sensors

MDPI

Article

Energy-Efficient Patching Strategy for Wireless Sensor Networks

Pengdeng Li [1], Lu-Xing Yang [2], Xiaofan Yang [1,*], Xiang Zhong [1,3], Junhao Wen [1] and Qingyu Xiong [1]

1 School of Big Data & Software Engineering, Chongqing University, Chongqing 400044, China; pengdengli1992@cqu.edu.cn (P.L.); zx5587@hnu.edu.cn (X.Z.); jhwen@cqu.edu.cn (J.W.); xiong03@cqu.edu.cn (Q.X.)
2 School of Information Technology, Deakin University, Melbourne, VIC 3125, Australia; y.luxing@deakin.edu.au
3 College of Mechanical and Vehicle Engineering, Hunan University, Changsha 410082, China
* Correspondence: xfyang1964@cqu.edu.cn

Received: 4 December 2018; Accepted: 7 January 2019; Published: 10 January 2019

Abstract: Wireless sensor networks (WSNs) are vulnerable to computer viruses. To protect WSNs from virus attack, the virus library associated with each sensor node must be updated in a timely way. This article is devoted to developing energy-efficient patching strategies for WSNs. First, we model the original problem as an optimal control problem in which (a) each control stands for a patching strategy, and (b) the objective functional to be optimized stands for the energy efficiency of a patching strategy. Second, we prove that the optimal control problem is solvable. Next, we derive the optimality system for solving the optimal control problem, accompanied with a few examples. Finally, we examine the effects of some factors on the optimal control. The obtained results help improve the security of WSNs.

Keywords: wireless sensor network; computer virus; patching strategy; energy efficiency; optimal control theory; optimality system

1. Introduction

Smart sensor nodes, which are low-power devices equipped with a set of sensors, a processor, a memory, a power supply, a radio, and an actuator, can sense, measure, and gather information from the environment. Wireless sensor networks (WSNs), which are self-organized wireless networks of smart sensor nodes, are used to cooperatively transmit the sensed data to the base station [1]. See Figure 1 for a small-sized WSN. WSNs have important applications in many fields, ranging from military target surveillance and natural disaster relief to human health monitoring and hazardous environment exploration [2–4]. As WSNs are typically deployed in uncontrollable or even hostile environments, they are vulnerable to a wide range of cyberattacks. In particular, a cyber malefactor may launch a virus attack to the target WSN and perform intended malicious operations on each infected sensor node, ranging from stealing or falsifying the data in this node to destroying the node [5,6]. In the past few decades, numerous WSN-related virus accidents have been reported in the literature [7–9]. Consequently, protecting WSNs from virus attack has long been a major issue in the domain of cybersecurity [10].

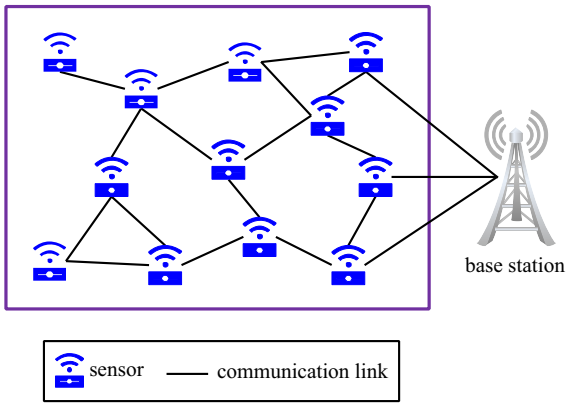

Figure 1. A small-sized WSN.

1.1. The Energy-Efficient Patching Problem

To enable a WSN to automatically defend against virus attack, all sensor nodes in the network must be equipped with an intrusion response system (IRS). With the continual emergence of new viruses, the virus libraries associated with these IRSs must be updated in a timely manner to deal with new viruses [11]. For this purpose, new virus patches must be continually injected into a subset of sensor nodes from outside the network and then forwarded from patched node to unpatched node until the whole network is covered [12]. See Figure 2 for a diagram of patching the WSN shown in Figure 1. Technically, patching can be realized by reprogramming the underlying communication protocols [13–15]. From the perspective of defending against new viruses, new patches should be injected and forwarded as early as possible.

On the other hand, all sensor nodes in a WSN are with limited power resources. When the energy of a node is depleted, it will die and disconnect from the network [16–18]. As the lifetime of the network depends on the number of active nodes and the connectivity of the network, energy must be used efficiently to maximize the network lifetime. As patches are injected and forwarded at the energy cost, we face the following problem:

Energy-efficient patching (EEP) problem: For a given WSN, develop an energy-efficient patching strategy.

To our knowledge, to date this problem has not been addressed. This paper focuses on the EEP problem.

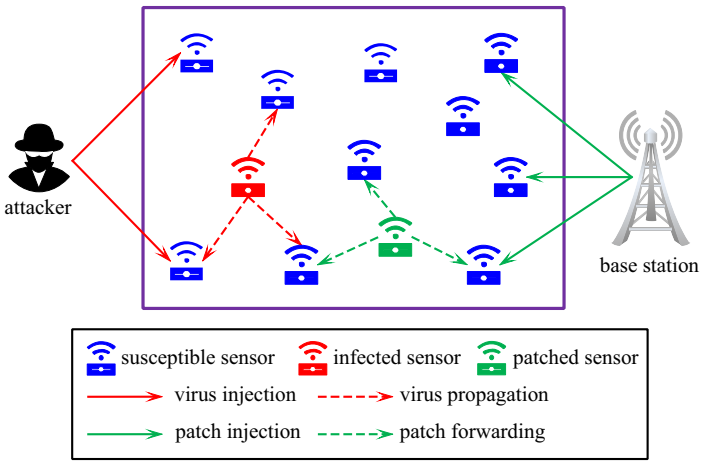

Figure 2. A diagram of patch injection and forwarding in the WSN shown in Figure 1.

1.2. Our Research Approach and Related Work

Optimal control theory deals with the problem of finding a control law for a given dynamic system such that a certain performance index is optimized [19,20]. Many practical problems have been

resolved using this theory [21–23]. In this paper, we are going to deal with the EEP problem in the framework of optimal control theory. The key to accomplishing this task is to measure the energy efficiency of a patching strategy. For this purpose, we need to accurately characterize the propagating process of digital viruses over a WSN.

In recent years, several WSN-oriented virus propagation models have been suggested. All these models build on the premise that the sensor nodes are distributed uniformly over a highly regular region (rectangular or circular, say). As a result, the virus propagation process can be characterized by a coarse-grained compartmental epidemic model [24–31]. For most real-world WSNs, however, the sensor nodes are distributed nonuniformly over a highly irregular region. Unfortunately, none of the above models applies to such WSNs.

The fine-grained node-level epidemic modeling [32,33] is especially suited to the characterization of propagation processes on arbitrary networks, because in the modeling process the topological structure of the network rather than its geometrical shape is accounted for. In recent years, this modeling technique has been successfully applied to diverse areas such as epidemic spreading [34], malware spreading [35–40], rumor spreading [41,42], and cybersecurity [43–45]. In this article, we are going to employ this modeling technique to establish a WSN-oriented virus-patch mixed propagation model. On this basis, we will model the EEP problem as an optimal control problem.

1.3. Main Contributions

This paper is devoted to dealing with the EEP problem. Our main contributions are overviewed as follows.

- By employing the node-level epidemic modeling technique, we establish a WSN-based virus-patch mixed propagation model. Thereby, we measure the energy efficiency of a patching strategy. On this basis, we model the EEP problem as an optimal control problem we refer to as the *EEP model* in which (a) each control stands for a patching strategy, and (b) the objective functional to be optimized stands for the energy efficiency of a patching strategy.
- We show that the EEP model admits an optimal control and hence is solvable. We then give a necessary condition for optimal control of the EEP model, from which we conclude that the optimal control is bang-bang and hence is easily realizable. On this basis, we derive the optimality system for solving the EEP model and illustrate its application. Finally, we examine the effects of some factors on the optimal patching strategy.

The remaining materials are organized in this fashion: Section 2 introduces the EEP model. Sections 3 and 4 present a method for solving the EEP model and give a few numeric examples, respectively. Section 5 reveals the effects of some factors on the optimal patching strategy. This work is closed by Section 6.

2. The Modeling of the Energy-Efficient Patching Problem

This section is devoted to the modeling of the EEP problem following these steps: (1) introduce basic terms and notations, (2) establish a WSN-related virus-patch mixed propagation model, (3) formulate a patching strategy, (4) measure the energy efficiency of a patching strategy, and (5) model the EEP problem as an optimal control problem.

