Cognitive Radio Anti-Jamming Scheme for Security Provisioning IoT Communications

Sungwook Kim*
Department of Computer Science, Sogang University,
35 Baekbeom-ro (Sinsu-dong), Mapo-gu, Seoul, 121-742, South Korea
E-mail: swkim01@sogang.ac.kr
* Corresponding author: Sungwook Kim

Received April 8, 2015; revised July 8, 2015; accepted August 29, 2015; published October 31, 2015

Abstract

Current research on Internet of Things (IoT) has primarily addressed the means to enhancing smart resource allocation, automatic network operation, and secure service provisioning. In particular, providing satisfactory security service in IoT systems is indispensable to its mission critical applications. However, limited resources prevent full security coverage at all times. Therefore, these limited resources must be deployed intelligently by considering differences in priorities of targets that require security coverage. In this study, we have developed a new application of Cognitive Radio (CR) technology for IoT systems and provide an appropriate security solution that will enable IoT to be more affordable and applicable than it is currently. To resolve the security-related resource allocation problem, game theory is a suitable and effective tool. Based on the Blotto game model, we propose a new strategic power allocation scheme to ensure secure CR communications. A simulation shows that our proposed scheme can effectively respond to current system conditions and perform more effectively than other existing schemes in dynamically changeable IoT environments.

Keywords: Internet of Things, Cognitive Radio, Power Resource Allocation, Blotto Game, Learning-based game model, Iterative Nash Bargaining

This research was supported by the MSIP (Ministry of Science, ICT and Future Planning), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2015-H8501-15-1018) supervised by the IITP(Institute for Information & communications Technology Promotion) and by the Sogang University Research Grant of 2014(201410020.01).

http://dx.doi.org/10.3837/tiis.2015.10.023 **ISSN : 1976-7277**

1. Introduction

The rapid development of communication technology has enabled various smart objects to connect through the Internet and provided many data interoperability methods for application purposes. Thus, many technologies currently exist that have the single objective of providing a truly connected world of not only people but also everyday objects. Internet-of-Things (IoT) communications is an emerging communication paradigm that provides ubiquitous connectivity between devices as well as an ability to communicate autonomously and thus requiring no human operators. The vision of IoT represents a future in which billions of everyday objects and the environments in which they exist are connected and managed through a range of communication networks and cloud-based servers [1].

The most critical resource for IoT system communications is radio spectrum. With the dramatic development of IoT communications, the demand for wireless spectrum resources has been growing rapidly. However, the inflexible spectrum policies by the Federal Communications Commission result in a large portion of scarce spectrum resources remaining unused. The inefficient usage of the limited radio spectrum necessitates recent development of dynamic spectrum access techniques by means of Cognitive Radio (CR) technology. CR is a promising communication paradigm designed to solve the conflict between the limited spectrum resources and increasing demand for wireless services. By exploiting the spectrum in an opportunistic fashion, unlicensed users (i.e., secondary users) are allowed to access licensed channels on a non-interference basis to legacy spectrum holders (i.e., primary users) [2]. Therefore, the CR paradigm has emerged as a promising technology to enhance IoT systems by efficiently and smartly using the limited radio spectrum resources.

For traditional CR operations, secondary users are not assumed to be in a hostile environment. However, in real world operations, malicious attackers can cause damage to legitimate users and prevent the spectrum from being used efficiently. In fact, cognitive radio networks are extremely vulnerable to malicious attacks, partly because secondary users do not own the spectrum; Hence, their opportunistic access cannot be protected from adversaries. Moreover, highly dynamic spectrum availability and often distributed network structures mean that implementing effective security countermeasures is difficult. Therefore, methods of securing spectrum sharing is critical to the wide deployment of CR technology. However, only recently, security issues have received much attention [3],[4].

Although malicious attackers can launch many types of attacks, the most critical malicious attack in a CR network is jamming, in which a malicious user, or the ‘jammer’, seeks to prevent or jam the communications of secondary users. The secondary user, however, monitors the presence or absence of several Primary Users (PUs) to identify spectrum opportunities, and allocates power to those fallow channels using some randomized strategy. This is necessary to avoid jamming as much as possible [2]. In this work, a fallow channel refers to an idle channel which the PU does not use temporarily. Recently, jamming attacks have occurred in wireless networking, and existing anti-jamming solutions have included physical layer defenses. However, they are not directly applicable to CR networks, because the radio spectrum availability continues to change with the PUs returning or vacating licensed channels [3],[5],[6].

