Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 3183699, 12 pages
https://doi.org/10.1155/2022/3183699

Research Article

Dynamic Resource Allocation in an Adversarial Urban IoBT Environment

Weiwei Wu and Di Lin

University of Electronic Science and Technology of China, China

Correspondence should be addressed to Di Lin; lindi@uestc.edu.cn

Received 8 August 2022; Revised 19 September 2022; Accepted 23 September 2022; Published 11 October 2022

Academic Editor: Mingqian Liu

The advances of the Internet of Battlefield Things (IoBT) would improve the flexibility and efficiency of military operations. Without an effective dynamic adversarial mechanism, soldier devices might malfunction, and machine intelligence technologies could hardly support military operations on a battlefield. In this paper, we propose a game theoretical model considering the adversarial and dynamic nature of the urban IoBT environment. Our algorithm is designed to optimize the whole network's efficiency with the premise that both the attacking and defending parties can maximize their benefit. Meanwhile, we also attempt to consider the interactive effects of channel fading by using a Nakagami distribution based Markov process. The experimental results show that considering the impact of the adversarial and dynamic nature of urban IoBT, our proposed algorithm can improve network performance by 30%-50%.

1. Introduction

In the Internet of Things (IoT) applications, a remarkable amount of data has been produced by intelligent mobile devices such as sensors, mobile computers, and drones [1–7]. As a potential technology, IoT has been applied and promoted in various industrial domains. For example, in an application of Internet of Medical Things (IoMT), an intelligent hospital collects information through sensors and uploads it to a doctor's device for real-time monitoring. In case of emergency, the patient's medical examination reports can timely be transferred to remote experts, thereby reducing the risk of accidental death [8–10].

Unlike the consistent network environment in a regular IoT, e.g., IoMT, the Internet of Battlefield Things (IoBT) has highly changeable and adversarial characteristics in nature [11, 12]. The overall vision of an IoBT is to minimize soldier mortality by collecting battlefield information through intelligent devices and by enabling human decision-making with intelligent means [13]. However, in an extreme battlefield scenario, physical devices and channels are vulnerable to various adversarial attacks [11]. For example, high-power electromagnetic weapon attacks might lead to the physical destruction of base stations or end devices for network communication [14]. Thus, the dynamic adaptability for a highly adversarial environment is the most dominant feature in IoBT, so it is crucial to establish a dynamic mechanism to optimize the entire network's utility [11, 13, 15].

In the special interest of mitigating the adversarial problems in urban IoBT environments, we propose a dynamic adversarial mechanism under a Stackelberg game theoretic framework in consideration of channel fading effects. Despite a bunch of literature on the optimization of IoBT networks [16–18], most existing algorithms may not work well in urban adversarial scenarios, which face the challenges of adversarial battlefield environment and changeable fading channels. The main contributions of our work are summarized as follows:

(1) We address the architecture of communication networks in adversarial urban scenarios, and propose a network utility optimization problem in consideration of each player's benefit on a battlefield. To

Table 1: Description table for key notations.

Key notations	Descriptions
$F(\alpha)$	Nakagami distribution of channel fading
$\Gamma(.)$	Gamma function
ϕ, m	Parameters of a Nakagami distribution
h_{t_i}	Channel fading characteristics at time slot t_i
$I_m(.)$	The m-order Bessel function;
ρ	Correlation between channels
I_0	Zero-order Bessel function
f_d	Doppler frequency
μ	Angle of arrival
λ	A parameter of bandwidth
p_{ij}	Transition probability
U_k^a	Overall utility of attacker k
L_i^d	Decrease of channel capacity of defender i
L_k^a	Cost of attacker k to degrade the network performance
P_i^d	Transmission power defender i
h_{mi}^k	Interferences of defender i at kth stage
δ	Power of noise
M	Number of attackers
N	Number of defenders
P_k^a	Transmission power of attacker k
α	Cost per unit power consumption by an attacker
C_i^d	Channel capacity of defender i after being attacked
$\widehat{L_i^d}$	Cost of defender i to maintain the capacity of channel
η	Cost per unit power consumption by a defender

our knowledge, there are very few studies on network optimization in a secure IoU network in an adversarial scenario

(2) We establish a Stackelberg game theoretic model to characterize the dynamic adversarial process between both parties of a battlefield in an IoBT. The existence of Nash equilibrium is proofed in such a game, and a closed-form mathematical expression of equilibrium is presented when an inequality constraint holds

(3) We also show the existence of Nash equilibrium in the proposed Stackelberg game when an inequality constraint does not hold, and present a numerical algorithm to compute the equilibrium

In Section 2, we review the literature on adversarial cases in IoBT. Following this, Section 3 demonstrates a system model of an adversarial game with both defenders and attackers. Based on the system model, we describe the optimal solutions in Section 4. Section 5 shows the simulation results. The conclusion is finally discussed in Section 6.

2. Related Work

Military missions depend on real-time information processing and data analysis for making accurate decisions in IoBT networks. However, any connectivity problems might result in inaccurate decisions on military operations, so the connectivity problem has triggered much academic debate. For example, in [15], a mechanism on connectivity reestablishment at the presence of dumb nodes that cannot transmit the data to the neighborhood nodes is proposed, and it can enable reestablishment of connectivity between dumb nodes and the centralized node. In [17], a fusion-based defense scheme is employed for defending the attacks at the network level. By characterizing the attack and defense as a zero-sum game, the proposed method can effectively improve network stability even with a fragile network structure. The above-mentioned studies merely consider all sensors/devices with the same type and capabilities. To remedy this issue, in consideration of heterogeneous characteristics of the devices in a network, Abuzainab and Saad use a multistage Stackelberg game to mitigate the IoBT connectivity problem by either activating sleeping nodes or by changing the roles of current nodes [13].

For adversarial IoBT networks, security attacks can be categorized into two types including disruption ones and manipulation ones. While disruption attacks try to paralyze IoT networks by launching physical destructions or jamming the entire system, i.e., denial of service attacks (DDoS) and manipulation attacks seek to control a few nodes in network to inject false information. The attacks mentioned in the previous paragraph are mostly relevant to disruption ones. However, other literature also considers the impact of the action that injects misinformation or imposes human interventions on IoBT nodes. In [18], the misinformation attack has been countered by determining the optimal probability of accepting the information. Similarly, building on a psychological game theory, the authors focus on how the misinformation from human psychological interventions influences game-theoretic decision making on the battlefield [19].