2.1. Terms and Notations

Consider a WSN that operates in the time horizon $[0, T]$. Let $V = \{1, 2, \cdots, N\}$ denote the set of all sensor nodes in the network. Let $G = (V, E)$ denote the topological structure of the network, i.e., $\{i, j\} \in E$ if and only if nodes i and j are within the communication range of each other. Let $\mathbf{A} = \left(a_{ij}\right)_{N\times N}$ denote the adjacency matrix of G, i.e., $a_{ij} = 1$ or 0 according as $\{i, j\} \in E$ or not.

For our purpose, all nodes in the network are classified as three categories: *susceptible nodes*, *infected nodes*, and *patched nodes*. A susceptible node is one that is not infected with virus and has not received the newest patch. As a result, it is vulnerable to the viruses that can be handled only with the newest patch. An infected node is one that is infected with virus. A patched node is one that is not infected with virus and has received the newest patch. As a result, it is immune of all viruses. Let $X_i(t) = 0, 1$, and 2 denote that node i is susceptible, infected, and patched at time t, respectively. Then the vector

$$\mathbf{X}(t) = (X_1(t), \cdots, X_N(t)) \tag{1}$$

stands for the state of the network at time t. Let $S_i(t)$, $I_i(t)$, and $P_i(t)$ denote the probability of node i being susceptible, infected, and patched at time t, respectively.

$$S_i(t) = \Pr\{X_i(t) = 0\}, \quad I_i(t) = \Pr\{X_i(t) = 1\}, \quad P_i(t) = \Pr\{X_i(t) = 2\}. \tag{2}$$

As $S_i(t) = 1 - I_i(t) - P_i(t)$, the vector

$$\mathbf{E}(t) = (I_1(t), \cdots, I_N(t), P_1(t), \cdots, P_N(t)). \tag{3}$$

stands for the expected state of the network at time t.

Remark 1. *The initial network expected state* $\mathbf{E}(0)$ *can be estimated employing network probe.*

2.2. A Virus-Patch Mixed Propagation Model

For our purpose, we need to establish a WSN-related virus-patch mixed propagation model. To this end, let us make a set of hypotheses as follows.

Hypothesis 1. *Due to the emergence of new virus, each patched node becomes susceptible at an average rate of* δ*, which we refer to as the patch failure rate.*

Hypothesis 2. *Due to the injection of a new virus, each susceptible node gets infected at an average rate of* β_I*. We refer to* β_I *as the virus injection rate.*

Hypothesis 3. *Due to the impact of the infected node* j*, each susceptible node* i *with* $a_{ij} = 1$ *gets infected at an average rate of* β_P*, which we refer to as the virus propagation rate.*

Hypothesis 4. *Due to the injection of new patch, each unpatched node gets patched at time* t *at the rate of* $\gamma_I(t)$*, which we refer to as the patch injection rate at time* t*.*

Hypothesis 5. *Due to the influence of the patched node* j*, each unpatched node* i *with* $a_{ij} = 1$ *gets patched at time* t *at the rate of* $\gamma_F(t)$*, which we refer to as the patch forwarding rate at time* t*.*

Remark 2. *The patch failure rate* δ*, the virus injection rate* β_I*, and the virus propagation rate* β_P *can be estimated through collecting and analyzing the relevant historical data.*

Figure 3 shows the above hypotheses schematically. By the theory on continuous-time Markov chain [46], each susceptible node i gets infected at time t at an average rate of $\beta_I + \beta_P \sum_{j=1}^{N} a_{ij} I_j(t)$, and each infected node i gets patched at time t at the average rate of $\gamma_I(t) + \gamma_F(t) \sum_{j=1}^{N} a_{ij} P_j(t)$. It follows by Total Probability Formula that $I_i(t)$ ascends at time t at an average rate of

$$\left[\beta_I + \beta_P \sum_{j=1}^{N} a_{ij} I_j(t)\right] [1 - I_i(t) - P_i(t)] - \left[\gamma_I(t) + \gamma_F(t) \sum_{j=1}^{N} a_{ij} P_j(t)\right] I_i(t).$$

Similarly, $P_i(t)$ ascends at time t at an average rate of

$$\left[\gamma_I(t) + \gamma_F(t)\sum_{j=1}^{N} a_{ij}P_j(t)\right][1 - P_i(t)] - \delta P_i(t).$$

Combining the above discussions, the expected state of the network obeys the following differential system:

$$\begin{cases} \dfrac{dI_i(t)}{dt} = \left[\beta_I + \beta_P\sum_{j=1}^{N} a_{ij}I_j(t)\right][1 - I_i(t) - P_i(t)] - \left[\gamma_I(t) + \gamma_F(t)\sum_{j=1}^{N} a_{ij}P_j(t)\right] I_i(t), \\ \dfrac{dP_i(t)}{dt} = \left[\gamma_I(t) + \gamma_F(t)\sum_{j=1}^{N} a_{ij}P_j(t)\right][1 - P_i(t)] - \delta P_i(t), \\ 0 \le t \le T, 1 \le i \le N, \\ \mathbf{E}(0) = \mathbf{E}_0. \end{cases} \tag{4}$$

We refer to the system as a *WSN-oriented virus-patch mixed propagation model*.

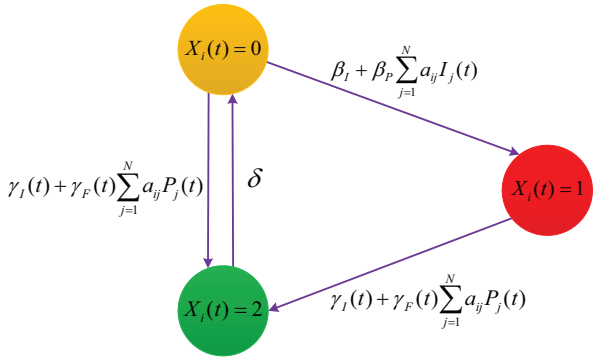

Figure 3. Diagram of the hypotheses (H_1)–(H_5).

2.3. Formulating a Patching Strategy

We refer to the function $\gamma_I(t)$ $(0 \le t \le T)$ as a *patch injection strategy*, the function $\gamma_F(t)$ $(0 \le t \le T)$ as a *patch forwarding strategy*, and the two-dimensional vector-valued function $\mathbf{u}$ defined by

$$\mathbf{u}(t) = (\gamma_I(t), \gamma_F(t)), \quad 0 \le t \le T, \tag{5}$$

as a *patching strategy*. The patching strategy is under control of the network administrator. In this paper, we assume the admissible set of patching strategy is

$$\mathcal{U} = \left\{\mathbf{u} \in L[0,T]^2 \mid \gamma_I(t) \le \overline{\gamma_I}, \gamma_F(t) \le \overline{\gamma_F}, 0 \le t \le T\right\}, \tag{6}$$

where $L[0,T]$ stands for the set of all Lebesgue integrable functions defined on the interval $[0,T]$ [47].

Remark 3. *The maximum allowable patch injection rate $\overline{\gamma_I}$ is determined by the budget for developing new patches. The maximum allowable patch forwarding rate $\overline{\gamma_F}$ is determined by the energy budget for forwarding patches.*

In this context, we may write the model (4) in matrix notation as follows.

$$\begin{cases} \dfrac{d\mathbf{E}(t)}{dt} = \mathbf{F}(\mathbf{E}(t), \mathbf{u}(t)), \quad 0 \le t \le T, \\ \mathbf{E}(0) = \mathbf{E}_0. \end{cases} \tag{7}$$

2.4. Measuring the Energy Efficiency of a Patching Strategy

This subsection is dedicated to estimating the energy efficiency of a patching strategy. The energy efficiency of a patching strategy $\mathbf{u} = (\gamma_I, \gamma_F)$ consists of two parts: the losses caused by viruses, and the energy cost used for patching. For our purpose, let us introduce a pair of hypotheses as follows.

