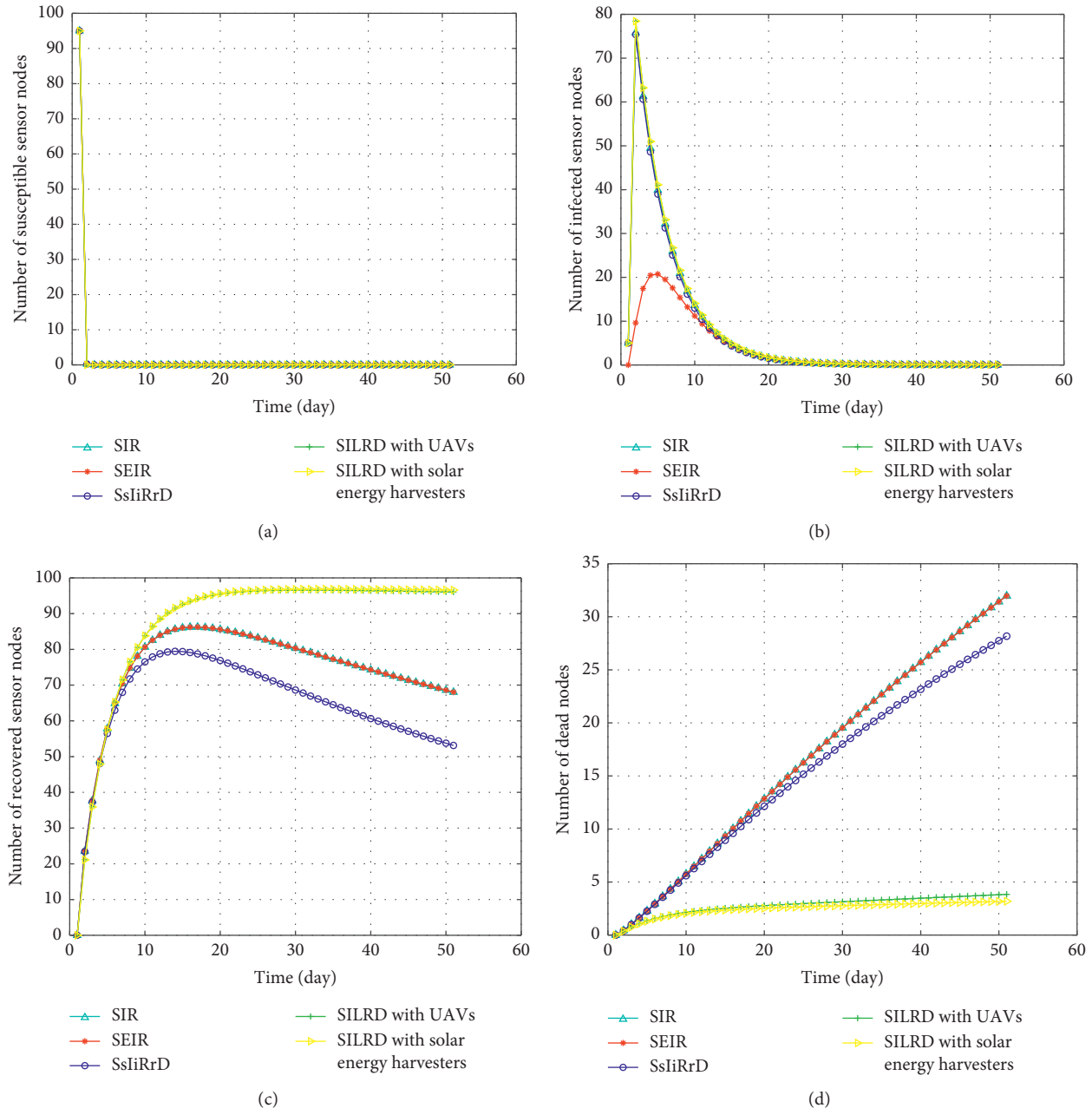

Figure 3: Evolution of node states under 5 epidemic models. (a) Susceptible state; (b) infected state; (c) recovered state; (d) dead state.

variables in SILRD with UAVs, and Figure 5(c) shows the changes in control variables in SILRD without charging.

In all three cases, the malicious programs stopped spreading at the beginning and peaked when $t = 2$. After propagation stops, the malicious programs still exist in the infected sensor nodes. After patching with maximum effort, due to the accumulation of costs, the networks stop patching after weighing. If the networks were patched again, the cost of patching would be higher than the cost of damage caused by malicious programs, so the networks stopped using the UAVs.

After UAVs stop patching, there are still exist malicious programs with strong and weak ability to destroy in the networks. Among them, the strategy with UAVs can quickly eliminate the malicious programs with weak damage ability ($t = 2$), followed by the solar charging strategy ($t = 4$) and finally the noncharging strategy ($t = 15$). However, malicious programs with strong destructive ability still present in the networks without completely clearing away.

4.2.3. Variation on the Quantity of High- and Low-Energy Nodes. In order to directly express the quantity of high- and low-energy sensor nodes in the networks, the form of histogram has been applied to show the variation on the quantity of high- and low-energy sensor nodes over time under different charging strategies, as depicted in Figure 6.