Most previous studies on IoBT have paid particular attention to connectivity problems in which the researchers focus on optimizing the network by measuring the number of connected nodes from the network layer. However, few studies have attempted to use a specific indicator such as bit error rate (BER) or power to optimize network resources from the physical layer. Building on the work [20], a power control based connectivity reconstruction game can reduce energy consumption while maintaining the performance of localization. That is, the number of connected nodes is a fairly broad indicator that can hardly reflect the quality of services (QoS) in an IoBT network. Even if all nodes in the network are successfully connected, the quality of communication might still be unsatisfactory. Thus, it is necessary to use a specific indicator such as power to measure the QoS of IoBT. Furthermore, the current relevant studies primarily

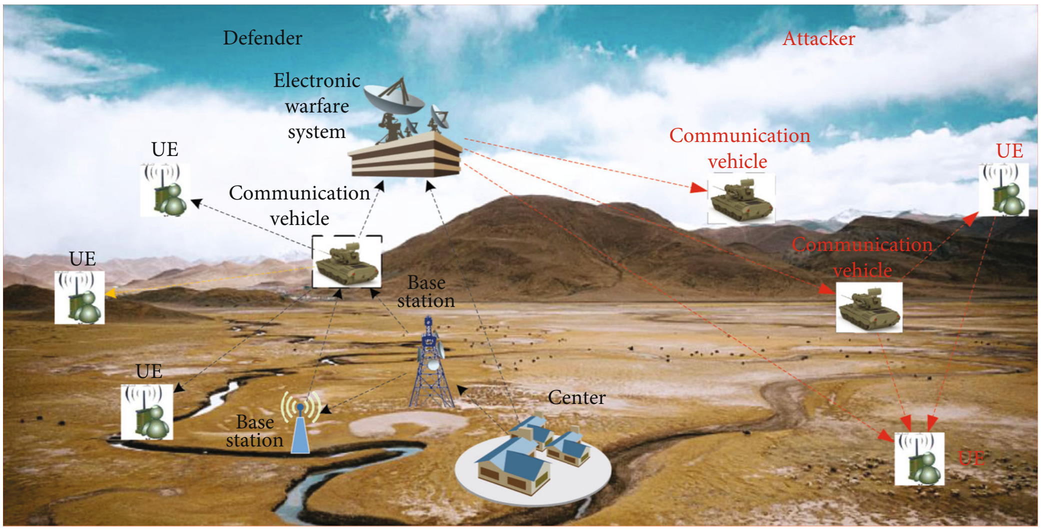


Figure 1: System architecture in an urban IoBT.

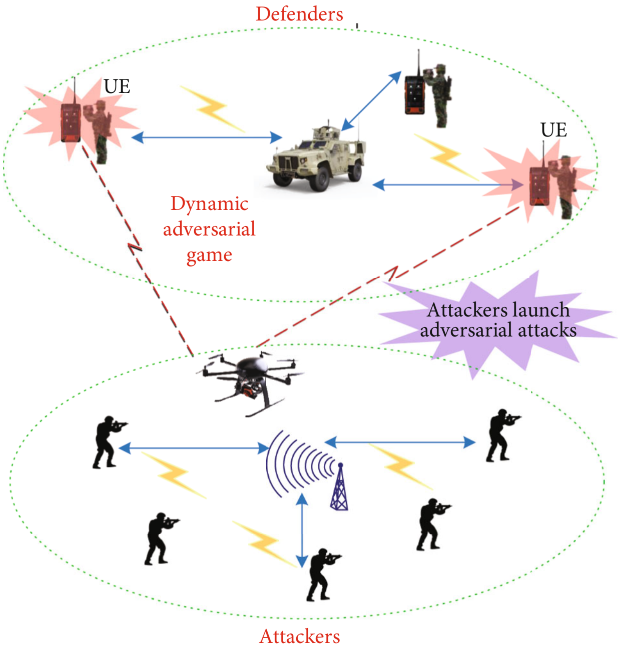


Figure 2: An adversarial game model in the IoBT.

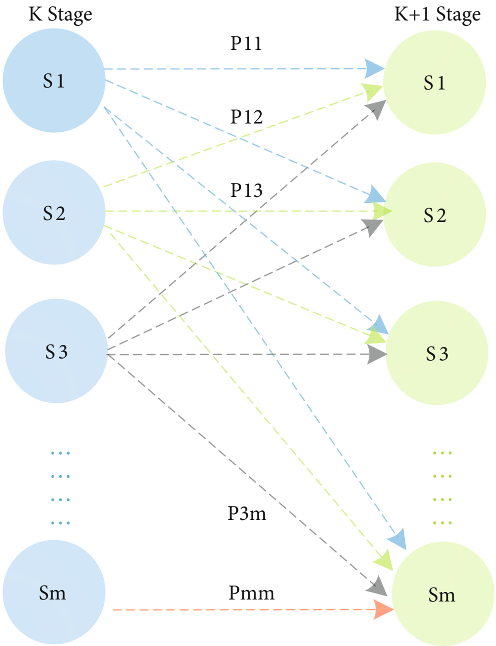


Figure 3: Dynamic channel fading in the IoBT.

focus on building a dynamic scheme to adjust the focal network's topology, but they have not taken into account the dynamic adjustment to channel changes.

3. System Model

As discussed in the previous section, the two factors that dynamic adjustment to the fading channels and reasonable allocation for network resources are fairly important in the urban IoBT environment. To familiarize readers, in the following, we firstly discuss a model that reflects the effects of channel fading in the urban IoBT environment. By using Stackelberg game theory, we then propose a dynamic channel-based adversarial game model that reflects the adversarial process between both parties of a battlefield. The strategies of the network players depend on those of their competitors. To be specific, the attackers in the network actively deploy strategies, while the defenders make passive adjustments based on the attackers™ strategies. This framework can match the adversarial situation in an IoBT well. The key notations in Table 1 will be used in the following sections.

3.1. Channel Fading Models. By facilitating an effective decision making process, intelligent tools used in the urban IoBT scenarios may include on-board servers, sensors, mobile computers, and drones. In cities, vehicle speed is limited to less than 60 meters per minute, and intervehicle distance is from a few meters to approximately 100 meters. As shown

```
Step 1: Initialize the relevant parameters: $B$ that represents bandwidth, $h_{mi}$ that represents a set for interferences at the first round ($h_{mi}$ would dynamically change according to the Markov transition probability matrix), $\delta$ that represents the power of noise, and $P_m$ that represents a reasonable maximum power that the attackers can accept. Additionally, set $U_a = U_d = P_a = 0$.
Step 2: By using a searching algorithm, the maximum value of $U_a$ can be found. The maximum $U_a$ corresponds to the optimal solution of the attacker's power $P_a^*$.
  Let $X = 0$: $\Delta P$: $P_m$, $\Delta P = \lceil P_m/N \rceil$
  For $i = 1$: $\Delta P$
    Set $P_a = X(i)$
    Compute $U_a$ based on the function (18)
    If $U_a(P_a) > U_a$
        Update $U_a^* = U_a(P_a)$
        Set $P_a^* = P_a$
Step 3: Building on the above steps, the algorithm searches the optimal solution within the closed interval range$[0, P_m]$ to determine the game equilibrium $P_a^*$ and the corresponding utilities of the attackers and defenders $U_a^*$, $U_d^*$.
```

Algorithm 1: Computing algorithm for achieving Stackelberg game equilibrium.