Hypothesis 6. *The average loss per unit time caused by each infected node is w_1 units (dollars, say), which we refer to as the loss coefficient.*

Hypothesis 7. *The average energy cost per unit time used for each node to transmit or receive patches at a rate of γ is $w_2\gamma$ units. We refer to w_2 as the energy coefficient.*

Remark 4. *The loss coefficient w_1 can be estimated by estimating the average value of the environmental data gained by the sensor nodes in the network. The energy coefficient w_2 is a common physical parameter of the sensor nodes in the network.*

According to the hypothesis (H_6), the average loss caused by the node i in the infinitesimal time horizon $[t, t+dt)$ is $w_1 dt$ or zero according as this node is infected or not at time t. Therefore, the expected loss caused by the node i in the infinitesimal time horizon $[t, t+dt)$ is $I_i(t) \cdot w_1 dt + (1 - I_i(t)) \cdot 0 = w_1 I_i(t) dt$. Hence, the expected loss of the whole network in the time horizon $[0, T]$ is

$$L(\mathbf{u}) = w_1 \int_0^T \sum_{i=1}^N I_i(t) dt. \tag{8}$$

Similarly, the expected energy overhead of the whole network for transmitting patches in the time horizon $[0, T]$ is

$$E_T(\mathbf{u}) = w_2 \int_0^T \gamma_F(t) \sum_{i=1}^N [1 - P_i(t)] \sum_{j=1}^N a_{ij} P_j(t) dt. \tag{9}$$

and the expected energy overhead of the whole network for receiving patches in the time horizon $[0, T]$ is

$$E_R(\mathbf{u}) = w_2 \int_0^T \gamma_I(t) \sum_{i=1}^N [1 - P_i(t)]\, dt + w_2 \int_0^T \gamma_F(t) \sum_{i=1}^N [1 - P_i(t)] \sum_{j=1}^N a_{ij} P_j(t) dt. \tag{10}$$

Hence, the expected energy overhead of the whole network for transmitting and receiving patches in the time horizon $[0, T]$ is

$$\begin{aligned} E(\mathbf{u}) &= E_T(\mathbf{u}) + E_R(\mathbf{u}) \\ &= w_2 \int_0^T \gamma_I(t) \sum_{i=1}^N [1 - P_i(t)]\, dt + 2w_2 \int_0^T \gamma_F(t) \sum_{i=1}^N [1 - P_i(t)] \sum_{j=1}^N a_{ij} P_j(t) dt. \end{aligned} \tag{11}$$

Combining the above discussions, we conclude that the energy efficiency of the patching strategy $\mathbf{u}$ can be measured by

$$\begin{aligned} J(\mathbf{u}) &= L(\mathbf{u}) + E(\mathbf{u}) \\ &= w_1 \int_0^T \sum_{i=1}^N I_i(t) dt + w_2 \int_0^T \gamma_I(t) \sum_{i=1}^N [1 - P_i(t)]\, dt + 2w_2 \int_0^T \gamma_F(t) \sum_{i=1}^N [1 - P_i(t)] \sum_{j=1}^N a_{ij} P_j(t) dt. \end{aligned} \tag{12}$$

2.5. The Modeling of the EEP Problem

Based on previous discussions, we model the EEP problem as the following optimal control problem:

$$\begin{aligned} &\mathrm{Min}_{\mathbf{u}\in\mathcal{U}} J(\mathbf{u}) = \int_0^T L(\mathbf{E}(t),\mathbf{u}(t))dt \\ &\text{subject to } \begin{cases} \dfrac{d\mathbf{E}(t)}{dt} = \mathbf{F}(\mathbf{E}(t),\mathbf{u}(t)), \quad 0 \le t \le T, \\ \mathbf{E}(0) = \mathbf{E}_0. \end{cases} \end{aligned} \tag{13}$$

Here,

$$L(\mathbf{E}(t),\mathbf{u}(t)) = w_1 \sum_{i=1}^{N} I_i(t) + w_2\gamma_I(t) \sum_{i=1}^{N} [1 - P_i(t)] + 2w_2\gamma_F(t) \sum_{i=1}^{N} [1 - P_i(t)] \sum_{j=1}^{N} a_{ij}P_j(t). \tag{14}$$

We refer to this optimal control problem as the *EEP model*. In the model, each admissible control stands for an allowable patching strategy, the objective functional stands for the energy efficiency of an allowable patching strategy, and each optimal control stands for an EEP strategy.

The EEP model (13) is determined by the 10-tuple

$$\mathcal{M} = (G, T, \beta_I, \beta_P, \delta, \overline{\gamma_I}, \overline{\gamma_P}, w_1, w_2, \mathbf{E}_0) \tag{15}$$

3. A Method for Solving the EEP Model

In the previous section, the EEP problem was modeled as an optimal control problem we refer to as the EEP model. This section is dedicated to deriving a systematic method for solving the EEP model using optimal control theory. First, we show that the EEP model is solvable. Second, we give a necessary condition for optimal control of the EEP model. On this basis, we present the optimality system for solving the EEP model.

3.1. The Solvability of the EEP Model

First, let us examine the solvability of the EEP model. For this purpose, we need the following lemma, which is a direct corollary of a classical theorem in optimal control theory [20].

Lemma 1. *The EEP model (13) has an optimal control if the following five conditions hold simultaneously.*

(C_1) $\mathcal{U}$ is closed and convex.
(C_2) There is $\mathbf{u} \in \mathcal{U}$ such that the affiliated model (7) is solvable.
(C_3) $\mathbf{F}(\mathbf{E},\mathbf{u})$ is bounded by a linear function in $\mathbf{E}$.
(C_4) $L(\mathbf{E},\mathbf{u})$ is convex on $\mathcal{U}$.
(C_5) $L(\mathbf{E},\mathbf{u}) \ge c_1\|\mathbf{u}\|_2^{\rho} + c_2$ for some $\rho > 1$, $c_1 > 0$ and c_2.

The main result in this subsection is given below.

Theorem 1. *The EEP model (13) admits an optimal control.*

Proof. Let $\mathbf{u} = (\gamma_I, \gamma_F)$ be a limit point of $\mathcal{U}$. Then there is a sequence of points of $\mathcal{U}$, $\mathbf{u}^{(n)} = \left(\gamma_I^{(n)}, \gamma_F^{(n)}\right), n = 1, 2, \cdots$, that approaches $\mathbf{u}$. As the function space $L[0,T]^2$ is complete, we have $\mathbf{u} \in L[0,T]^2$. Hence, the closeness of $\mathcal{U}$ follows from the observation that for $0 \le t \le T$, there hold

$$\gamma_I(t) = \lim_{n\to\infty} \gamma_I^{(n)}(t) \le \overline{\gamma_I}, \quad \gamma_F(t) = \lim_{n\to\infty} \gamma_F^{(n)}(t) \le \overline{\gamma_F}.$$

Let $\mathbf{u}^{(1)}, \mathbf{u}^{(2)} \in \mathcal{U}$, $0 < \alpha < 1$. As $L[0,T]^2$ is a real vector space, we have $(1-\alpha)\mathbf{u}^{(1)} + \alpha\mathbf{u}^{(2)} \in L[0,T]^2$. Hence, the convexity of $\mathcal{U}$ follows from the observation that for $0 \le t \le T$, there hold

$$(1-\alpha)\gamma_I^{(1)}(t) + \alpha\gamma_I^{(2)}(t) \le \overline{\gamma_I}, \quad (1-\alpha)\gamma_F^{(1)}(t) + \alpha\gamma_F^{(2)}(t) \le \overline{\gamma_F}.$$

The first condition of Lemma 1 is proven. Let $\overline{\mathbf{u}}(t) \equiv (\overline{\gamma_I}, \overline{\gamma_F})$. Then $\overline{\mathbf{u}} \in \mathcal{U}$. As $\mathbf{F}(\mathbf{E}, \overline{\mathbf{u}})$ is continuously differentiable, it follows by Continuation Theorem for Differential Systems [48] that the model (7) is solvable. The second condition is proven. The third condition follows from the boundedness of I_i, P_i, and $\mathbf{u}$, and the fourth condition follows from that L is linear in $\mathbf{u}$ and hence is convex. The fifth condition follows from the observation that

$$L(\mathbf{E}, \mathbf{u}) \ge 0 \ge \left(\gamma_I^2 + \gamma_F^2\right) - \left(\overline{\gamma_I}^2 + \overline{\gamma_F}^2\right) = \|\mathbf{u}\|_2^2 - \left(\overline{\gamma_I}^2 + \overline{\gamma_F}^2\right).$$

By Lemma 1, the proposition holds. □

3.2. A Necessary Condition for Optimal Control of the EEP Model

For our purpose, we need to give a necessary condition for optimal control of the EEP model. To this end, consider the Hamiltonian of the EEP model (13), which is given by

$$\begin{aligned} H(\mathbf{E}, \mathbf{u}, \mathbf{z}) = {} & w_1 \sum_{i=1}^{N} I_i(t) + w_2\gamma_I(t) \sum_{i=1}^{N} [1 - P_i(t)] + 2w_2\gamma_F(t) \sum_{i=1}^{N} [1 - P_i(t)] \sum_{j=1}^{N} a_{ij} P_j(t) \\ & + \sum_{i=1}^{N} \lambda_i(t) \left\{ \left[\beta_I + \beta_P \sum_{j=1}^{N} a_{ij} I_j(t) \right] [1 - I_i(t) - P_i(t)] - \left[\gamma_I(t) + \gamma_F(t) \sum_{j=1}^{N} a_{ij} P_j(t) \right] I_i(t) \right\} \\ & + \sum_{i=1}^{N} \mu_i(t) \left\{ \left[\gamma_I(t) + \gamma_F(t) \sum_{j=1}^{N} a_{ij} P_j(t) \right] [1 - P_i(t)] - \delta P_i(t) \right\}, \end{aligned} \tag{16}$$

where $\mathbf{z}(t) = (\lambda_1(t), \cdots, \lambda_N(t), \mu_1(t), \cdots, \mu_N(t))$ $(0 \le t \le T)$ is the adjoint.