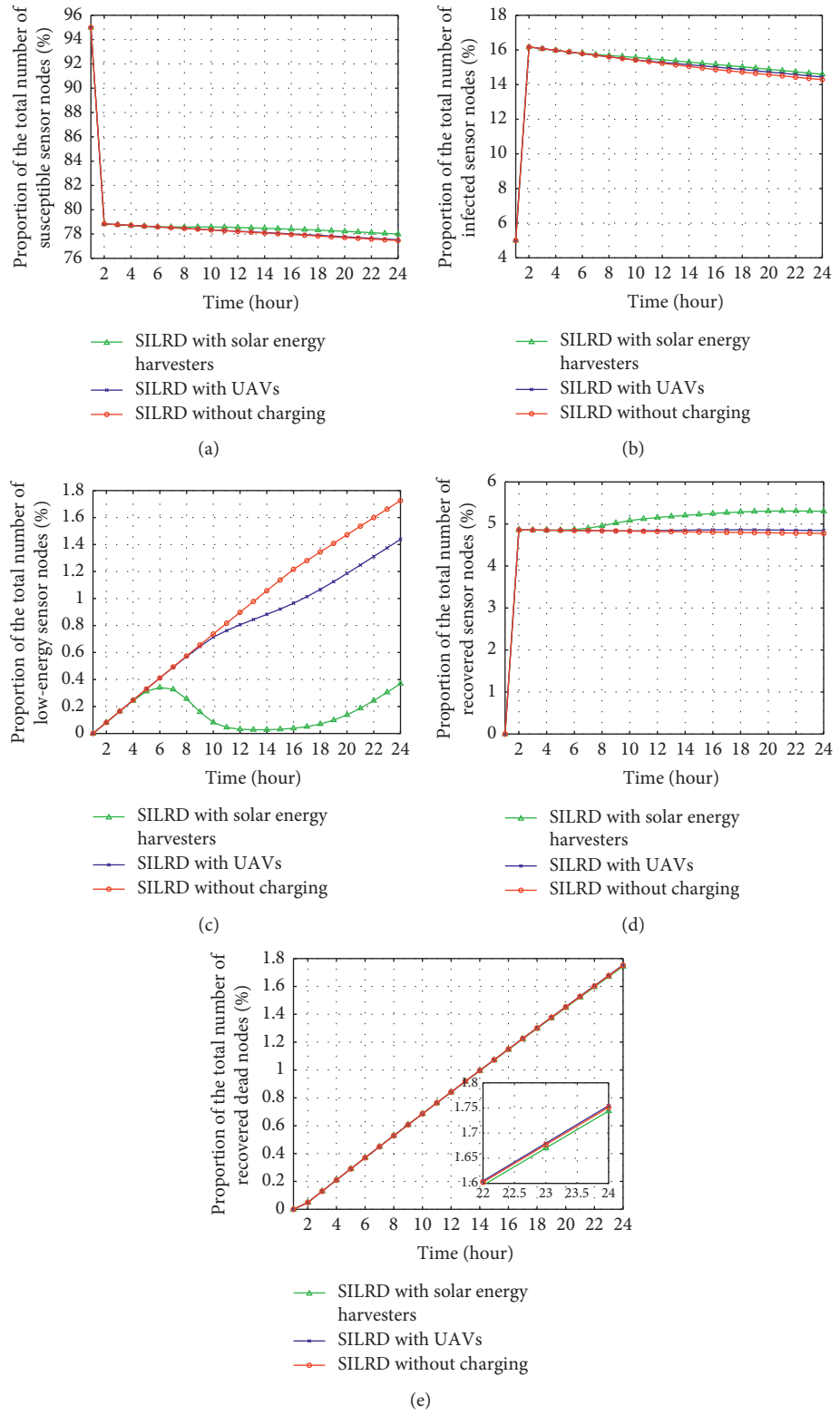

Figure 4: Evolution of sensor nodes under 3 charging strategies. (a) Susceptible state; (b) infected state; (c) low-energy state; (d) recovered state; (e) dead state.

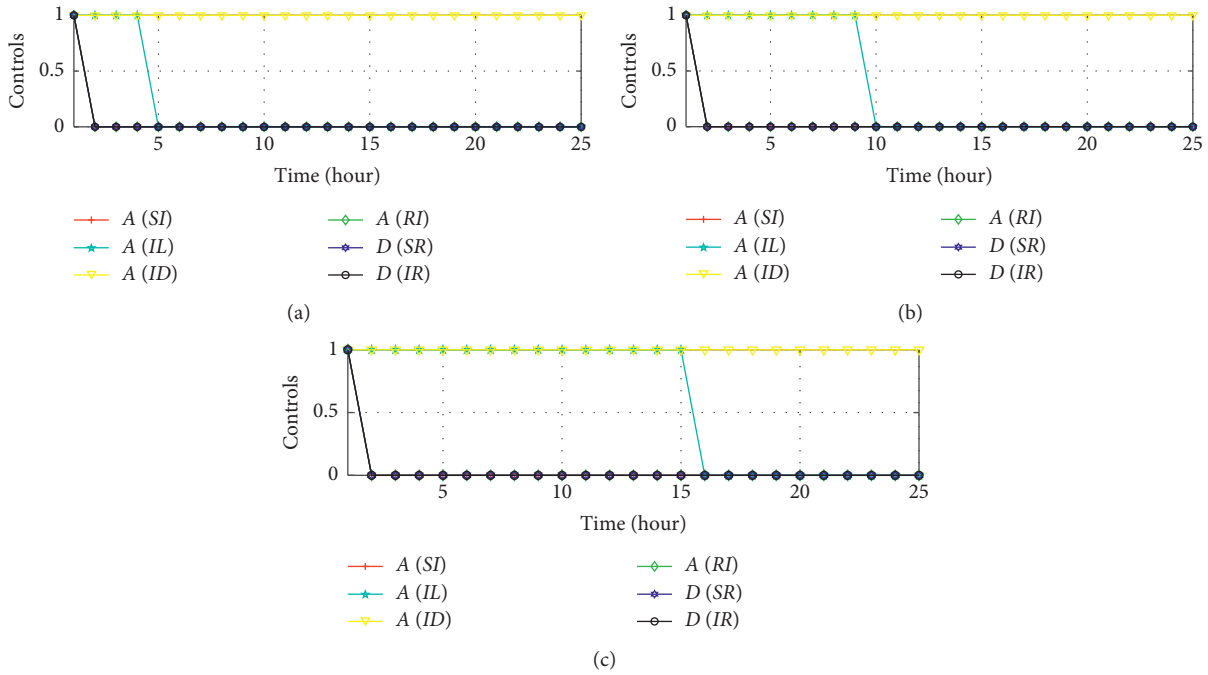

Figure 5: Dynamic control under 3 charging strategies. (a) Strategy with solar energy harvesters; (b) strategy with UAVs; (c) strategies without charging.