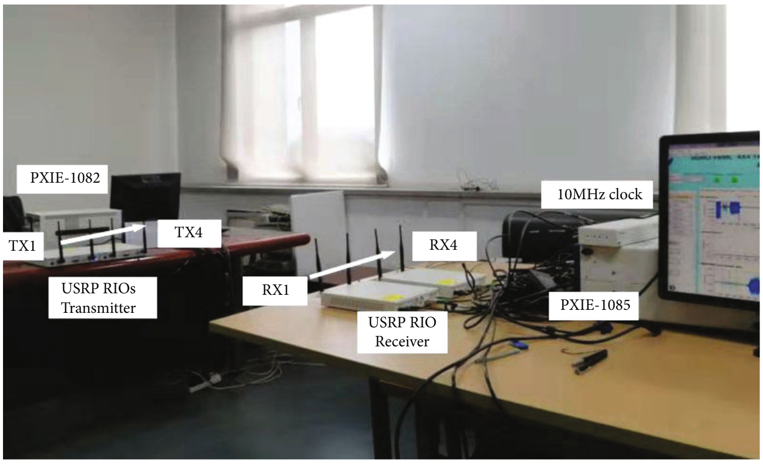


Figure 4: Experimental settings for data collection in the simulation.

in Figure 1, two sides including defenders and attackers are involved in an IoBT network. The center on the defending side plays an essential role in monitoring and decision making. An electronic defending system could facilitate communication tasks between user ends (UEs) and the centralized node, as well as monitoring tasks. The collected information and data would be forwarded to the center for further analysis and actions.

By considering both the urban IoBT environment and widely used channel models, in [21–23], the researchers conclude that the channel fading in all line of sight and nonline of sight cases can be modeled as Nakagami distributions with particular parameters. The Nakagami distribution can be used to capture the changes of signal amplitude after channel fading in an urban IoT scenario. The channel characteristics of Nakagami are determined by parameters ϕ and m, and thus the generalized Nakagami distribution of channel fading α can be shown as

$$F(\alpha) = \frac{2m^m \alpha^{2m-1}}{\phi^m \Gamma(m)}, \tag{1}$$

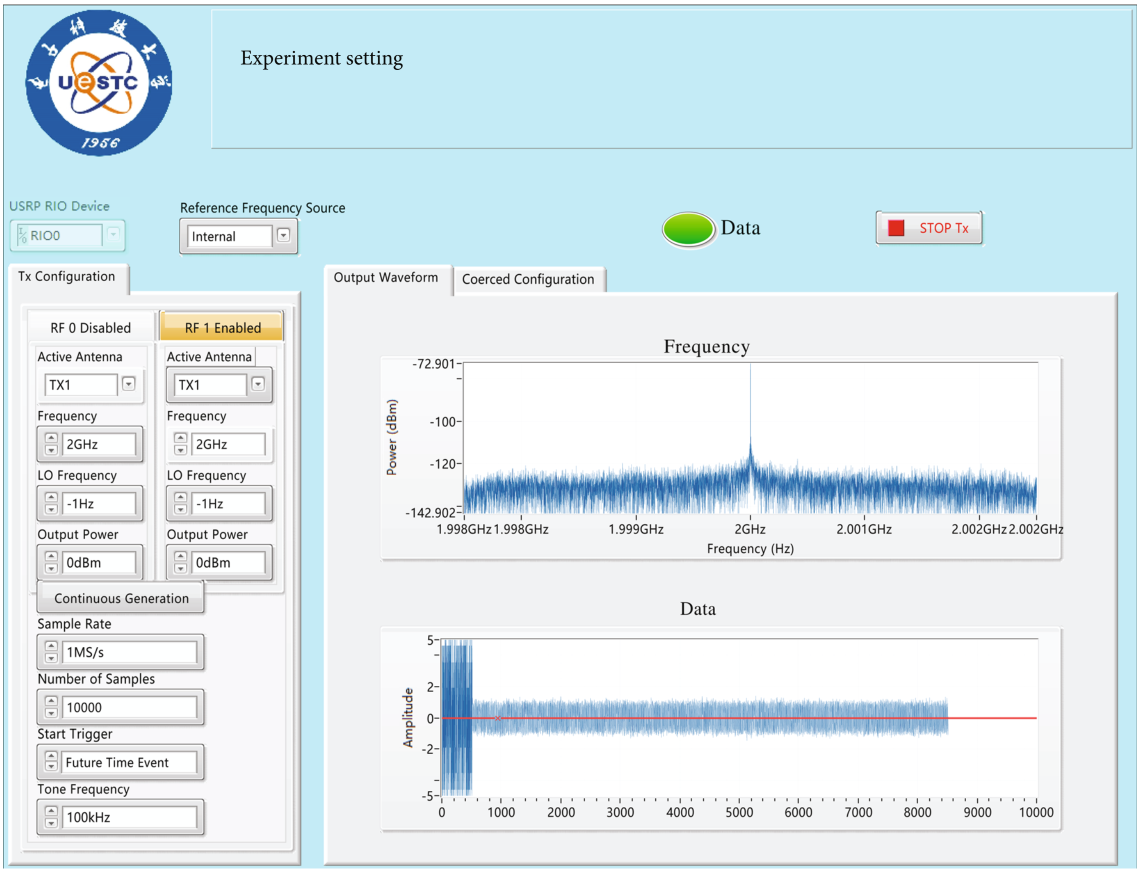
where $\Gamma(.)$ is a gamma function and ϕ, m are two determinant parameters of a Nakagami distribution.

Represent h_{t_1} and h_{t_2} as the channel fading characteristics at the time slots of t_1 and t_2, respectively. Building on the generalized Nakagami channel model Formula (1), we can denote the joint probability density function as [24]:

$$F\left(h_{t_1}, h_{t_2}\right) = \frac{4\left(h_{t_1} h_{t_2}\right)^m}{(1-\rho)\Gamma(m)\rho^{m-1/2}} \left(\frac{m}{\phi}\right)^{m+1} \times I_{m-1}\left\{\frac{2m\sqrt{\rho} h_{t_1} h_{t_2}}{(1-\rho)\phi}\right\} \times \exp\left\{-\frac{m\left(h_{t_1}^2 + h_{t_2}^2\right)}{1-\rho}\right\}, \tag{2}$$

where $I_m(.)$ denotes the m-order Bessel function, ϕ and m denote the parameters of a Nakagami fading channel (1), and ρ denotes the correlation between channels [24]:

$$\rho(\tau) = \frac{I_0\left(\sqrt{\lambda^2 - 2\pi f_d(\tau)^2 + j4\pi\lambda f_d(\tau) \cos \mu}\right)}{I_0(\lambda)}, \tag{3}$$



Experiment setting

USRP RIO Device: RIO0

Reference Frequency Source: Internal

Tx Configuration

RF 0 Disabled	RF 1 Enabled
Active Antenna: TX1	Active Antenna: TX1
Frequency: 2GHz	Frequency: 2GHz
LO Frequency: -1Hz	LO Frequency: -1Hz
Output Power: 0dBm	Output Power: 0dBm

Continuous Generation

Sample Rate: 1MS/s

Number of Samples: 10000

Start Trigger: Future Time Event

Tone Frequency: 100kHz

Figure 5: User interface of experimental setting.

where I_0 denotes zero-order Bessel function, f_d denotes the Doppler frequency, μ denotes the angle of arrival, and λ denotes a parameter of bandwidth.