A necessary condition for optimal control of the EEP model is given below.

Theorem 2. *Suppose* $\mathbf{u}$ *is an optimal control of the EEP model (13),* $\mathbf{E}$ *is the solution to the affiliated model (7). Then there exists* $\mathbf{z}$ *with* $\mathbf{z}(T) = \mathbf{0}$ *such that*

$$\begin{cases} \dfrac{d\lambda_i(t)}{dt} = -w_1 + \lambda_i(t) \left[\beta_I + \beta_P \sum_{j=1}^{N} a_{ij} I_j(t) + \gamma_I(t) + \gamma_F(t) \sum_{j=1}^{N} a_{ij} P_j(t) \right] - \beta_P \sum_{j=1}^{N} a_{ji} \lambda_j(t) \left[1 - I_j(t) - P_j(t) \right], \\ \dfrac{d\mu_i(t)}{dt} = w_2\gamma_I(t) - \gamma_F(t) \sum_{j=1}^{N} a_{ji} \left[(2w_2 + \mu_j(t))(1 - P_j(t)) - \lambda_j(t) I_j(t) \right] + 2w_2\gamma_F(t) \sum_{j=1}^{N} a_{ij} P_j(t) \\ \qquad\qquad + \lambda_i(t) \left[\beta_I + \beta_P \sum_{j=1}^{N} a_{ij} I_j(t) \right] + \mu_i(t) \left[\delta + \gamma_I(t) + \gamma_F(t) \sum_{j=1}^{N} a_{ij} P_j(t) \right], \\ \qquad\qquad 1 \le i \le N, 0 \le t \le T. \end{cases} \tag{17}$$

Moreover,

$$\gamma_I(t) = \begin{cases} 0 & \text{if } \sum_{i=1}^{N} (w_2 + \mu_i(t))(1 - P_i(t)) > \sum_{i=1}^{N} \lambda_i(t) I_i(t), \\ \overline{\gamma_I} & \text{if } \sum_{i=1}^{N} (w_2 + \mu_i(t))(1 - P_i(t)) < \sum_{i=1}^{N} \lambda_i(t) I_i(t). \end{cases} \tag{18}$$

$$\gamma_F(t) = \begin{cases} 0 & \text{if } \sum_{i=1}^{N}(2w_2 + \mu_i(t))(1 - P_i(t)) \sum_{j=1}^{N} a_{ij}P_j(t) > \sum_{i=1}^{N} \lambda_i(t)I_i(t) \sum_{j=1}^{N} a_{ij}P_j(t), \\ \overline{\gamma_F} & \text{if } \sum_{i=1}^{N}(2w_2 + \mu_i(t))(1 - P_i(t)) \sum_{j=1}^{N} a_{ij}P_j(t) < \sum_{i=1}^{N} \lambda_i(t)I_i(t) \sum_{j=1}^{N} a_{ij}P_j(t). \end{cases} \tag{19}$$

Proof. According to Pontryagin Minimum Principle [20], there exists $\mathbf{z}$ such that

$$\frac{d\lambda_i(t)}{dt} = -\frac{\partial H(\mathbf{E}(t), \mathbf{u}(t), \mathbf{z}(t))}{\partial I_i(t)}, \quad 1 \le i \le N, 0 \le t \le T,$$
$$\frac{d\mu_i(t)}{dt} = -\frac{\partial H(\mathbf{E}(t), \mathbf{u}(t), \mathbf{z}(t))}{\partial P_i(t)}, \quad 1 \le i \le N, 0 \le t \le T.$$

Thus, the system (17) follows by direct calculations. As the terminal cost is unspecified, and the final state is free, the transversality condition $\mathbf{z}(T) = \mathbf{0}$ holds. Finally, by using the optimality condition we have

$$\mathbf{u}(t) = \arg\min_{\widetilde{\mathbf{u}} \in \mathcal{U}} H(\mathbf{E}(t), \widetilde{\mathbf{u}}(t), \mathbf{z}(t)), \quad 0 \le t \le T.$$

The systems (18) and (19) follow by direct calculations. □

Remark 5. *By this theorem, every optimal control of the EEP model (13) is bang-bang and hence easily realizable.*

3.3. The Optimality System for the EEP Model

By optimal control theory, the systems (4), (17), (18), and (19) together with $\mathbf{E}(0) = \mathbf{E}_0$ and $\mathbf{z}(T) = \mathbf{0}$ constitute the optimality system for the EEP model (13). In view of the existence of optimal control, we can get an optimal control of the EEP model by solving the optimality system using Forward-Backward Euler Scheme.

4. Numerical Examples

In the previous section, we presented the optimality system for solving the EEP model (13). In this section, we solve three instances of the EEP model to get their respective optimal controls. For this purpose, consider the real-world WSN given in [49] in which there are 66,917 nodes and 885,441 edges. Denote this network by G. First, we take a subnet G_1 with 100 nodes from G, which is plotted in Figure 4.

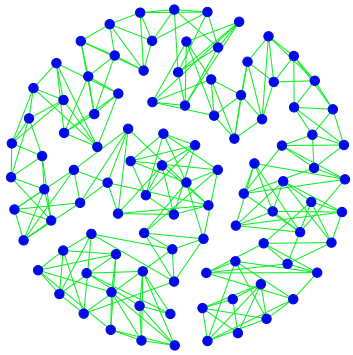

Figure 4. The subnet G_1 of G.

Example 1. *Consider the instance of the EEP model in which $G = G_1$, $T = 10$, $\beta_I = 0.2$, $\beta_P = 0.15$, $\delta = 0.1$, $w_1 = w_2 = 1$, $\overline{\gamma_I} = 0.4$, $\overline{\gamma_F} = 0.3$, and $\mathbf{E}_0 = (0.3, \cdots, 0.3)$. By solving the corresponding optimality system, we get an optimal control $\mathbf{u}^{opt}$, which is shown in Figure 5a. It is seen that either of the two components of $\mathbf{u}^{opt}$ is bang-bang, as expected by Theorem 2. Furthermore, it is seen that either of the two components of $\mathbf{u}^{opt}$ first stays at the maximum allowable rate, then abruptly drops to the zero rate, and finally stays at the zero rate.*

Let $A = \{0, 0.04, 0.08, \cdots, 0.4\}$, $B = \{0, 0.03, 0.06, \cdots, 0.3\}$. *For* $g \in A$, $h \in B$, *let* $\mathbf{u}^{g,h} = (\gamma_I^{g,h}, \gamma_F^{g,h})$ *denote the static control with* $\gamma_I^{g,h}(t) = g$, $\gamma_F^{g,h}(t) = h$, $0 \le t \le T$. *For comparative purpose, Figure 5b plots* $J(\mathbf{u})$ *for all* $\mathbf{u} \in \{\mathbf{u}^{opt}\} \bigcup \left\{\mathbf{u}^{g,h} | g \in A, h \in B\right\}$. *It is seen that* $\mathbf{u}^{opt}$ *is superior to all the static controls in terms of the energy efficiency, as expected.*

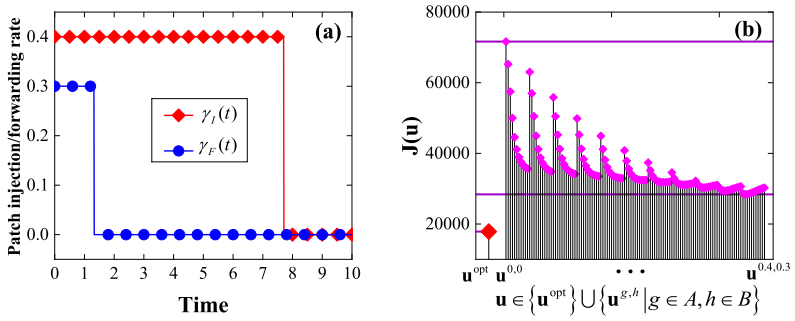

Figure 5. The experimental results in Example 1: (**a**) an optimal control, (**b**) a comparison between the optimal control and the set of static controls in terms of the energy efficiency.