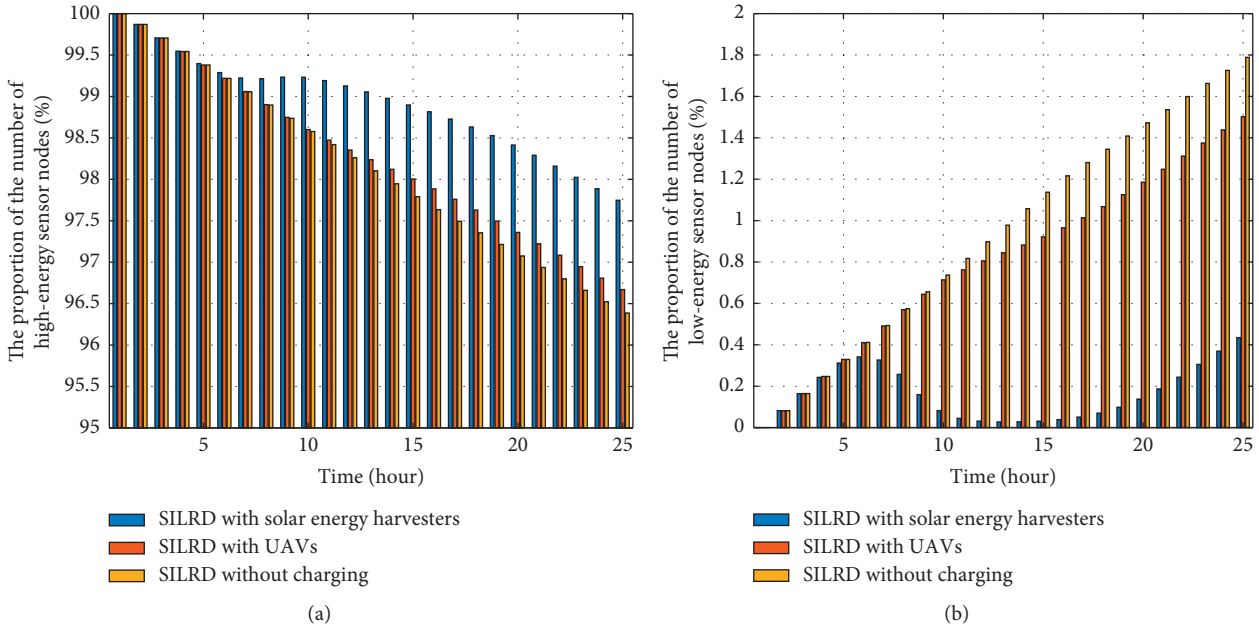

Figure 6: Variations on the quantity of high- and low-energy sensor nodes. (a) High-energy sensor nodes; (b) low-energy sensor nodes.

As can be seen from Figure 6(a), sensor nodes with high energy show a downward trend under the three strategies. Among them, the strategy without charging fell by the most quickly. The degree of elevation of the strategy with UAVs is determined by the quantity of UAVs. This paper assumes a small quantity of UAVs deployed because too many deployments would be costly. The strategy with solar energy harvesters assumes that each sensor node is equipped with the energy harvester, which is close to reality. Based on the analysis of Figures 6(a) and 6(b), it can be seen that, due to the comprehensive deployment of sensor nodes equipped with solar energy harvesters, the quantity of high-energy

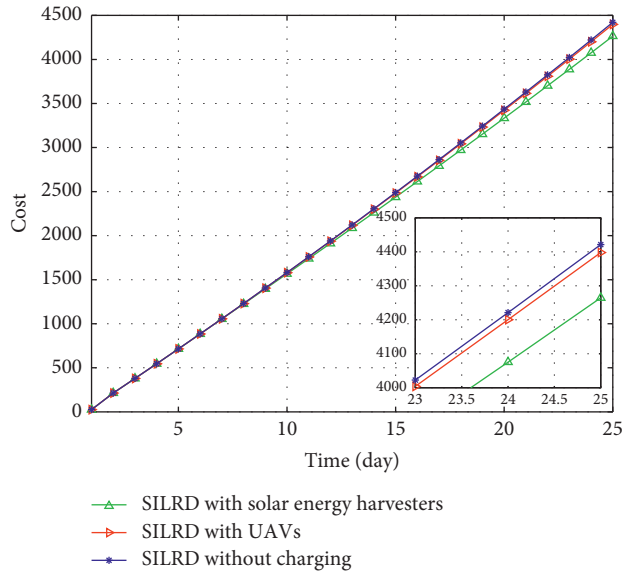

Figure 7: Overall costs under three charging strategies.