In the following, we consider M channel states, i.e., $S_i (i = 1, 2 \cdots M)$. S_i is dependent on the values of channel fading h_k at time slot k. Let $h_k \in (S^t_{i-1}, S^t_i)$, and let h_k and h_{k+1} denote the channel fading at the kth and $(k+1)$th time slots, respectively. Thus, the transition probability p_{ij} can be characterized as

$$\begin{aligned} p_{\mathrm{ij}} &= \Pr\left\{ h_{k+1} \in \left(S^k_{i-1}, S^k_i\right) \middle| h_k \in \left(S^t_{j-1}, S^t_j\right) \right\} \\ &= \frac{\Pr\left\{ h_{k+1} \in \left(S^k_{i-1}, S^k_i\right), h_k \in \left(S^k_{j-1}, S^k_j\right) \right\}}{\Pr\left\{ h_k \in \left(S^k_{j-1}, S^k_j\right) \right\}} \\ &= \frac{\int_{S^k_{i-1}}^{S^k_i} \int_{S^k_{j-1}}^{S^k_j} F\left(h_{t_1}, h_{t_2}\right) \mathrm{dh}_{t_1} \mathrm{dh}_{t_2}}{\int_0^\infty \int_{S^t_{j-1}}^{S^t_j} F\left(h_{t_1}, h_{t_2}\right) \mathrm{dh}_{t_1} \mathrm{dh}_{t_2}}. \end{aligned} \tag{4}$$

By submitting (2) into (4), we can achieve the probability of a transition between channel states and simulate the future channel states based on previous information. We denote Equation (4) as the probability of one-step transition between channel states, and build up the matrix of probabilities as one-step transition matrix. Mathematically, we can denote the one-step transition matrix as

$$\begin{bmatrix} \mathrm{p}_{11} & \mathrm{p}_{12} & \cdots & \mathrm{p}_{1m} \\ \mathrm{p}_{21} & \mathrm{p}_{22} & \cdots & \mathrm{p}_{2m} \\ \vdots & \vdots & \cdots & \vdots \\ \vdots & \vdots & \cdots & \vdots \\ \mathrm{p}_{m1} & \mathrm{p}_{22} & \cdots & \mathrm{p}_{\mathrm{mm}} \end{bmatrix}. \tag{5}$$

Based on the Markov properties of Nakagami fading channels [25], we can compute the N-step transition matrix as P^N. Actually, we can estimate one-step transition probability by statistically averaging the data of observations in a long period.

3.2. Adversarial Game Model. As shown in Figure 2, attackers might launch adversarial attacks on defenders by using high power electromagnetic weapons. The performance of base station or edge server would degrade or even corrupt in the presence of attackers, so computing tasks need to be processed from the cloud server to heterogeneous edge servers or end devices. Thus, it is essential to build a dynamic algorithm to optimize insufficient network resources in such a dynamic, adversarial, and unpredictable scenario. The adversarial process between defenders and

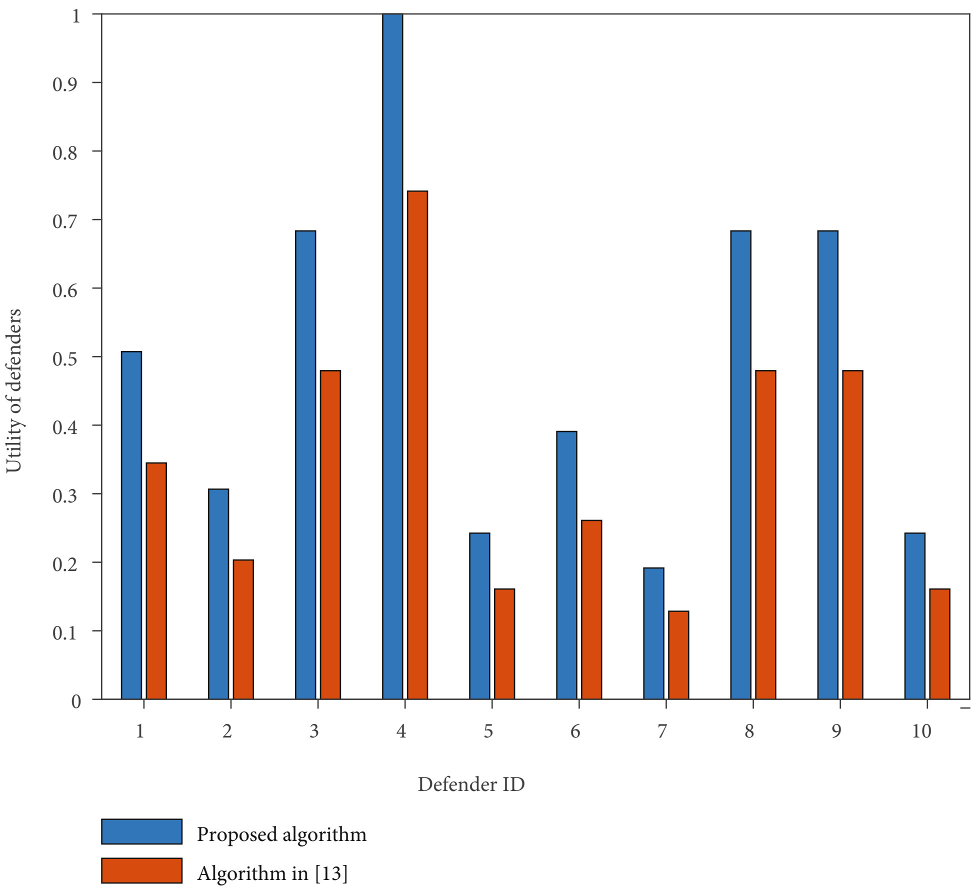


Figure 6: Individual utility of defenders (proposed vs. traditional algorithm [12]).

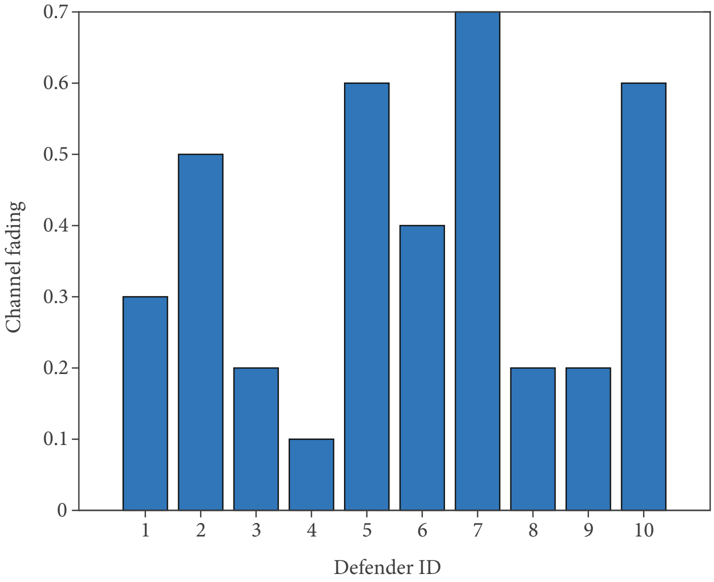


Figure 7: Individual channel fading of defenders.

attackers can be regarded as a classic game theory problem. By ensuring the optimization of the overall network resources, the Stackelberg game theory is proposed. An attacker actively deploys military strategy, while a defender makes passive adjustments based on the attacker's strategy, assuming that both parties are aware of the other's strategy.