Second, we take a subnet G_2 with 300 nodes from G, which is exhibited in Figure 6.

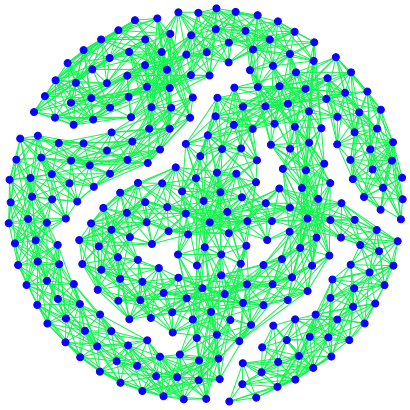

Figure 6. The subnet G_2 of G.

Example 2. *Consider the instance of the EEP model in which* $G = G_2$, $T = 10$, $\beta_I = 0.2$, $\beta_P = 0.15$, $\delta = 0.1$, $w_1 = w_2 = 1$, $\overline{\gamma_I} = 0.4$, $\overline{\gamma_F} = 0.3$, *and* $\mathbf{E}_0 = (0.3, \cdots, 0.3)$. *By solving the corresponding optimality system, we get an optimal control* $\mathbf{u}^{opt}$, *which is shown in Figure 7a. It is seen that either of the two components of* $\mathbf{u}^{opt}$ *is bang-bang, as expected by Theorem 2. Again, it is seen that either of the two components of* $\mathbf{u}^{opt}$ *first stays at the maximum allowable rate, then abruptly drops to the zero rate, and finally stays at the zero rate.*

Let $A = \{0, 0.04, 0.08, \cdots, 0.4\}$, $B = \{0, 0.03, 0.06, \cdots, 0.3\}$. *For* $g \in A$, $h \in B$, *let* $\mathbf{u}^{g,h} = (\gamma_I^{g,h}, \gamma_F^{g,h})$ *denote the static control with* $\gamma_I^{g,h}(t) = g$, $\gamma_F^{g,h}(t) = h$, $0 \le t \le T$. *For comparative purpose, Figure 7b plots* $J(\mathbf{u})$ *for all* $\mathbf{u} \in \{\mathbf{u}^{opt}\} \bigcup \left\{\mathbf{u}^{g,h} | g \in A, h \in B\right\}$. *Again, it is seen that* $\mathbf{u}^{opt}$ *outperforms all the static controls in terms of the energy efficiency, as expected.*

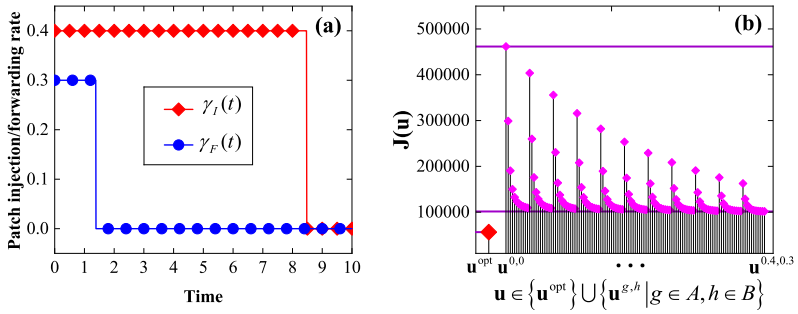

Figure 7. The experimental results in Example 2: (**a**) an optimal control, (**b**) a comparison between the optimal control and the set of static controls in terms of the energy efficiency.

Finally, we take a subnet G_3 with 500 nodes from G, which is displayed in Figure 8.

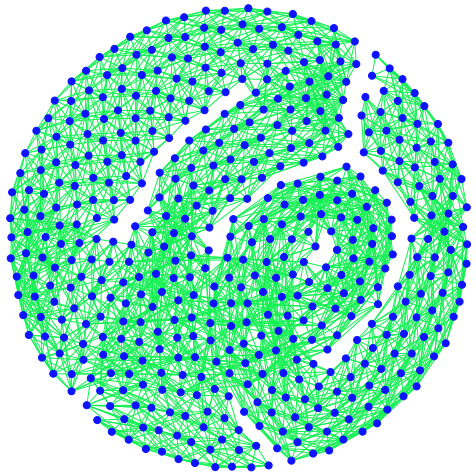

Figure 8. The subnet G_3 of G.

Example 3. *Consider the instance of the EEP model in which* $G = G_3$, $T = 10$, $\beta_I = 0.2$, $\beta_P = 0.15$, $\delta = 0.1$, $w_1 = w_2 = 1$, $\overline{\gamma_I} = 0.4$, $\overline{\gamma_F} = 0.3$, *and* $\mathbf{E}_0 = (0.3, \cdots, 0.3)$. *By solving the corresponding optimality system, we get an optimal control* $\mathbf{u}^{opt}$, *which is shown in Figure 9a. It is seen that either of the two components of* $\mathbf{u}^{opt}$ *is bang-bang, as expected by Theorem 2. Once more, it is seen that either of the two components of* $\mathbf{u}^{opt}$ *first stays at the maximum allowable rate, then abruptly drops to the zero rate, and finally stays at the zero rate.*

Let $A = \{0, 0.04, 0.08, \cdots, 0.4\}$, $B = \{0, 0.03, 0.06, \cdots, 0.3\}$. *For* $g \in A$, $h \in B$, *let* $\mathbf{u}^{g,h} = (\gamma_I^{g,h}, \gamma_F^{g,h})$ *denote the static control with* $\gamma_I^{g,h}(t) = g$, $\gamma_F^{g,h}(t) = h$, $0 \le t \le T$. *For comparative purpose, Figure 9b plots* $J(\mathbf{u})$ *for all* $\mathbf{u} \in \{\mathbf{u}^{opt}\} \bigcup \left\{\mathbf{u}^{g,h} | g \in A, h \in B\right\}$. *Also, it is seen that* $\mathbf{u}^{opt}$ *overmatches all the static controls in terms of the energy efficiency, as expected.*

From the above three examples and 100 similar examples, we conclude the following results:

(i) For each instance of the EEP model, the patch injection strategy in the optimal patching strategy obtained by solving the optimality system first attains the maximum allowable patch injection rate for a period of time, then jumps sharply to the zero rate, and finally keeps the zero rate for the remaining period of time.

(ii) For each instance of the EEP model, the patch forwarding strategy in the optimal patching strategy obtained by solving the optimality system first attains the maximum allowable patch forwarding rate for a period of time, then jumps sharply to the zero rate, and finally keeps the zero rate for the remaining period of time.

In practice, such patching strategies are easily implementable. Therefore, we recommend to WSN administrators the EEP strategies obtained in this way.

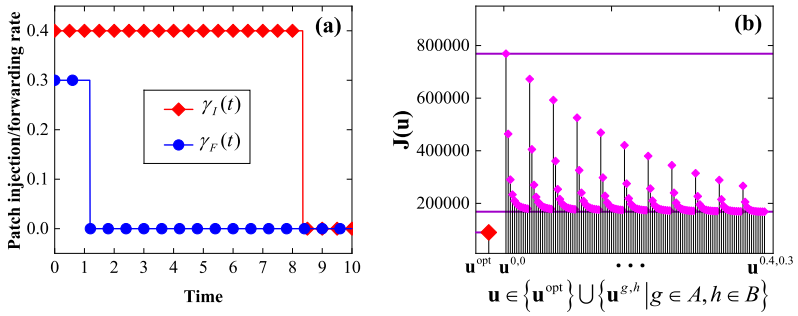

Figure 9. The experimental results in Example 3: (**a**) an optimal control, (**b**) a comparison between the optimal control and the set of static controls in terms of the energy efficiency.

5. Further Discussions

In the previous section, a method for calculating EEP strategies for WSNs was presented. In this section, we experimentally examine the effects of some factors on the optimal patching strategy obtained in this way.

5.1. The Effects of the Loss and Energy Coefficients

First, we study the effects of the loss coefficient and the energy coefficient on the optimal patching strategy, respectively.

Experiment 1. *Consider a set of instances of the EEP model in which* $G \in \{G_1, G_2, G_3\}$, $T = 10$, $\beta_I = 0.1$, $\beta_P = 0.2$, $\delta = 0.1$, $\overline{\gamma_I} = 0.4$, $\overline{\gamma_F} = 0.3$, *and* $\mathbf{E}(0) = (0.3, \cdots, 0.3)$.