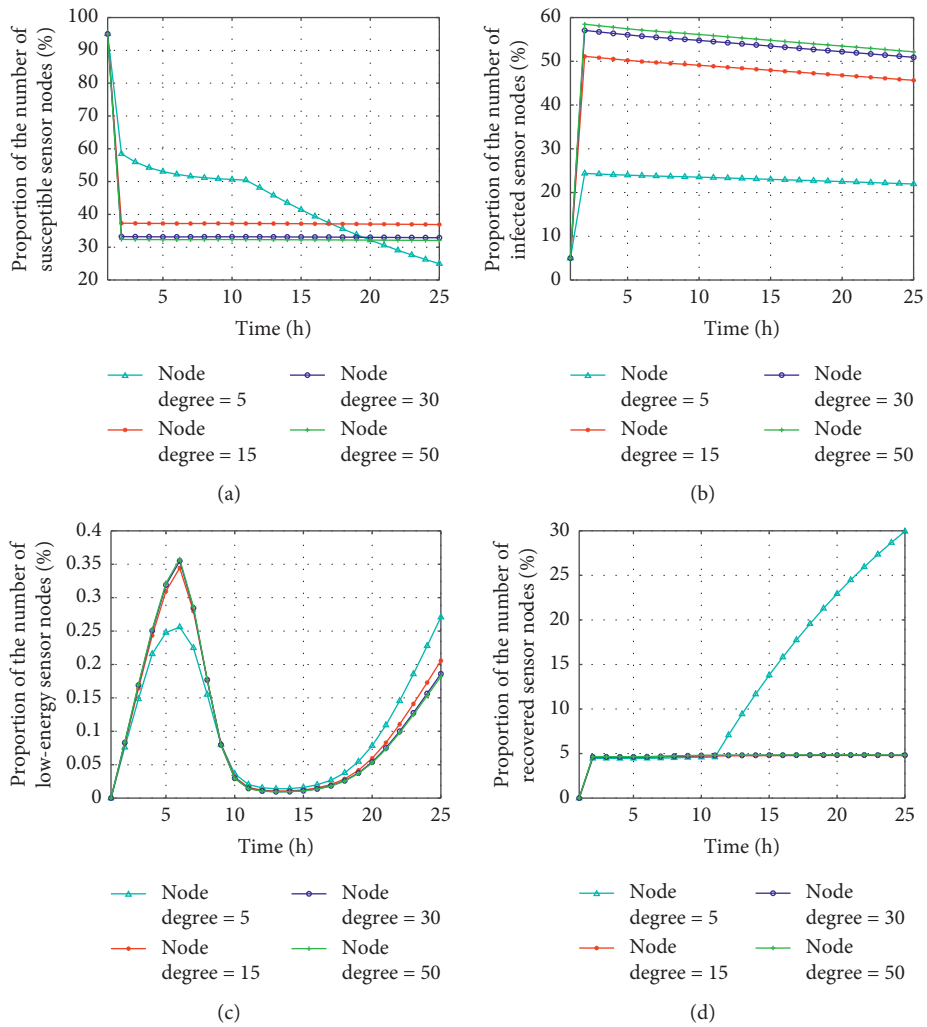

Figure 8: Continued.

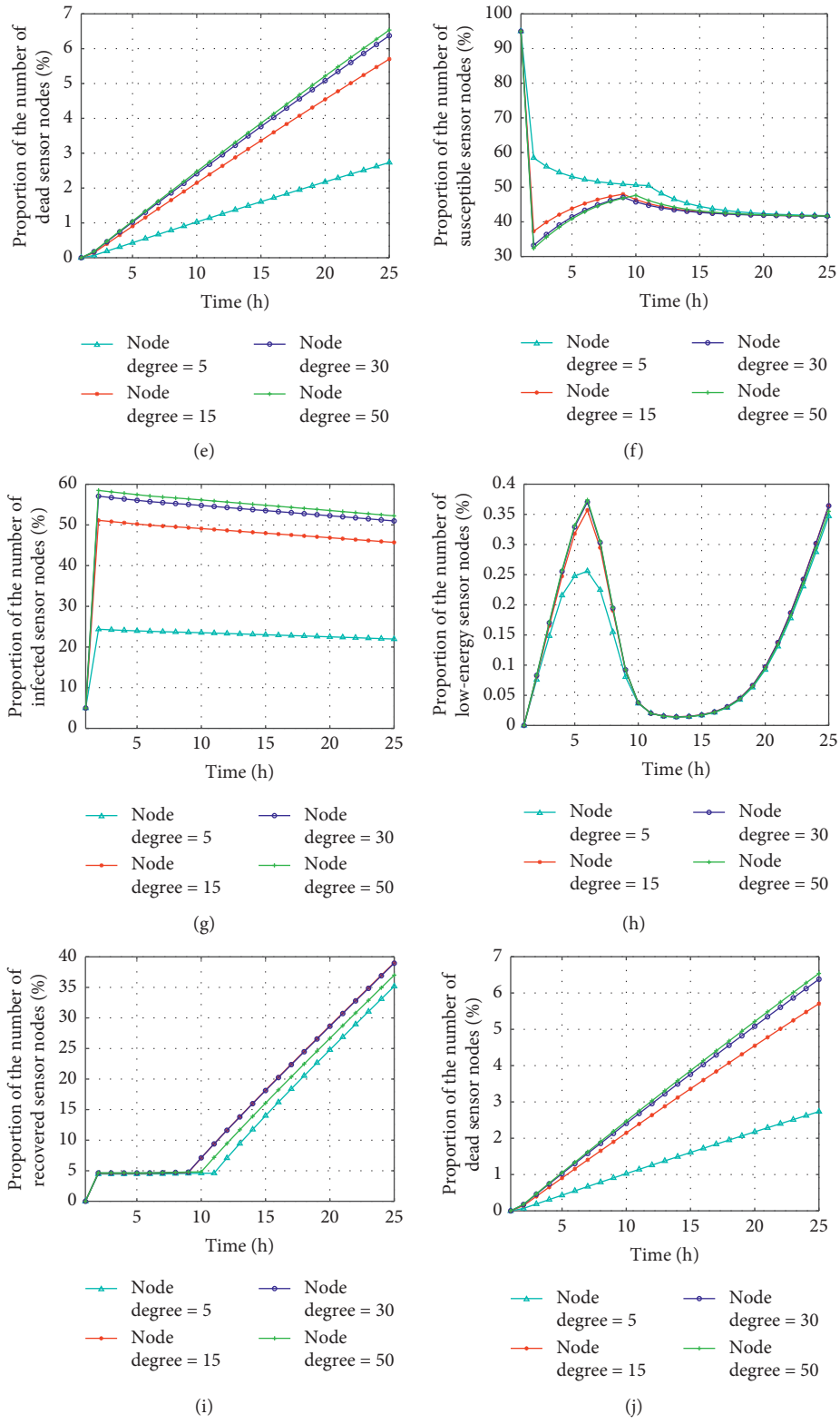

Figure 8: Evolution of sensor nodes with Logistic Growth in susceptible sensor nodes. (a) The quantity of susceptible sensor nodes with controllable input; (b) the quantity of infected sensor nodes with controllable input; (c) the quantity of low-energy sensor nodes with controllable input; (d) the quantity of recovered sensor nodes with controllable input; (e) the quantity of dead sensor nodes with controllable input; (f) the quantity of susceptible sensor nodes with uncontrollable input; (g) the quantity of infected sensor nodes with uncontrollable input; (h) the quantity of low-energy sensor nodes with uncontrollable input; (i) the quantity of recovered sensor nodes with uncontrollable input; (j) the quantity of dead sensor nodes with uncontrollable input.