To address efficiently the jamming attack in CR networks, game theory is increasingly garnering attention. Game theory is a field of applied mathematics that provides an effective tool to model interactions among independent decision makers. It can describe the reactions of

one set of decision makers to another and analyze the situations in terms of conflict and cooperation [7]. Thus, game theory is a major paradigm for modeling security domains that feature complex resource allocation. Most game theoretic approaches applied to security-related problems require attack-defense interactions. Based on the interactions between attackers and defenders, the security resource allocation problem can be formulated as a non-cooperative game model.

In 1921, French mathematician Émile Borel proposed the concept of the Blotto game. This game is a two-person constant-sum game in which each player has limited resources to distribute onto n independent battlefields and without knowledge of the opponent's actions. The player who allocates more resources on the battlefield i ($1 \leq i \leq n$) wins that battle and its associated payoff. Both players seek to maximize the number of battles won. The Blotto game is a fundamental model for multidimensional strategic resource allocation and is widely applicable in fields from operations research, to advertising and to military and systems defense [8]. After the Blotto game was introduced in 1950, John Nash introduced the Nash Bargaining Solution (NBS) to allocate resources fairly and optimally [7]. NBS is a field of cooperative game theory and an effective tool to achieve a mutually desirable solution with an acceptable balance between efficiency and fairness. Due to its many appealing properties, the basic concept of NBS has become an interesting research topic in a wider range of real life situations. Recently, network security problems have been added to this range [7].

Motivated by the aforementioned discussion, we design a new strategic security provisioning scheme for CR-based IoT communications. To formulate a security provisioning problem, we adopt a two-person (i.e., attacker and defender) constant-sum Blotto game model. In addition, the basic concept of the iterative Nash bargaining solution is used to solve the developed Blotto game model. By using these features, we can allocate the secondary user's power as efficiently as possible to ensure IoT communication security. Under dynamic situations, our approach can be used for optimal system performance in an acceptable time constraint. The major features of the proposed scheme are i) the ability to guarantee a security level as high as possible, ii) the ability to respond to a current IoT situation for adaptive management, iii) a dynamically adjustable approach that considers real-time information, and iv) an adaptively interactive learning process to approximate an efficient equilibrium. The chief novelty of our proposed scheme is its self-adaptability for dynamics, feasibility in providing a globally desirable solution and effectiveness in realistic IoT system operations.

2. Related Work

Recently, several strategic CR based communication control schemes have been presented to ensure the system security. The *Reinforcement Learning based Anti-Jamming* (*RLAJ*) scheme [9] has considered the jammer's attack on the secondary user in CR networks. By using the stochastic zero-sum game and Markov decision process (MDP) model, secondary users in the *RLAJ* scheme can learn the time varying characteristics of the channel as well as the jammer's random strategy using the reinforcement learning algorithms. In this scheme, learning algorithms are developed as on-policy and non-greedy algorithms, and learn a separate state-value function. This state-value function is action independent, so trained by using more experiences. The independence of state value function on the actions results in the faster learning rate.

The *Cognitive Radio Anti-Jamming* (*CRAJ*) scheme [4] focuses on the anti-jamming game by modeling the interaction between a secondary user and attackers. First, the *CRAJ* scheme investigates the situation where a secondary user can access only one channel at a time and hop

among different channels, and models it as an anti-jamming game. Second, to analyze the interaction between the secondary user and attacker, the *CRAJ* scheme derives a channel hopping defense strategy using the Markov decision process approach. In the scenario where both the secondary user and attackers are equipped with a single radio and access only one channel at any time, the secondary user hop proactively between channels as the defense strategy. This scenario is extended to where secondary users can access all available channels simultaneously. The *CRAJ* scheme shows that the MDP-based hopping is a good approximation to the game equilibrium.

The *Blotto Game based Power Allocation* (*BGPA*) scheme [2] has modeled the power allocation problem under malicious jamming attacks as a two-player zero-sum game. This jamming game has been converted to the Blotto game, which provides a minimax strategy that the secondary user should adopt in order to minimize the worst case damage caused by the attacker. Aware of the absence of several primary users and the presence of a malicious user, a secondary user can allocate power to those fallow channels with a randomized strategy, in hope of alleviating the damage caused by the malicious user. Under certain conditions, the unique Nash Equilibrium can be derived. However, it still remains a question to find the specific NE strategy determined by the joint probability distribution function. The *BGPA* scheme can finally obtain the NE strategy through constructing one kind of joint distribution that matches desired marginal distribution and meets the total power restriction.