(a) *Suppose* $w_2 = 1$, $w_1 \in \{0.25, 0.5, 1, 2\}$. *By solving these optimality systems, we get the respective optimal patching strategies, in which the patch injection strategies and the patch forwarding strategies are depicted in Figure 10a–c and Figure 10c–f, respectively. It is seen that with the increase of* w_1, *the jump point of either of the patch injection strategy and the patch forwarding strategy in* $\mathbf{u}^{opt}$ *moves to the right.*

(b) *Suppose* $w_1 = 1$, $w_2 \in \{0.25, 0.5, 1, 2\}$. *By solving these optimality systems, we get the respective optimal patching strategies, in which the patch injection strategies and the patch forwarding strategies are exhibited in Figure 11a–c and Figure 11c–f, respectively. It is seen that with the increase of* w_2, *the jump point of either of the patch injection strategy and the patch forwarding strategy in* $\mathbf{u}^{opt}$ *moves to the left.*

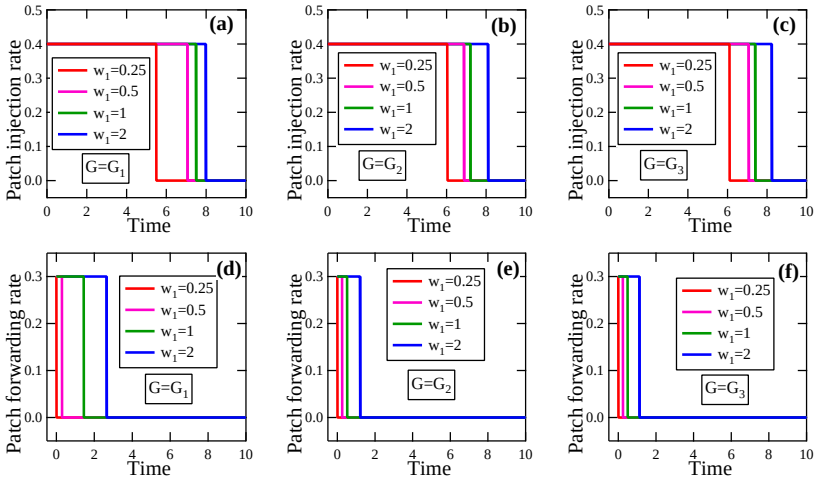

Figure 10. The experimental results in Experiment 1 about the effect of the loss coefficient on the optimal patching strategy. (**a**) Patch injection rate, $G = G_1$; (**b**) Patch injection rate, $G = G_2$; (**c**) Patch injection rate, $G = G_3$; (**d**) Patch forwarding rate, $G = G_1$; (**e**) Patch forwarding rate, $G = G_2$; (**f**) Patch forwarding rate, $G = G_3$.

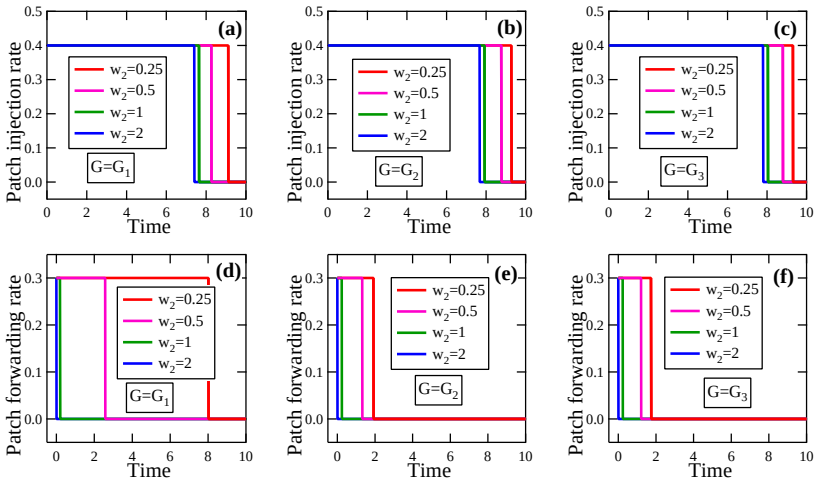

Figure 11. The experimental results in Experiment 1 about the effect of the energy coefficient on the optimal patching strategy. (**a**) Patch injection rate, $G = G_1$; (**b**) Patch injection rate, $G = G_2$; (**c**) Patch injection rate, $G = G_3$; (**d**) Patch forwarding rate, $G = G_1$; (**e**) Patch forwarding rate, $G = G_2$; (**f**) Patch forwarding rate, $G = G_3$.

From this experiment and 100 similar experiments, we conclude the following results about the EEP model:

(i) With the increase of the loss coefficient, the jump point of the patch injection strategy in the optimal patching strategy obtained by solving the optimality system moves to the right, as does the jump point of the patch forwarding strategy in the optimal patching strategy. Hence, with the increase of the loss coefficient, the energy overhead for patching must be enhanced to achieve a higher energy efficiency.

(ii) With the increase of the energy coefficient, the jump point of the patch injection strategy in the optimal patching strategy obtained by solving the optimality system moves to the left, as does the jump point of the patch forwarding strategy in the optimal patching strategy. Hence, with the increase of the energy coefficient, the energy overhead for patching must be reduced to achieve a higher energy efficiency.

5.2. The Effects of the Maximum Allowable Patch Injection and Forwarding Rates

Second, let us inspect the effects of the maximum allowable patch injection rate and the maximum allowable forwarding rates on the optimal patching strategy, respectively.

Experiment 2. *Consider a set of instances of the EEP model in which* $G \in \{G_1, G_2, G_3\}$, $T = 10$, $\beta_I = 0.1$, $\beta_P = 0.2$, $\delta = 0.15$, $w_1 = w_2 = 1$, *and* $\mathbf{E}_0 = (0.3, \cdots, 0.3)$.

(a) Suppose $\overline{\gamma_F} = 0.3$, $\overline{\gamma_I} \in \{0.1, 0.2, 0.3, 0.4\}$. *By solving these optimality systems, we get the respective optimal patching strategies, in which the patch injection strategies are plotted in Figure 12a–c, and the patch forwarding strategies are portrayed in Figure 12d–f. It is seen that with the increase of* $\overline{\gamma_I}$, *the jump point of the patch injection strategy in* $\mathbf{u}^{opt}$ *moves to the left, so does the jump point of the patch forwarding strategy in* $\mathbf{u}^{opt}$.

(b) Suppose $\overline{\gamma_I} = 0.3$, $\overline{\gamma_F} \in \{0.1, 0.2, 0.3, 0.4\}$. *By solving these optimality systems, we get the respective optimal patching strategies, in which the patch injection strategies are displayed in Figure 13a–c, and the patch forwarding strategies are depicted in Figure 13d–f. It is seen that with the increase of* $\overline{\gamma_F}$, *the jump point of the patch injection strategy in* $\mathbf{u}^{opt}$ *moves to the left, so does the jump point of the patch forwarding strategy in* $\mathbf{u}^{opt}$.

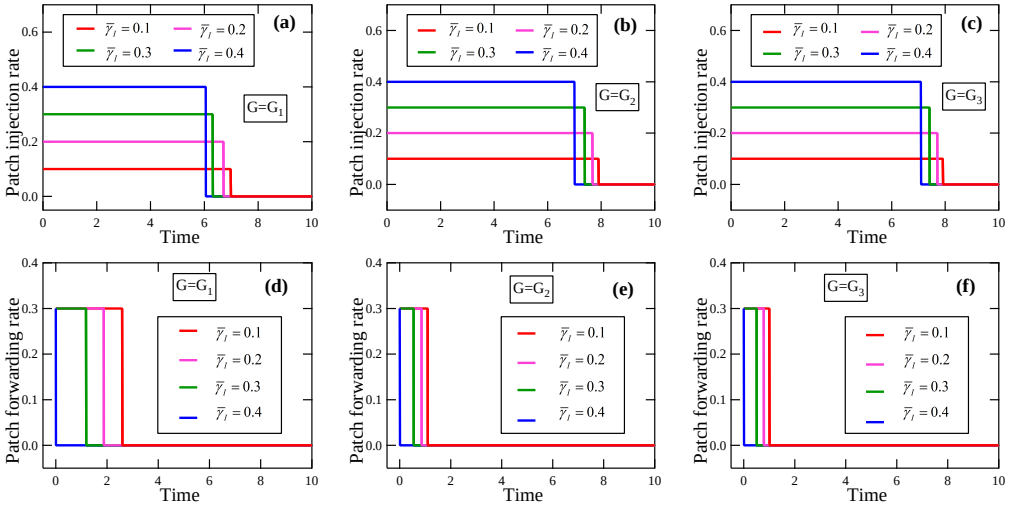

Figure 12. The experimental results in Experiment 2 about the effect of the maximum allowable patch injection rate on the optimal patching strategy. (**a**) Patch injection rate, $G = G_1$; (**b**) Patch injection rate, $G = G_2$; (**c**) Patch injection rate, $G = G_3$; (**d**) Patch forwarding rate, $G = G_1$; (**e**) Patch forwarding rate, $G = G_2$; (**f**) Patch forwarding rate, $G = G_3$.