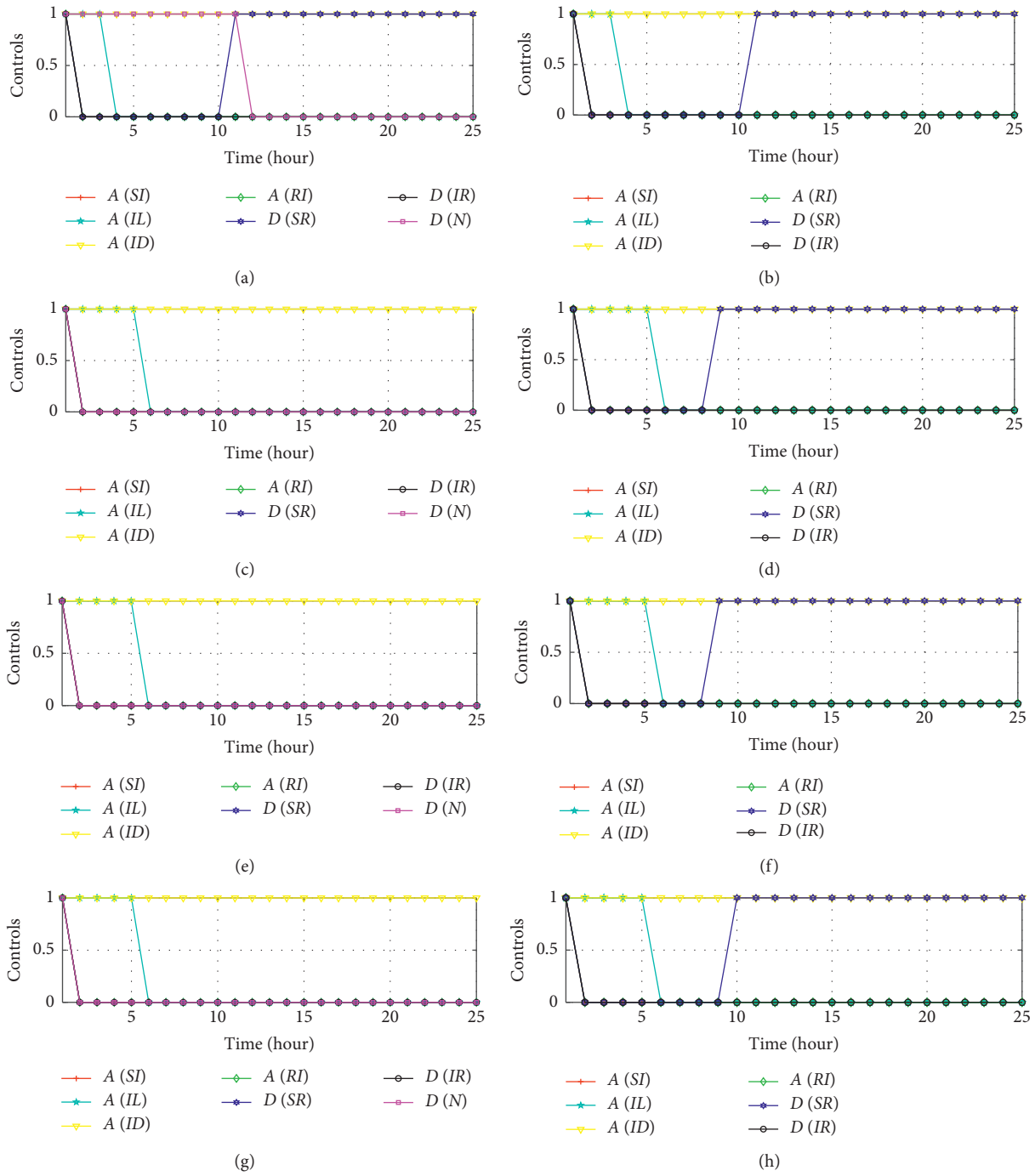

Figure 9: Variation of dynamic control variables. (a) Controllable input with node degree = 5; (b) controllable input with node degree = 15; (c) controllable input with node degree = 30; (d) controllable input with node degree = 50; (e) uncontrollable input with node degree = 5; (f) uncontrollable input with node degree = 15; (g) uncontrollable input with node degree = 30; (h) uncontrollable input with node degree = 50.

sensor nodes declines slowly. Moreover, the low-energy sensor nodes not only did not rise but also fell.

4.2.4. Overall Cost under Various Charging Strategies. Figure 7 shows the cost trends of the three strategies. The cost of solar charging is the lowest, followed by the strategy of deploying UAVs and finally the strategy of noncharging. For solar charging, since each sensor node is equipped with a solar energy harvester, there is no additional cost during capturing solar energy compared to the deployment of UAVs. In the conclusion of the previous section, charging can effectively improve the immunity of EHWSNs and reduce the quantity of dead sensor nodes, so as to achieve the purpose of reducing costs.