All the earlier work has attracted a lot of attention and introduced unique challenges to efficiently solve the strategic security problems in CR based communications. However, there are several disadvantages. First, these existing schemes rely on the high complexity and extra overhead; the increased overhead needs intractable computations. Second, they developed their schemes under inappropriate assumptions. Control algorithms based on the inapplicable presumption can cause potential erroneous decisions. Third, these schemes cannot adaptively estimate the current IoT system conditions. Under dynamic system environments, it is an ineffective operation approach. Compared to these schemes [2],[4],[9], the proposed scheme attains better system performance.

This paper is organized as follows. Section II presents the basic ideas of Blotto game model and Nash bargaining solution, and describes the proposed algorithms in detail. In Section III, performance evaluation results are presented along with comparisons with the existing schemes proposed in [2], [4] and [9]. In addition, concluding remarks and future work are given in Section IV.

3. Power Allocation Algorithms for CR Communications

In this section, we describe the proposed strategic power allocation algorithms in detail. To develop our security provisioning algorithms, the Blotto game model and Nash bargaining solution are used as major elements. In dynamic CR network environments, our game-based approach is proven to be an effective solution for IoT security problems.

3.1 Anti-Jamming Blotto Game Model for Cognitive Radio Networks.

In this study, we consider a dynamic CR spectrum access network where Secondary Users (SU) equipped with cognitive radio are allowed to access temporarily unused licensed spectrum channels that belong to multiple PUs. To avoid conflict or harmful interference to the PUs, the SU must listen to the spectrum before every attempt of transmission. In this study, we assume that the CR network is a time-slotted system, and the SU can take every opportunity to use the currently unused licensed spectrum, and vacate the spectrum whenever a PU reclaims the

spectrum rights [3].

For our system model, we assume that *M* channels and *m* fallow channels (i.e., available channels for the SU where M > *m*) exist for CR services. The SU has a total power $\mathcal{P}$ and can allocate power p_k to the kth fallow channel under the constraint that the total power should not exceed the limit $\sum_{k=1}^{m} p_k = \mathcal{P}$. At the beginning of each time slot, the SU senses several channels to locate the fallow ones that are not occupied by PUs. Simultaneously, a jammer may sabotage a communication link by injecting interference power $\mathcal{J}_k$ to the kth fallow channel. In addition, we assume the jammer has a total power constraint $\sum_{k=1}^{m} \mathcal{J}_k = \mathfrak{T}$, where $\mathfrak{T}$ is the power budget for the jammer. Therefore, the power allocation vectors $\mathbb{P} = (p_1, p_2, \cdots, p_m)$ and $\mathbb{I} = (\mathcal{J}_1, \mathcal{J}_2, \cdots, \mathcal{J}_m)$ are actions of the SU and jammer, respectively [2], [4]. At the receiver, if the received *signal-to-interference-and-noise* ratio (*SINR*) exceeds the minimum requirement Γ suck as in the following

$$\frac{p_k}{\mathcal{J}_k + \sigma_k^2} \geq \Gamma \tag{1}$$

packets can be transmitted successfully. Otherwise, when the *SINR* drops below a certain threshold (Γ), the link is too poor to be useful, and packet transmissions fail. In addition, σ_k^2 is the noise variance of channel k, which we assume is the same for all channels, i.e., $\sigma_k^2 = \sigma^2$, and Γ is determined by the type of service [2], [4].

To simplify analysis, we assume both the SU and jammer have perfect spectrum sensing that they know at each time slot. In the presence of a jammer, the SU wants to maximize the number of successful transmissions, by randomizing his power allocation strategy. However, the jammer also allocates his power to minimize successful transmissions of the SU. With interference power jammed into spectrum channels, the *SINR* at the SU's receiver will be dragged down [2]. To maximize their payoffs, the SU and jammer adaptively allocate their power resources in different channels with their power constraints. Therefore, the SU and jammer play a game in every time slot, iteratively. This game falls into the category of Colonel Blotto games in which two opponents distribute limited resources over several battlefields with a payoff equal to the sum of outcomes from individual battles [4].

The traditional Blotto game is considered a classic in game theory. This model assumes that two generals are competing in a battle across a certain number of battlefields. Each general must decide how to divide his available troops on the fields. On each field, the side that deploys the most troops wins the battle. The general who divides his troops most effectively and wins the most battles wins the game. The Blotto game has far-reaching implications a wherever multi-front division of resources is involved, including business, logistics, and political campaigns [8].