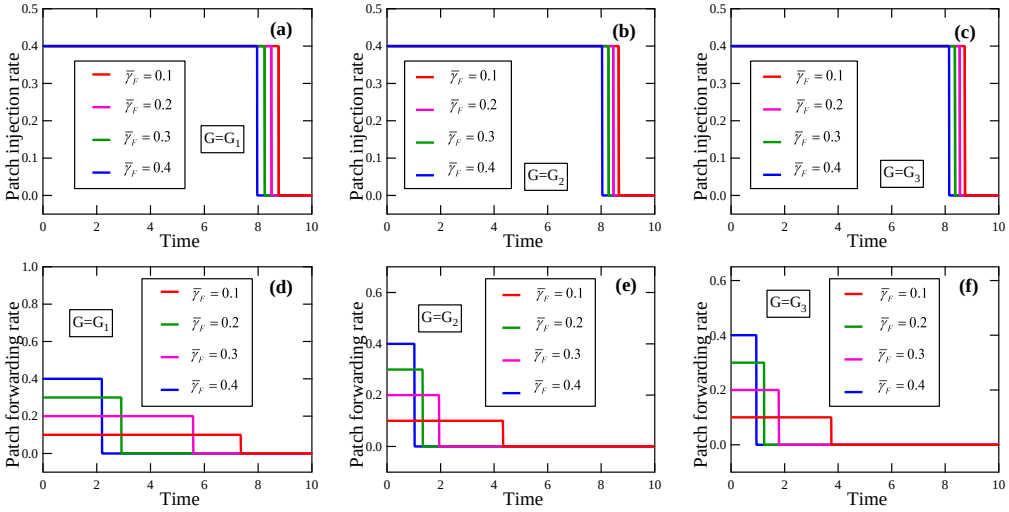

Figure 13. The experimental results in Experiment 2 about the effect of the maximum allowable patch forwarding rate on the optimal patching strategy. (**a**) Patch injection rate, $G = G_1$; (**b**) Patch injection rate, $G = G_2$; (**c**) Patch injection rate, $G = G_3$; (**d**) Patch forwarding rate, $G = G_1$; (**e**) Patch forwarding rate, $G = G_2$; (**f**) Patch forwarding rate, $G = G_3$.

From this experiment and 100 similar expects, we conclude the following results about the EEP problem:

(i) With the increase of the maximum allowable patch injection rate, the jump point of the patch injection strategy in the optimal patching strategy moves to the left, so does the jump point of the patch forwarding strategy in the optimal patching strategy. Hence, with the increase of the maximum allowable patch injection rate, the energy overhead for patching must be reduced to achieve a higher energy efficiency.

(ii) With the increase of the maximum allowable patch forwarding rate, the jump point of the patch injection strategy in the optimal patching strategy moves to the left, so does the jump point of the patch forwarding strategy in the optimal patching strategy. Hence, with the increase of the maximum allowable patch forwarding rate, the energy overhead for patching must be reduced to achieve a higher energy efficiency.

6. Concluding Remarks

This article has studied the problem of developing EEP strategies for WSNs. Based on a novel virus-patch mixed propagation model, the problem has been modeled as an optimal control problem. The solvability of this optimal control problem has been proved, and a systematic method for solving the optimal control problem has been presented. These results may help us to defending against virus attacks to WSNs in an energy-efficient way.

Still, there are some relevant problems that are worth study. The practicality of the proposed EEP strategies should be considered very carefully. This work builds on the premise that virus patches can be injected into any of the sensor nodes in the WSN. In practice, however, patches can be injected into only those nodes that are in the proximity of the base station. Therefore, this work should be extended to such scenarios. In this paper, the virus attack strategy is assumed to be static. In practice, the malefactor may intelligently change the attack strategy over time to gain a larger benefit. In this situation, it is appropriate to study the EEP problem in the framework of game theory [50–56].

Author Contributions: All authors of this article have made substantial contributions in all aspects of this work, including problem modeling, theoretical analysis, computer experiments, and writing.

Acknowledgments: The authors are grateful to the anonymous reviewers and the editor for their valuable comments and suggestions that have greatly improved the quality of the article. This work was supported by Natural Science Foundation of China (Grant No. 61572006) and Chongqing Basic Research and Front Exploration Project (Grant No. cstc2018jcyjA3093).

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

Abbreviations

The following abbreviations are used in this manuscript:

WSN	Wireless sensor network
IRS	Intrusion response system
EEP	Energy-efficient patching

References

1. Ayyash, M.; Alsbou, Y.; Anan, M. Introduction to mobile ad-hoc and vehicular networks. In *Wireless Sensor and Mobile Ad-Hoc Networks*; Benhaddou, D., Al-Fuqaha A., Eds.; Springer: New York, NY, USA; Heidelberg, Germany; Dordrecht, The Netherlands; London, UK, 2015; ISBN 9781493924677.
2. Sohraby, K.; Minoli, D.; Znati, T. *Wireless Sensor Networks: Technology, Protocols, and Applications*; John Wiley & Sons: Hoboken, NJ, USA, 2007; ISBN 9780470112755.
3. Dargie, W.; Poellabauer, C. *Fundamentals of Wireless Sensor Networks: Theory and Practice*; John Wiley & Sons: West Sussex, UK, 2010; ISBN 9780470975688.
4. Fahmy, H.M.A. *Wireless Sensor Networks: Concepts, Applications, Experimentation and Analysis*; Springer Science + Business Media: Singapore, 2016; ISBN 9789811004124.
5. Del Rey, A.M.; Batista, F.; Dios, A.Q. Malware propagation in wireless sensor networks: Global models vs. individual-based models. *Adv. Distr. Comput. Artif. Intell. J.* **2017**, *6*, 5–15.
6. Khouzani, M.H.R.; Sarkar, S. Maximum damage battery depletion attack in mobile sensor networks. *IEEE Trans. Autom. Control* **2013**, *56*, 2358–2368.
7. Hu, Y.C.; Perrig, A.; Johnson, D.B. Packet leashes: A defense against wormhole attacks in wireless networks. In Proceedings of the IEEE Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003), San Francisco, CA, USA, 30 March–3 April 2003; Volume 3, pp. 1976–1986.
8. Karlof, C.; Wagner, D. Secure routing in wireless sensor networks: Attacks and countermeasures. *Ad Hoc Netw.* **2003**, *1*, 293–315.
9. Newsome, J.; Shi, E.; Song, D.; Perrig, A. The Sybil attack in sensor networks: Analysis & defenses. In Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks, Berkeley, CA, USA, 26–27 April 2004; pp. 259–268.