At each stage of a game, attackers and defenders have their respective strategy sets. In the following, we will

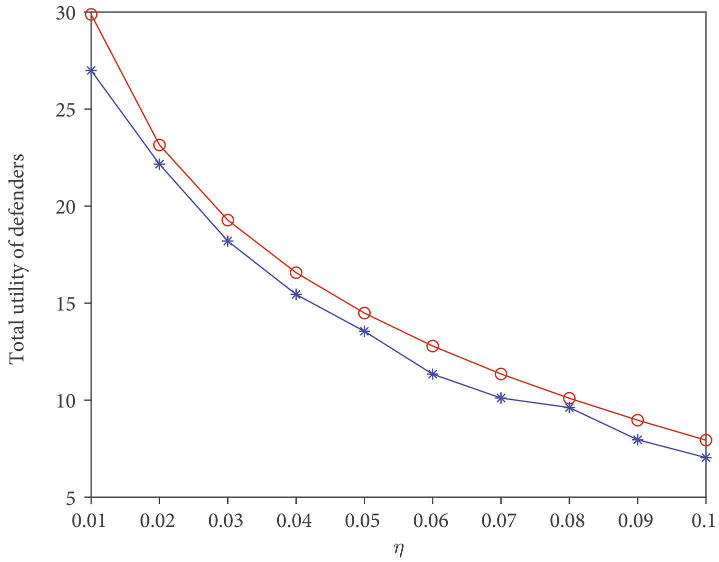


Figure 8: Total utility of defenders with different η (proposed vs. traditional algorithm [12]).

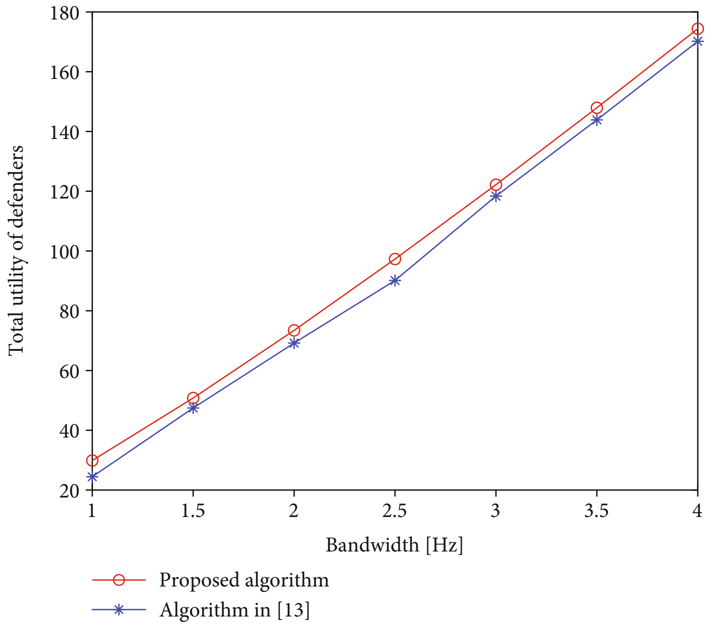


Figure 9: Total utility of defenders with different bandwidth (proposed vs. traditional algorithm [12].

consider the utility function from the attacker or the defender perspective. Firstly, the attackers' strategies primarily depend on two factors, including the decrease of network performance and the cost of interference to defenders. Therefore, the overall utility of attacker k, i.e., U_k^a can be expressed as

$$U_k^a = \sum_{i=1}^{N} L_i^d - L_k^a, \quad (6)$$

where L_i^d represents the decrease of channel capacity of defender i. L_k^a represents the cost of attacker k to degrade the network performance. N represents the number of defenders in a network.

Building on the channel fading model in the previous section, the transfer of channel fading h_{mi}^k between stage k and stage $k+1$ follows a transfer matrix, shown in Equation (5). The dynamic channel fading h_{mi}^k is illustrated in Figure 3. S_1, $S_2 \ldots S_M$ refer to M states of channel fading.

Thus, L_i^d can be denoted as

$$L_i^d = B\log_2\left(1+\frac{P_i^d}{\delta}\right) - B\log_2\left(1+\frac{P_i^d}{\sum_{k=1}^{M} P_k^a h_{\mathrm{mi}}^k + \delta}\right), \quad (7)$$

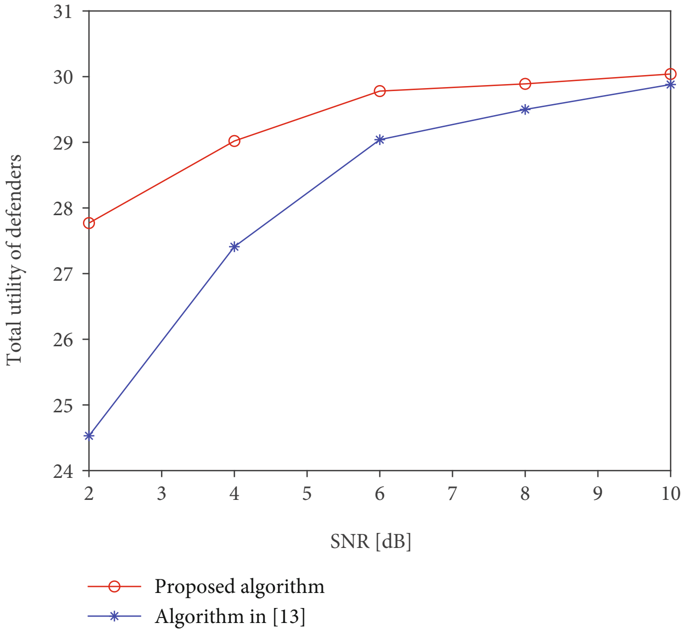


FIGURE 10: Total utility of defenders with different SNRs (proposed vs. traditional algorithm [12].

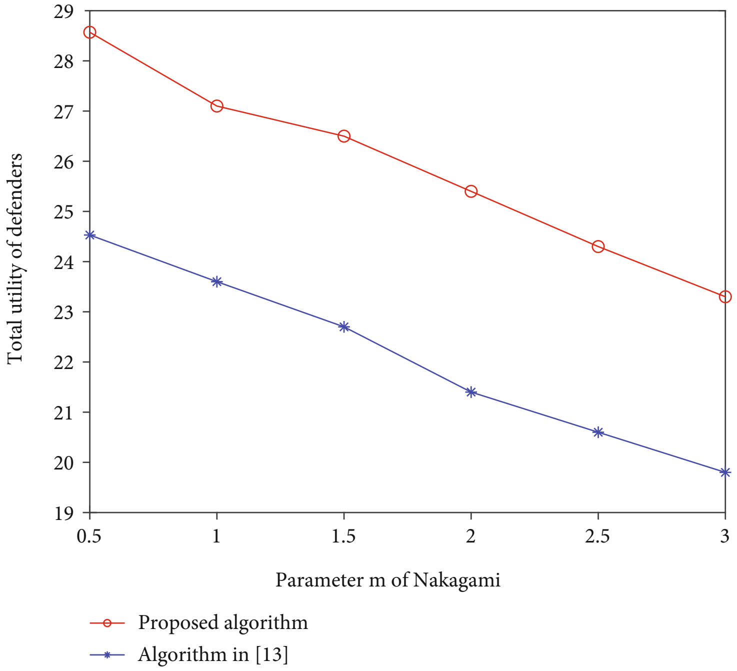


FIGURE 11: Total utility of defenders with different values of m in Nakagami (proposed vs. traditional algorithm [12]).

where P_i^d represents the transmission power defender i, h_{mi}^k represents the dynamic interferences of defender i at kth stage, and δ represents the power of noise. In equation (7), $B\log_2(1+P_i^d/\delta)$ represents the channel capacity of defender i before a network is attacked, and $B\log_2(1+P_i^d/\sum_{k=1}^{M}P_k^a h_{\mathrm{mi}}^k+\delta)$ represents the channel capacity of defender i after the network is attacked. M represents the number of attackers in a network.