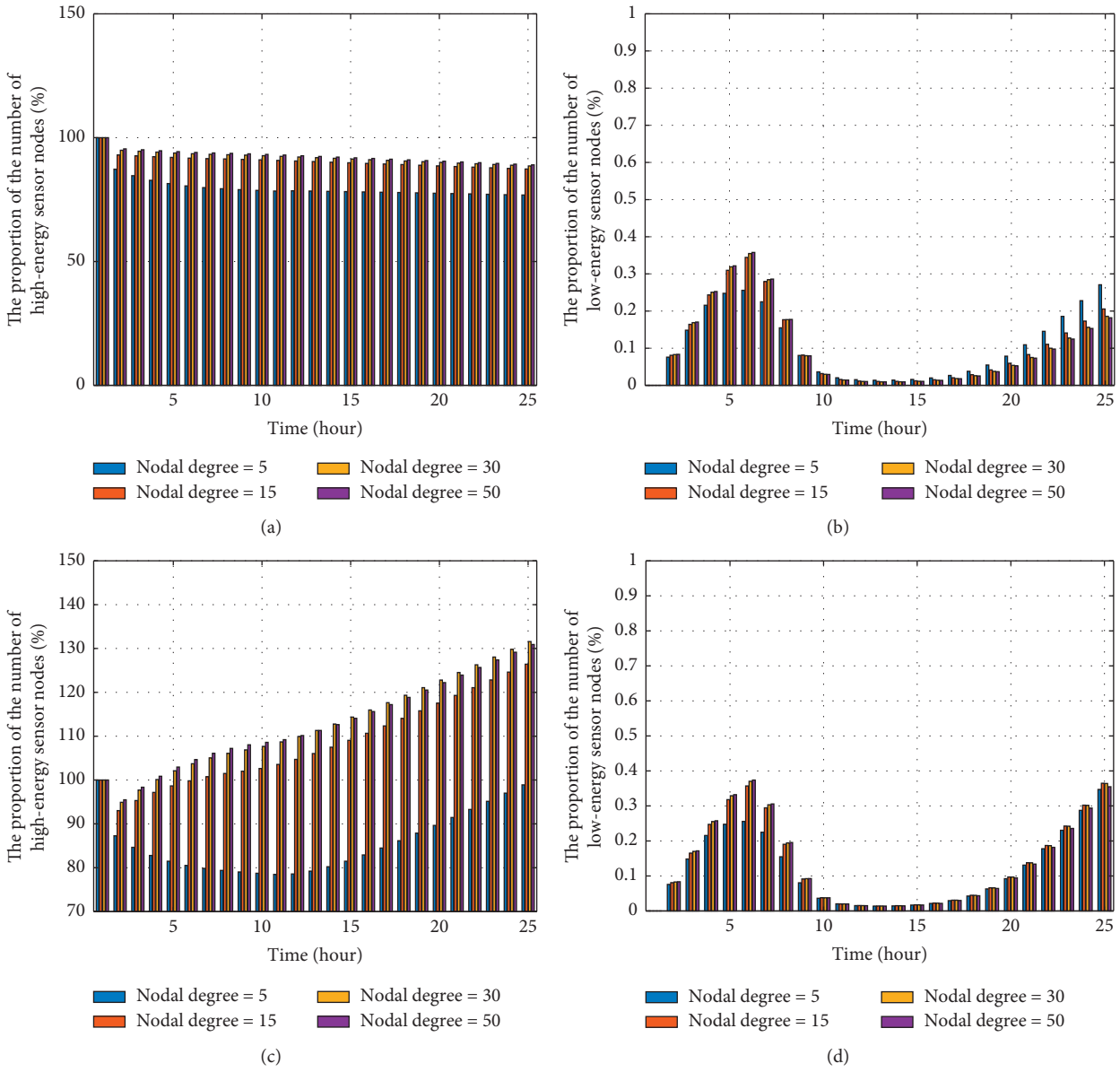

Figure 10: Variations in the quantity of high- and low-energy sensor nodes. (a) Variation of the quantity of high-energy sensor nodes with controllable input; (b) variation of the quantity of low-energy sensor nodes with controllable input; (c) variation of the quantity of high-energy sensor nodes with uncontrollable input; (d) variation of the quantity of low- energy sensor nodes with uncontrollable input.

4.3. Influence of Networks Input and Node Degree on ΛSILRD Model. This section mainly discusses the influence of controllable and uncontrollable input and node degree on ΛSILRD model. The formulation of networks input adopts (17). Node degrees are set to 5, 15, 30, and 50, respectively.

Similar to the previous section, this section also discusses the variation trend of four aspects, which are sensor nodes in various states, control variables, quantity of high- and low-energy sensor nodes, and overall costs.

The experimental parameters are the same as those in Section 4.2.

4.3.1. Evolution of Sensor Nodes in ΛSILRD Model. As a control group, uncontrollable input into the system will be considered. Figures 8(a)–8(e) show the evolution of node state when networks input contains control variables, and Figures 8(f)–8(j) show the evolution with uncontrollable input.

In both cases, evolutions of sensor nodes change uniformly except when node degree equals 5, as depicted in Figure 8. The quantity of susceptible sensor nodes fell rapidly in the first hour before reaching equilibrium, as depicted in Figures 8(a) and 8(f). In the case of input with control variables, the final stable value of the quantity of susceptible

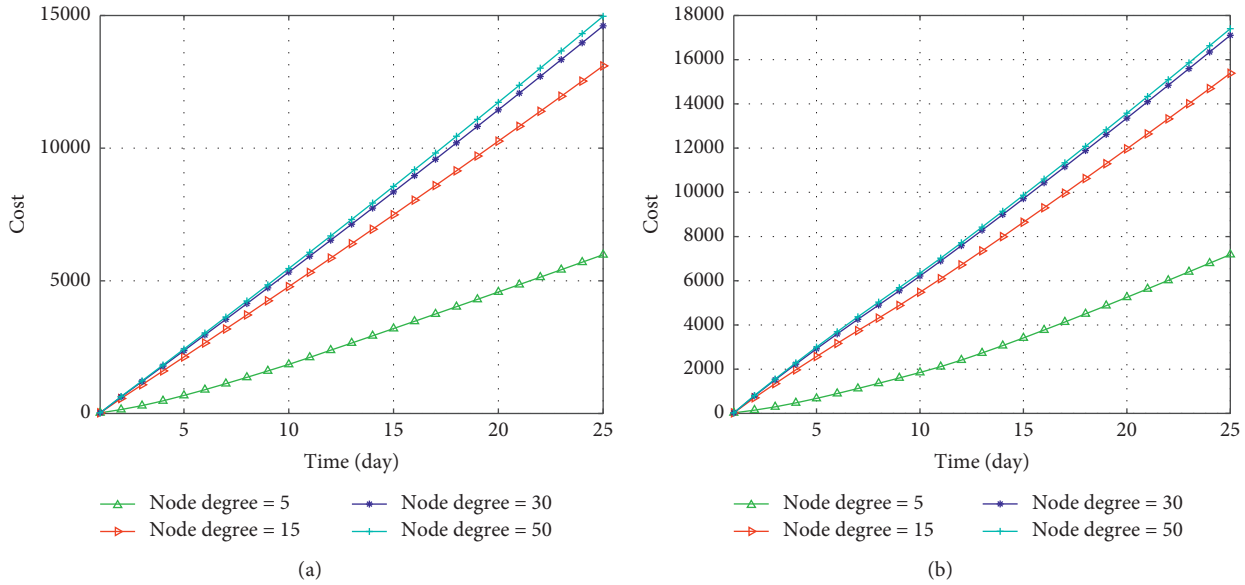

FIGURE 11: Overall cost with Logistic Growth in susceptible sensor nodes under different node degrees. (a) Strategy with controllable input; (b) strategy with uncontrollable input.

sensor nodes is related to node degree, as shown in Figure 8(a). With the increase of node degree, the stable value of the quantity of susceptible sensor nodes becomes lower. On the contrary, in the case of input without control variables, the quantity of susceptible nodes experienced a process of rapid decrease and then a slow rise and finally reached an equilibrium, as shown in Figure 8(f).