10. Wang, Y.; Attebury, G.; Ramamurthy, B. A survey of security issues in wireless sensor networks. *IEEE Commun. Surv. Tutor.* **2006**, *8*, 2–23.
11. Szor, P. *The Art of Computer Virus Research*; Pearson Education, Inc.: Upper Saddle River, NJ, USA, 2005; 0321304543.
12. Haghighi, M.S.; Wen, S.; Xiang, Y.; Quinn, B.; Zhou, W. On the race of worms and patches: Modeling the spread of information in wireless sensor networks. *IEEE Trans. Inf. Forensic Secur.* **2016**, *11*, 2854–2865.
13. Wang, Q.; Zhu, Y.; Cheng, L. Reprogramming wireless sensor networks: Challenges and approaches. *IEEE Netw.* **2006**, *20*, 48–55.
14. Kulkarni, S.; Wang, L. Energy-efficient multihop reprogramming for sensor networks. *ACM Trans. Sens. Netw.* **2009**, *5*, 16.
15. Gao, Y.; Chen, C.; Liu, X.; Bu, J.; Dong, W.; Xu, X. Reprogramming over low power link layer in wireless sensor networks. In Proceedings of the IEEE 10th International Conference on Mobile Ad-Hoc and Sensor Systems, Hangzhou, China, 14–16 October 2013; pp. 461–469.
16. Grover, J.; Rani, R. Probabilistic density based adaptive clustering scheme to improve network survivability in WSN. In Proceedings of the Fifth International Conference on Computing, Communications and Networking Technologies, Hefei, China, 11–13 July 2014; pp. 1–7.
17. Grover, J. Wireless Sensor network in railway signalling system. In Proceedings of the Fifth International Conference on Communication Systems and Network Technologies, Gwalior, India, 4–6 April 2015; pp. 308–313.
18. Yi, X.; Bouguettaya, A.; Georgakopoulos, D.; Song, A.; Willemson, J. Privacy protection for wireless medical sensor data. *IEEE Trans. Dependable Secur. Comput.* **2016**, *13*, 369–380.
19. Donald, E.K. *Optimal Control Theory: An Introduction*; Dover Publications, Inc.: Mineola, NY, USA, 2012; ISBN 9780486135076.
20. Liberzon, D. *Calculus of Variations and Optimal Control Theory: A Concise Introduction*; Princeton University Press: Princeton, NJ, USA; Oxfordshire, UK, 2012; ISBN 9781400842643.
21. Zhang, T.; Yang, L.X.; Yang, X.; Wu, Y.; Tang, Y.Y. Dynamic malware containment under an epidemic model with alert. *Phys. A* **2017**, *470*, 249–260.
22. Li, P.; Yang, X.; Wu, Y.; He, W.; Zhao, P. Discount pricing in word-of-mouth marketing: An optimal control approach. *Phys. A* **2018**, *505*, 512–522.
23. Li, P.; Yang, X.; Xiong, Q.; Wen, J.; Tang, Y.Y. Defending against the advanced persistent threat: An optimal control approach. *Secur. Commun. Netw.* **2018**, *2018*, 2975376.
24. Syed, K.A.; Hayder, R. Using signal processing techniques to model worm propagation over wireless sensor networks. *IEEE Signal Process. Mag.* **2006**, *23*, 164–169.
25. Tang, S. Analysis of virus spread in wireless sensor networks: An epidemic model. In Proceedings of the 7th International Workshop on Design of Reliable Communication Networks, Washington, DC, USA, 25–28 October 2009; pp. 86–91.
26. Wang, X.; Li, Q.; Li, Y. EiSIRS: A formal model to analyze the dynamics of worm propagation in wireless sensor networks. *J. Comb. Optim.* **2010**, *20*, 47–62.
27. Tang, S. A modified epidemic model for virus spread control in wireless sensor networks. In Proceedings of the IEEE Global Telecommunications Conference–GLOBECOM, Kathmandu, Nepal, 5–9 December 2011; pp. 1–5.
28. Tang, S.; Li, W. An epidemic model with adaptive virus spread control for wireless sensor networks. *Int. J. Sec. Netw.* **2011**, *6*, 201–211.
29. Feng, L.; Song, L.; Zhao, Q.; Wang, H. Modeling and stability analysis of worm propagation in wireless sensor network. *Math. Probl. Eng.* **2015**, *2015*, 129598.
30. Wang, T.; Wu, Q.; Wen, S.; Cai, Y.; Cai, H.; Chen, Y.; Wang, B. Propagation modeling and defending of a mobile sensor worm in wireless sensor and actuator networks. *Sensors* **2017**, *17*, 139.
31. Singh, A.; Awasthi, A.K.; Singha, K.; Srivastava, P.K. Modeling and analysis of worm propagation in wireless sensor networks. *Wirel. Pers. Commun.* **2018**, *98*, 2535–2551.
32. Van Mieghem, P.; Omic, J.S.; Kooij, R.E. Virus spread in networks. *IEEE-ACM Trans. Netw.* **2009**, *17*, 1–14.
33. Van Mieghem, P. The N-Intertwined SIS epidemic network model. *Computing* **2009**, *93*, 147–169.
34. Sahneh, F.D.; Chowdhury, F.N.; Scoglio, C.M. On the existence of a threshold for preventive behavioral responses to suppress epidemic spreading. *Sci. Rep.* **2012**, *2*, 623.

35. Xu, S.; Lu, W.; Xu, L. Push-and pull-based epidemic spreading in networks: Thresholds and deeper insights. *ACM Trans. Auton. Adapt. Syst.* **2012**, *7*, 32.
36. Xu, S.; Lu, W.; Xu, L.; Zhan, Z. Adaptive epidemic dynamics in networks: Thresholds and control. *ACM Trans. Auton. Adapt. Syst.* **2014**, *8*, 19.
37. Yang, L.X.; Draief, M.; Yang, X. The impact of the network topology on the viral prevalence: A node-based approach. *PLOS ONE* **2015**, *10*, e0134507.
38. Yang, L.X.; Draief, M.; Yang, X. Heterogeneous virus propagation in networks: A theoretical study. *Math. Meth. Appl. Sci.* **2017**, *40*, 1396–1413.
39. Yang, L.X.; Yang, X.; Wu, Y. The impact of patch forwarding on the prevalence of computer virus. *Appl. Math. Model.* **2017**, *43*, 110–125.
40. Yang, L.X.; Yang, X.; Tang, Y.Y. A bi-virus competing spreading model with generic infection rates. *IEEE Trans. Netw. Sci. Eng.* **2018**, *5*, 2–13.
41. Yang, L.X.; Li, P.; Li, X.; Wu, Y.; Tang, Y.Y. On the competition of two conflicting messages. *Nonlinear Dyn.* **2018**, *91*, 1853–1869.
42. Yang, L.X.; Zhang, T.; Yang, X.; Wu, Y.; Tang, Y.Y. Effectiveness analysis of a mixed rumor-quelling strategy. *J. Frankl. Inst.-Eng. Appl. Math.* **2018**, *355*, 8079–8105.
43. Xu, S.; Lu, W.; Li, H. A stochastic model of active cyber defense dynamics. *Internet Math.* **2015**, *11*, 28–75.
44. Yang, L.X.; Li, P.; Yang, X.; Tang, Y.Y. Security evaluation of the cyber networks under advanced persistent threats. *IEEE Access* **2017**, *5*, 20111–20123.
45. Zheng, R.; Lu, W.; Xu, S. Preventive and reactive cyber defense dynamics is globally stable. *IEEE Trans. Netw. Sci. Eng.* **2017**, doi: 10.1109/TNSE.2017.2734904.
46. Stewart, W.J. *Probability, Markov Chains, Queues, and Simulation: The Mathematical Basis of Performance Modeling*; Princeton University Press: Princeton, NJ, USA, 2009; ISBN 9780691140629.
47. Stein, E.M.; Shakarchi, R. *Real Analysis: Measure Theory, Integration, & Hilbert Spaces*; Princeton University Press: Princeton, NJ, USA; Oxfordshire, UK, 2005; ISBN 9781400835560.
48. Robinson, R.C. *An Introduction to Dynamical Systems: Continuous and Discrete*; American Mathematical Society: Providence, RI, USA, 2004; ISBN 9780821891353.
49. Rossi R.A.; Ahmed N.K. The Network Data Repository with Interactive Graph Analytics and Visualization. In Proceedings of the Twenty-Ninth AAAI Conference on Artificial Intelligence, Austin, TX, USA, 25–30 January 2015. Available online: http://networkrepository.com (accessed on 10 January 2019).
50. Shen, S.; Yue, G.; Cao, Q.; Yu, F. A survey of game theory in wireless sensor networks security. *J. Netw.* **2011**, *6*, 521–532.
51. Alpcan, T.; Basar, T. *Network Security: A Decision and Game-Theoretic Approach*; Cambridge University Press: Cambridge, UK; New York, NY, USA; Melbourne, Australia; Madrid, Spain; Cape Town, South Africa; Singapore; Sao Paulo, Brazil; Delhi, India; Dubai, United Arab Emirates; Tokyo, Japan; Mexico City, Mexico, 2011; ISBN 9781139491891.
52. Han, Z. *Game Theory in Wireless and Communication Networks: Theory, Models, and Applications*; Cambridge University Press: Cambridge, UK; New York, NY, USA; Melbourne, Australia; Madrid, Spain; Cape Town, South Africa; Singapore; Sao Paulo, Brazil; Delhi, India; Dubai, United Arab Emirates; Tokyo, Japan; Mexico City, Mexico, 2012; ISBN 9780521196963.
53. Abdalzaher, M.S.; Seddik, K.; Elsabrouty, M.; Muta, O.; Furukawa, H.; Abdel-Rahman, A. Game theory meets wireless sensor networks security requirements and threats mitigation: A survey. *Sensors* **2016**, *16*, 1003.
54. Yang, L.X.; Li, P.; Yang, X.; Xiang Y; Zhou W. A differential game approach to patch injection. *IEEE Access* **2018**, *6*, 58924–58936.
55. Yang, L.X.; Li, P.; Yang, X.; Tang Y.Y. A risk management approach to defending against the advanced persistent threat. *IEEE Trans. Dependable Secur. Comput.* **2018**, doi: 10.1109/TDSC.2018.2858786.
56. Yang, L.X.; Li, P.; Zhang, Y; Yang, X.; Zhou W. Effective repair strategy against advanced persistent threat: A differential game approach. *IEEE Trans. Inf. Forensic Secur.* **2018**, doi: 10.1109/TIFS.2018.2885251.