Similarly, by Shannon formula, the cost of the kth attacker L_k^a can be denoted as

$$L_k^a = \alpha P_k^a, \tag{8}$$

where P_k^a represents the transmission power of attacker k and α represents the cost per unit power consumption by an attacker.

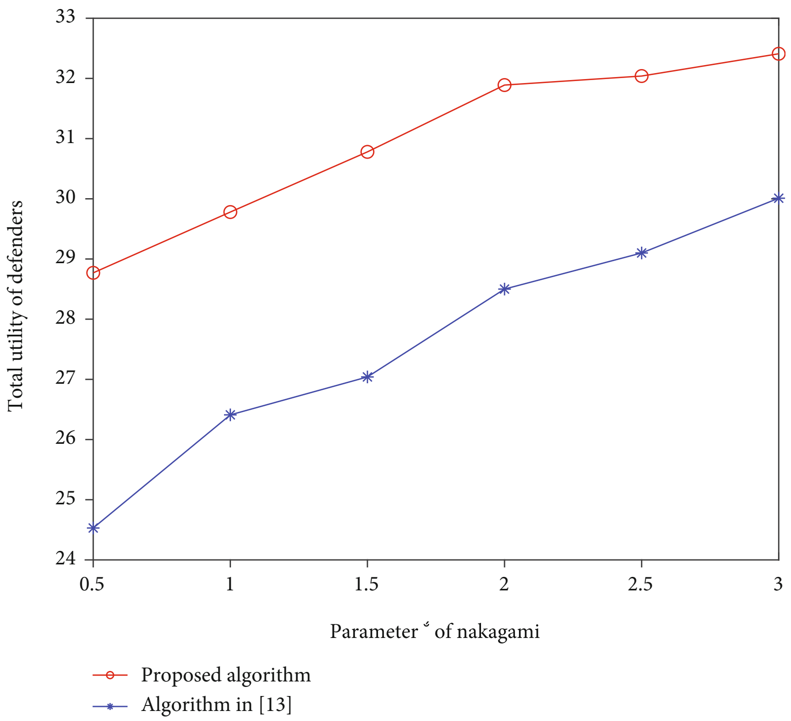


Figure 12: Total utility of defenders with different values of ϕ in Nakagami (proposed vs. traditional algorithm [12]).

Replacing Equation (6) with both Equation (7) and Equation (8), we can mathematically denote U_k^a as

$$U_k^a = \sum_{i=1}^{N}\left(B\log_2\left(1+\frac{P_i^d}{\delta}\right) - B\log_2\left(1+\frac{P_i^d}{\sum_{k=1}^{M}P_k^a+\delta}\right)\right) - \alpha P_k^a. \tag{9}$$

On the other hand, a defender's strategy is primarily dependent on two factors, including the defender's channel capacity after being attacked and the defender's transmission power. Therefore, the overall utility of defender i, i.e., U_i^d can be expressed as

$$U_i^d = C_i^d - \widehat{L_i^d}, \tag{10}$$

where C_i^d is defined as the channel capacity of defender i after being attacked and $\widehat{L_i^d}$ is defined as the cost of defender i to maintain the capacity of his/her channel.

By Shannon formula, C_i^d can be denoted as

$$C_i^d = B\log_2\left(1+\frac{P_i^d}{\sum_{k=1}^{M}P_k^a h_{\mathrm{mi}}^k+\delta}\right). \tag{11}$$

Also, by Shannon formula, L_i^d can be denoted as

$$\widehat{L_i^d} = \eta P_i^d, \tag{12}$$

where η represents the cost per unit power consumption by a defender.

Similarly, U_i^d can be formulated as

$$U_i^d = B\log_2\left(1+\frac{P_i^d}{\sum_{k=1}^{M}P_k^a h_{\mathrm{mi}}^k+\delta}\right) - \eta P_i^d. \tag{13}$$

4. Optimal Solution

Each party in a battlefield expects to adjust power to maximize its user capacity. This utility optimization problem can be defined as a Stackelberg game. In this section, a Nash equilibrium for the game would eventually be achieved on both sides. The defender always adjusts its strategy based on the attacker's, so the defender is defined as a leader while the attacker as a follower. Building on the above-mentioned mechanism, we would explore and prove the existence and exact solution of the best responses of both parties on a battlefield.

4.1. Optimal Strategy of the Defender. In the following, we discuss the optimal solution to maximize the utility of (13), and it can be characterized as Theorem 1.

Theorem 1. *The optimal solution of U_i^d to function (13) for the defender exists and can be denoted as*

$$\widehat{P}_i^d = \frac{B}{\eta} - \sum_{k=1}^{M} P_k^a h_{mi}^k - \delta. \tag{14}$$

Proof. We first prove the existence of the optimal solution of U_i^d. The existence can be proved by computing the second derivative of the utility function.

$$\frac{\partial^2 U_i^d}{\partial^2 P_i^d} = \frac{-B}{\left(\sum_{k=1}^{M} P_k^a h_{\mathrm{mi}}^k + \delta + P_i^d\right)^2} < 0. \tag{15}$$

In the equation, bandwidth is positive, so the second-order derivative $-B/(\sum_{k=1}^{M} P_k^a h_{mi}^k + \delta + P_i^d)^2 < 0$, which proves that the utility function U_i^d is concave. The optimal solution of the function that would maximize the utility of the defender can be computed by setting the first-order derivative to 0.

$$\frac{\partial U_i^d}{\partial P_i^d} = \frac{B}{\sum_{k=1}^{M} P_k^a + \delta + P_i^d} - \eta = 0. \tag{16}$$

By employing the equation, we can attain the optimal utility of the defender as $\widehat{P}_i^d = B/\eta - \sum_{k=1}^{M} P_k^a h_{\mathrm{mi}}^k - \delta$. □

4.2. Optimal Strategy of the Attacker. In the following, we discuss the optimal solution to maximize the utility of (9), and it can be characterized as Theorem 2.