The changes of the quantity of infected sensor nodes, low-energy sensor nodes, and dead sensor nodes are very similar, as shown in Figures 8(b), 8(c), 8(e), 8(g), 8(h), and 8(j). In the case of input with control variables, the quantity of recovered sensor nodes remained stable except when the node degree equals 5, as shown in Figure 8(d). In the case of input without control variables, the quantity of recovered sensor nodes increased rapidly after a period of stabilization, as shown in Figure 8(i). In a word, as the node degree increases, the infection will become more severe, and the quantity of low-energy and death sensor nodes will increase.

4.3.2. Variation of Control Variables. In both cases, the quantity of infected sensor nodes reaches its peak when $t = 1$, so the networks stop patching, as shown in Figure 9. When $t = 10$, as more vulnerable sensor nodes exist in the networks, there is a risk of reinfection by malicious programs, so the networks start to patch the vulnerable sensor nodes again, as depicted in Figures 9(a), 9(b), 9(d), 9(f), and 9(h). When $t = 11$, the existing quantity of vulnerable sensor nodes is enough to maintain the normal operation of the networks, and the deployment of new sensor nodes will only bring more extra burden, so the networks will stop casting new sensor nodes, as shown in Figure 9(a). With the increase of node degree, the control strategy will not change greatly, as shown in Figures 9(c)–9(h).

4.3.3. Variation on the Quantity of High- and Low-Energy Sensor Nodes. Figure 10 shows the changing trend of the quantity of high- and low-energy sensor nodes in the networks. The variation trend of low-energy sensor nodes is the same in both cases, but the influence of node degree on both cases is different when T is greater than 16, as shown in Figures 10(b) and 10(d). As can be seen from Figure 10(a), when network input contains control variables, the quantity of high-energy sensor nodes basically remains at a very high level, about 90%. In the case of uncontrollable input, the quantity of high-energy sensor nodes will increase continuously, as shown in Figure 10(c). It is worth noting that, with the increase of node degree, the quantity of high-energy sensor nodes will increase. As the infection rate continues to rise, sensor nodes in susceptible state will quickly convert to infected state, so that the quantity of susceptible sensor nodes will rapidly decline. Therefore, it is necessary to quickly cast new sensor nodes to maintain the operation of the networks.

4.3.4. Overall Cost. Figure 11 shows the cumulative cost in both cases. With the increase of node degree, the costs do not show the same growth trend but tend to be saturated. In Figure 11(a), the numerical difference between the cost of node degree equal to 5 and the cost of node degree equal to 15 is about 7000, but the difference between 15 and 30 is about 1000, and the difference between 30 and 50 is about 200. Figure 11(b) shows the same phenomenon. The costs are lower in the case of controllable input than uncontrollable input under the same node degree owing to the networks with controllable input which can reduce the quantity of new sensor nodes and cut the cost of patching new sensor nodes, as shown in Figures 11(a) and 11(b).

5. Conclusion

By introducing Logistic Growth, nonlinear incidence, and charging by solar energy, this paper builds an ΛSILRD model suitable for EHWSNs. At the same time, the introduction of multiple types of malicious programs refines the model. By comparing with the existing epidemic models, we found that the SILRD has obvious advantages in increasing the quantity of recovered sensor nodes and reducing the quantity of death sensor nodes, especially SILRD with solar charging. Meanwhile, compared with the three charging strategies, we found that the SILRD with solar charging has the lowest cost. Finally, the influence of controllable input, uncontrollable input, and node degree on ΛSILRD model is revealed through the simulations. When the node degree is higher, the quantity of infected sensor nodes and dead sensor nodes will increase rapidly under the attack of multitype malicious programs with nonlinear infection rate but will tend to be saturated. At the same time, input that contains control variables can timely stop the delivery of new nodes and affect the subsequent network patching behavior, thereby reducing costs.

Although this paper proposes a malicious programs' propagation model that is close to reality, there are still many deficiencies. In the establishment of the solar charging model, this paper uses a simplified model and does not consider some random factors, like weather factors, human factors, and so on. At the same time, the topology of the EHWSNs and various delay phenomena are not further analyzed in this paper. However, in spite of this, the model and analytical methods proposed in this paper are believed to provide scholars in related fields some inspiration in the future.

Data Availability

The data used to support the findings of this study are included within the article, such as the coverage area of the WSNs, the maximum transmission radius of nodes, and transition probabilities among five nodal states.

Disclosure

All authors declare that (1) no support, financial or otherwise, has been received from any organization that may have an interest in the submitted work and (2) there are no other relationships or activities that could appear to have influenced the submitted work.

Conflicts of Interest

The authors have no conflicts of interest, financial or otherwise.

References

[1] W. O. Kermack and A. G. McKendrick, "Contribution to the mathematical theory of epidemics," *Proceedings of the Royal Society of London Series A*, vol. 115, pp. 700–721, 1927.

[2] 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.

[3] 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.

[4] R. K. Shakya, "Modified SI epidemic model for combating virus spread in spatially correlated wireless sensor networks," 2018, https://arxiv.org/pdf/1801.04744.pdf.

[5] T. Wang, Y. Z. Liang, Y. Yang et al., "An intelligent edge computing-based method to counter coupling problems in cyber-physical systems," *IEEE Network*, vol. 34, no. 3, pp. 16–22, 2020.

[6] 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.

[7] Y. Wu, H. Huang, Q. Wu, A. Liu, and T. Wang, "A risk defense method based on microscopic state prediction with partial information observations in social networks," *Journal of Parallel and Distributed Computing*, vol. 131, pp. 189–199, 2019.

[8] T. Wang, D. Zhao, S. B. Cai, W. J. Jia, and A. F. Liu, "Bi-directional prediction-based underwater data collection protocol for end-edge-cloud orchestrated system," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 7, pp. 4761–4799, 2020.

[9] Z. Li, W. Li, F. Lin et al., "Hybrid malware detection approach with feedback-directed machine learning," *Science China Information Sciences*, vol. 63, no. 3, Article ID 139103, 2020.

[10] G. Han, H. Wang, X. Miao, L. Liu, J. Jiang, and Y. Peng, "A dynamic multipath scheme for protecting source-location privacy using multiple sinks in WSNs intended for IIoT," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 8, pp. 5527–5538, 2020.

[11] Z. G. Zhao, Y. M. Huang, Z. Y. Zhen, and Y. Z. Li, "Data-driven false data-injection attack design and detection in cyber-physical systems," *IEEE Transactions on Cybernetics*, 2020.

[12] X. C. Li, K. Xie, X. Wang et al., "Quick and accurate false data detection in mobile crowd sensing," in *Proceedings of the 2020 IEEE Conference on Computer Communications*, pp. 2215–2223, Paris, France, April 2020.

[13] L. Liu, G. Han, Y. He, and J. Jiang, "Fault-tolerant event region detection on trajectory pattern extraction for industrial wireless sensor networks," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 2072–2080, 2020.

[14] T. Wang, Q. Wu, S. Wen et al., "Propagation modeling and defending of a mobile sensor worm in wireless sensor and actuator networks," *Sensors*, vol. 17, no. 12, pp. 139–156, 2017.

[15] R. Z. Nicola, N. Enrico, R. Giuseppe, P. Michael, and M. Antonella, "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.

[16] Y. Wu, H. Huang, N. Wu, Y. Wang, M. Z. Alam Bhuiyan, and T. Wang, "An incentive-based protection and recovery strategy for secure big data in social networks," *Information Sciences*, vol. 508, pp. 79–91, 2020.

[17] 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.

[18] 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 2015 IEEE 34th International Performance Computing and Communications Conference (IPCCC)*, pp. 1–8, Nanjing, China, December 2015.

[19] Z. J. Ji, H. Lin, S. B. Cao, Q. Y. Qi, and H. Z. Ma, "The complexity in complete graphic characterizations of multi-agent controllability," *IEEE Transactions on Cybernetics*, 2020.

[20] L. P. Mo and S. Y. Guo, "Consensus of linear multi-agent systems with persistent disturbances via distributed output feedback," *Journal of Systems Science and Complexity*, vol. 32, no. 3, pp. 835–845, 2019.

[21] G. Y. Liu, B. H. Peng, X. J. Zhong, and X. J. Lan, "Differential games of rechargeable wireless sensor networks against malicious programs based on SILRD propagation model," *Complexity*, vol. 2020, Article ID 5686413, 13 pages, 2020.

[22] M. H. R. Khouzani, S. Sarkar, and E. Altman, "Optimal dissemination of security patches in mobile wireless networks," *IEEE Transactions on Information Theory*, vol. 58, no. 7, pp. 4714–4732, 2012.

[23] H. Xu and X. Zhou, "Optimal power control in cooperative relay networks based on a differential game," *ETRI Journal*, vol. 36, no. 2, pp. 280–285, 2014.

[24] M. Hosseinzadeh, B. Sinopoli, and E. Garone, "Feasibility and detection of replay attack in networked constrained cyber-physical systems," in *Proceedings of the 2019 57th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pp. 712–717, Monticello, IL, USA, September 2019.

[25] 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.

[26] X. Ju, W. Liu, C. Zhang et al., "An energy conserving and transmission radius adaptive scheme to optimize performance of energy harvesting sensor networks," *Sensors*, vol. 18, no. 9, pp. 2885–2926, 2018.

[27] W. Qi, W. Liu, X. Liu et al., "Minimizing delay and transmission times with long lifetime in code dissemination scheme for high loss ratio and low duty cycle wireless sensor networks," *Sensors*, vol. 18, no. 10, pp. 3516–3560, 2018.

[28] M. Huang, W. Liu, T. Wang et al., "A game-based economic model for price decision making in cyber-physical-social systems," *IEEE Access*, vol. 7, pp. 111559–111579, 2019.

[29] J. A. Ansere, G. J. Han, L. Liu, Y. Peng, and M. Kamal, "Optimal resource allocation in energy efficient internet of things networks with imperfect CSI," *IEEE Internet Things Journal*, vol. 7, no. 6, pp. 5401–5411, 2020.

[30] 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.

[31] 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.

[32] L. Miao and S. Li, "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.

[33] 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. 55–68, 2012.

[34] S. Climent, A. Sanchez, S. Blanc, J. V. Capella, and R. Ors, "Wireless sensor network with energy harvesting: modeling and simulation based on a practical architecture using real radiation levels," *Concurrency and Computation: Practice and Experience*, vol. 28, no. 6, pp. 1812–1830, 2016.

[35] M. H. R. Khouzani, S. Sarkar, and E. Altman, "Maximum damage battery depletion attack in mobile sensor networks," *IEEE Transactions on Automatic Control*, vol. 56, no. 10, pp. 2358–2368, 2011.

[36] F. Avner, "Differential games," in *Handbook of Game Theory*, pp. 781–799, Elsevier, Amsterdam, Netherlands, 1994.

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

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

[39] J. C. Frauenthal, *Mathematical Modeling in Epidemiology*, Springer, New York, NY, USA, 1981.

[40] J. E. Cohen and E. Joel, "Infectious diseases of humans: dynamics and control," *JAMA: The Journal of the American Medical Association*, vol. 268, no. 23, p. 3381, 1992.

[41] 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.