Theorem 2. *In consideration of the optimal strategy of the defender, the optimal solution of U_k^a to function (9) for the attacker can be achieved when the following equation holds:*

$$\sum_{i=1}^{N} \frac{\delta h_{mi}^k}{\left(\sum_{k=1}^{M} P_k^a h_{mi}^k - B/\eta\right)} + \sum_{i=1}^{N} \frac{h_{mi}^k}{\left(\sum_{k=1}^{M} P_k^a h_{mi}^k + \delta\right)} = \frac{\alpha}{B}. \tag{17}$$

Proof. By substituting the optimal solution of the defender into the function (9), and the function can be transformed into

$$\begin{aligned} U_k^a = {} & \sum_{i=1}^{N} \left\{ B \log_2 \left[1 + \frac{1}{\delta} \left(\frac{B}{\eta} - \sum_{k=1}^{M} P_k^a h_{\mathrm{mi}}^k - \delta \right) \right] \right\} \\ & - \sum_{i=1}^{N} \left\{ B \log_2 \left[1 + \frac{B/\eta - \sum_{k=1}^{M} P_k^a h_{\mathrm{mi}}^k - \delta}{\sum_{k=1}^{M} P_k^a h_{\mathrm{mi}}^k + \delta} \right] \right\} - \alpha P_k^a. \end{aligned} \tag{18}$$

Based on the function (18), we first prove the existence of the optimal solution of U_k^a. The existence can be proved by computing the second derivative of the utility function.

$$\frac{\partial^2 U_k^a}{\partial^2 P_k^a} = \sum_{i=1}^{N} \left[-B\delta \left(h_{\mathrm{mi}}^k \right)^2 \right] \left(\frac{B}{\eta} - \sum_{k=1}^{M} P_k^a h_{\mathrm{mi}}^k \right)^{-2} + \sum_{i=1}^{N} \left(-\mathrm{Bh}_{\mathrm{ki}}^2 \right) \left(\delta + \sum_{k=1}^{M} P_k^a h_{\mathrm{mi}}^k \right)^{-2} < 0. \tag{19}$$

It is not hard to reach the conclusion that the second-order derivative of U_k^a is less than 0, so the utility function U_k^a is concave. The optimal solution of the function that would maximize the utility of the attacker can be computed by setting the first-order derivative to 0.

$$\frac{\partial U_k^a}{\partial P_k^a} = \sum_{i=1}^{N} \frac{B\delta h_{\mathrm{mi}}^k}{\sum_{k=1}^{M} P_k^a h_{\mathrm{mi}}^k - B/\eta} + \sum_{i=1}^{N} \frac{\mathrm{Bh}_{\mathrm{mi}}^k \left(\delta + \sum_{k=1}^{M} P_k^a h_{\mathrm{mi}}^k \right)}{\left(\sum_{k=1}^{M} P_k^a h_{\mathrm{mi}}^k + \delta \right)^2} - \alpha. \tag{20}$$

Let $\partial U_k^a / \partial P_k^a = 0$, we have

$$\frac{\alpha}{B} = \sum_{i=1}^{N} \frac{\delta h_{\mathrm{mi}}^k}{\sum_{k=1}^{M} P_k^a h_{\mathrm{mi}}^k - B/\eta} + \sum_{i=1}^{N} \frac{h_{\mathrm{mi}}^k \left(\delta + \sum_{k=1}^{M} P_k^a h_{\mathrm{mi}}^k \right)}{\left(\sum_{k=1}^{M} P_k^a h_{\mathrm{mi}}^k + \delta \right)^2}. \tag{21}$$

□

4.3. Stackelburg Equilibrium Algorithm. The mutual best response is the Nash equilibrium of the Stackelberg game that maximizes the utility for both attackers and defenders. Building on the above-mentioned description on the Stackelberg game, we present an algorithm to determine the Nash equilibrium using a searching algorithm within a reasonable range of power that the attackers can accept. As shown in the Pseudo codes of Algorithm 1, we firstly initialize the relevant parameters, including B that represents bandwidth, h_{mi} that represents a set for interferences at the first round (h_{mi} would dynamically change according to the Markov transition probability matrix), δ that represents the power of noise, and P_m that represents a reasonable maximum power that the attackers can accept. Following this, we use a search algorithm with a reasonable range of power $[0, P_m]$ for the attackers to determine the game equilibrium P_a^* and the corresponding utilities of the attackers and defenders U_a^*, U_d^*.

5. Simulation Results

We experiment through a hardware platform that includes a NI-PXIe 1085 and three USRP-RIO-1082 devices. As shown in Figure 4, the NI-PXIe 1085 device is designed to display graphic results, while three USRP RIO-1082 devices are designed to simulate transmitters, receivers, and interference generators. Two USRP devices are equipped with four antennas, and we use them to simulate two transmitters and two receivers. The third USRP device is equipped with two antennas to simulate two interference generators. Additionally, we use a NI-PXIe 1085 platform to monitor the graphic results of interference, shown in Figure 5. We also load the data generated by USRP-RIO-1082 devices to MATLAB for subsequent numerical analysis. We compare the analytic results using the proposed algorithm and the algorithm in [19], respectively.

The simulation parameters are set as follows: the parameters of Nakagami channel models are $m = 1$ and $\eta = 0.5$; the signal to noise ratio ranges from 0 dB to 20 dB; the level of signal to interference ratio ranges from 0 dB to 20 dB; the cost parameter of transmission power by defenders ranges from 0.1 to 1.

5.1. Individual Utility of Defenders. In this section, we compare the individual utility of defenders using our proposed algorithm with the algorithm in [19], which is viewed as a benchmark. As shown in Figure 6, for each of defenders, our proposed algorithm can achieve a higher individual utility in comparison with the benchmark algorithm. The comparison result illustrates that our proposed algorithm outperforms the benchmark algorithm. Specifically, an extra 30%-50% of individual utility can be achieved using the proposed algorithm than the benchmark algorithm. The reason is that the proposed algorithm considers the dynamic variation of the system environment, and defenders can adjust their own strategies in view of both attackers' strategies and channel fading.

Across the defenders, the individual utility of each defender primarily depends on the strategies of attackers and the channel fading. Given the same attacker's strategies in each round of game, the difference of individual utility among defenders is dependent on their own channel fading. In the following, we investigate the channel fading of each defender. As shown in Figure 7, the individual utility decreases with the channel fading. For example, while defender 4 has the lowest channel fading and has the highest individual utility, defender 7 has the highest channel fading and has the lowest individual utility.

5.2. Total Utility of Defenders. In section, we investigate the total utility of defenders using both our proposed algorithm and the benchmark algorithm in [19]. Specifically, we consider the total utility with different values of cost parameter η, bandwidth, signal to noise ratio (SNRs), Nakagami channel model parameters m and ϕ, respectively.

As shown in Figure 8, the total utility of defenders decreases with the values of η, and the proposed algorithm can achieve a higher utility than the benchmark algorithm across various η. The reason is that a higher η indicates the defenders need to achieve a certain level of utility with a higher level of cost, and thus the total utility of defenders decreases with the values of η.

As shown in Figure 9, the total utility of defenders increases with the values of bandwidths, and the proposed algorithm can achieve a higher utility than the benchmark algorithm across various bandwidth. The reason is that a higher bandwidth indicates the defenders can achieve a higher utility with the same cost of transmission power, and thus the total utility of defenders increases with the values of bandwidth.

As shown in Figure 10, the total utility of defenders increases with the values of SNRs, and the proposed algorithm can achieve a higher utility than the benchmark algorithm across various SNRs. The reason is that a higher level of SNR indicates the defenders can achieve a higher utility when occupying the same amount of bandwidth, and thus the total utility of defenders increases with the values of SNRs.

As shown in Figure 11, the total utility of defenders decreases with the values of m in Nakagami, and the proposed algorithm can achieve a higher utility than the benchmark algorithm across various values of m. The reason is that a larger value of m in Nakagami leads to a higher channel fading, and thus the utility achieved by defenders is lower when occupying the same amount of bandwidth and paying the same cost of transmission power. Thus, the total utility of defenders decreases with the values of m in Nakagami.

As shown in Figure 12, the total utility of defenders increases with the values of ϕ in Nakagami, and the proposed algorithm can achieve a higher utility than the benchmark algorithm across various values of ϕ. The reason is that a smaller value of ϕ in Nakagami leads to a higher channel fading, and thus the utility achieved by defenders is lower when occupying the same amount of bandwidth and paying the same cost of transmission power. Thus, the total utility of defenders increases with the values of ϕ in Nakagami.

6. Conclusion

This paper has proposed a game theoretic model in consideration of the adversarial and dynamic nature of the urban IoBT environment. By employing a Stackelberg game theoretic method, our proposed framework can effectively leverage network resources and improve network performance in an adversarial scenario. We also consider the interactive effects of dynamic channel fading by using a Nakagami distribution based Markov process. The detailed analysis illustrates that with considering the impact of the adversarial and dynamic nature of urban IoBT, our proposed algorithm can improve the entire network performance. It is known that the security issues are the most significant perspective in the IoBT environment. So in our future work, in combination of network optimization, we will explore an authentication model to fit in the characteristics of IoBT scenario.

Data Availability

We have no data used in this work.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work is partially funded by Science and Technology Program of Sichuan Province (2021YFG0330), partially funded by Intelligent Terminal Key Laboratory of Sichuan Province (SCITLAB-0001), and partially funded by Fundamental Research Funds for the Central Universities (ZYGX2019J076).

References

[1] W. D. Lu, Y. Ding, Y. Gao et al., "Resource and trajectory optimization for secure communications in dual unmanned aerial vehicle mobile edge computing systems," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 4, pp. 2704–2713, 2022.

[2] Y. Xu, J. Tang, B. Li, N. Zhao, D. Niyato, and K. K. Wong, "Adaptive aggregate transmission for device-to-multi-device aided cooperative NOMA networks," *IEEE Journal on Selected Areas in Communications*, vol. 40, no. 4, pp. 1355–1370, 2022.

[3] W. D. Lu, P. Y. Si, Y. Gao et al., “Trajectory and resource optimization in OFDM-based UAV-powered IoT network,” *IEEE Transactions on Green Communications and Networking*, vol. 5, no. 3, pp. 1259–1270, 2021.

[4] W. D. Lu, P. Y. Si, G. X. Huang et al., “SWIPT cooperative spectrum sharing for 6G-enabled cognitive IoT network,” *IEEE Internet of Things Journal*, vol. 8, no. 20, pp. 15070–15080, 2021.

[5] C. Kai, H. Li, L. Xu, Y. Li, and T. Jiang, “Energy-efficient device-to-device communications for green smart cities,” *IEEE Transactions on Industrial Informatics*, vol. 14, no. 4, pp. 1542–1551, 2018.

[6] X. Li, R. Fan, H. Hu, N. Zhang, X. Chen, and A. Meng, “Energy-efficient resource allocation for mobile edge computing with multiple relays,” *IEEE Internet of Things Journal*, vol. 9, no. 13, pp. 10732–10750, 2022.

[7] X. An, R. Fan, H. Hu, N. Zhang, S. Atapattu, and T. A. Tsiftsis, “Joint task offloading and resource allocation for IoT edge computing eith sequential task dependency,” *IEEE Internet of Things Journal*, vol. 9, no. 17, pp. 16546–16561, 2022.

[8] H. N. Dai, Z. Zheng, and Y. Zhang, “Blockchain for Internet of Things: a survey,” *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8076–8094, 2019.

[9] J. Huang, L. Kong, G. Chen, M.-Y. Wu, X. Liu, and P. Zeng, “Towards secure industrial IoT: blockchain system with credit-based consensus mechanism,” *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3680–3689, 2019.

[10] K. L. Ang and J. K. P. Seng, “Application specific internet of things (ASIoTs): taxonomy, applications, use case and future directions,” *IEEE Access*, vol. 7, pp. 56577–56590, 2019.

[11] A. Kott, A. Swami, and B. J. West, “The Internet of Battle Things,” *Computer*, vol. 49, no. 12, pp. 70–75, 2016.

[12] R. Yang, F. Yu, P. Si, Z. Yang, and Y. Zhang, “Integrated blockchain and edge computing systems: a survey, some research issues and challenges,” *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1508–1532, 2019.

[13] N. Abuzainab and W. Saad, “Dynamic connectivity game for adversarial internet of battlefield things systems,” *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 378–390, 2018.

[14] J. F. Harvey, M. B. Steer, and T. S. Rappaport, “Exploiting high millimeter wave bands for military communications, applications, and design,” *IEEE Access*, vol. 7, pp. 52350–52359, 2019.

[15] P. Kar, A. Roy, and S. Misra, “Connectivity reestablishment in self-organizing sensor networks with dumb nodes,” *ACM Transactions on Autonomous and Adaptive Systems (TAAS)*, vol. 10, no. 4, 2016.

[16] A. R. Elsherif, W.-P. Chen, A. Ito, and Z. Ding, “Adaptive resource allocation for interference management in small cell networks,” *IEEE Transactions on Communications*, vol. 63, no. 6, pp. 2107–2125, 2015.

[17] P. Chen, S. Cheng, and K. Chen, “Information fusion to defend intentional attack in internet of things,” *IEEE Internet of Things Journal*, vol. 1, no. 4, pp. 337–348, 2014.

[18] N. Abuzainab and W. Saad, “Misinformation control in the internet of battlefield things: a multiclass mean-field game,” in *2018 IEEE Global Communications Conference (GLOBECOM)*, Abu Dhabi, United Arab Emirates, 2018.

[19] Y. Hu, A. Sanjab, and W. Saad, “Dynamic psychological game theory for secure internet of battlefield things (IoBT) systems,” *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 3712–3726, 2019.

[20] W. Lee, J. Choi, J. Lee, Y. Kim, and S. Kim, “Distributed power control-based connectivity reconstruction game in wireless localization,” *IEEE Communications Letters*, vol. 21, no. 2, pp. 334–337, 2017.

[21] D. Lin and L. Fabrice, “An algorithm that predicts CSI to allocate bandwidth for healthcare monitoring in hospital’s waiting rooms,” *International Journal of Telemedicine and Applications*, vol. 2012, Article ID 843527, 13 pages, 2012.

[22] D. W. Matolak, I. Sen, W. H. Xiong, and N. T. Yaskoff, “5 GHZ wireless channel characterization for vehicle to vehicle communications,” in *MILCOM 2005 - 2005 IEEE Military Communications Conference*, pp. 3016–3022, Atlantic City, NJ, USA, 2005.

[23] Y. Xu, B. Li, N. Zhao et al., “Coordinated direct and relay transmission with NOMA and network coding in Nakagami-m fading channels,” *IEEE Transactions on Communications*, vol. 69, no. 1, pp. 207–222, 2021.

[24] L. C. Wang, W. C. Liu, A. Chen, and K. N. Yen, “Joint rate and power adaptation for wireless local area networks in generalized Nakagami fading channels,” *IEEE Transactions on Vehicular Technology*, vol. 58, no. 3, pp. 1375–1386, 2009.

[25] C. D. Iskander and P. T. Mathiopoulos, “Fast simulation of diversity Nakagami fading channels using finite-state Markov models,” *IEEE Transactions on Broadcasting*, vol. 49, no. 3, pp. 26–277, 2003.