In this study, we develop a Blotto game model for making a power allocation in CR networks. To design our game model, game form ($\mathbb{G}$) can be formulated with four parameters: players, a strategy set for each player, the consequences of strategies (i.e., a set of payoffs), and the number of fallow spectrum channels. Mathematically, $\mathbb{G}$ can be defined as $\mathbb{G} = \{\mathcal{N}, \{S_i\}_{i\in\mathcal{N}}, \{\mathcal{U}_i\}_{i\in\mathcal{N}}, m\}$,

- $\mathcal{N}$ is the finite set of players; there are two players in our game. One is the SU, and the other is the jammer ($\|\mathcal{N}\|$ =2)
- S_i is the set of strategies with the player *i* ($i \in \mathcal{N}$). We consider two power vectors ($\mathbb{P}$ and $\mathbb{I}$). If the player i is the SU, $S_{SU} = (p_1, p_2, \cdots, p_m) \in \mathbb{P}$. Otherwise, $S_{jammer} = (\mathcal{J}_1, \mathcal{J}_2, \cdots, \mathcal{J}_m) \in \mathbb{I}$. The SU and jammer hide their power allocation strategies with one

another.

- $\mathcal{U}_i$ is the payoff received by the player *i*. After both players decide their power allocation, the payoff is given based on the number of successful transmissions.
  - if the player *i* is the SU,

$$\mathcal{U}_{SU}(\mathbb{P},\mathbb{I}) = \sum_{k=1}^{m} 1(p_k > \Gamma \times (\mathcal{I}_k + \sigma^2)), \qquad \text{s.t.}, p_k \in \mathbb{P} \tag{2}$$

  - if the player *i* is a jammer,

$$\mathcal{U}_{jammer}(\mathbb{P},\mathbb{I}) = \sum_{k=1}^{m} 1\left(\mathcal{I}_k > \frac{p_k}{\Gamma} - \sigma^2\right), \qquad \text{s.t.}, \mathcal{I}_k \in \mathbb{I} \tag{3}$$

  where 1(·) is the indicator function, returning the gaining value (*or* 0) when the argument in the parenthesis holds true (*or* false).
- m is the number of available fallow channels for CR services.

In this study, the Blotto game model is used to solve the security problem. To express mathematically the Blotto game for CR security problems, we assume that an attacker (i.e., a jammer) and a defender (i.e., the SU) have their private power resources ($\mathfrak{T}$ and $\mathcal{P}$), and that *m* battlefields exist (i.e., *m* fallow channels). A jammer and SU must allocate their $\mathfrak{T}$ and $\mathcal{P}$ across all *m* fallow channels, and compete all *m* fallow channels simultaneously. The SU wins the channel *i* ($1 \leq i \leq m$) if $p_i > \Gamma \times (\mathcal{I}_k + \sigma^2)$, where p_i (*or* $\mathcal{I}_i$) is the power resource allocation of SU (*or* jammer) for the channel *i*. The payoff function ($\mathcal{U}_{SU}$) for SU is defined as

$$\mathcal{U}_{SU}(\mathbb{P},\mathbb{I}) = \sum_{i=1}^{m} f_i(p_i,\mathcal{I}_i), \ \text{s.t.}, f_i(p_i,\mathcal{I}_i) = \begin{cases} \ln\alpha_i, & \text{if } p_k > \Gamma \times (\mathcal{I}_k + \sigma^2) \\ \ln {}^{\alpha_i}/_{2}, & \text{if } p_k = \Gamma \times (\mathcal{I}_k + \sigma^2) \\ 0, & \text{if } p_k < \Gamma \times (\mathcal{I}_k + \sigma^2) \end{cases} \tag{4}$$

where $\mathbb{P}$ and $\mathbb{I}$ are the sets of feasible power allocations of SU and jammer, respectively; they are m-dimensional vectors $(p_1, p_2, \cdots, p_m)$ and $(\mathcal{I}_1, \mathcal{I}_2, \cdots, \mathcal{I}_m)$. α_i is a weighted factor (i.e., relative importance) for the channel *i*. In this work, α_i is estimated based on the relative *SINR* ratio, like as

$$\alpha_i = e + \frac{SINR_k}{\max\limits_{1 \leq i \leq m}[SINR_i]} \tag{5}$$

where *e* is Euler's number. According to (4), $\mathcal{U}_{SU}(\mathbb{P},\mathbb{I})$ consists of *m* payoff functions ($f_{i,1\leq i\leq m}(p_i,\mathcal{I}_i)$), which can be rewritten as follows.

$$\mathcal{U}_{SU}(\mathbb{P},\mathbb{I}) = \ln(g_1 \times .. \times g_i \times .. \times g_m) = \ln(\prod_{i=1}^{m} g_i), \ \text{s.t.}, \ g_i \in \{\alpha_i, {}^{\alpha_i}/_{2}, 1\} \tag{6}$$

Therefore, all possible SU's payoff pairs ($f_1(p_1,\mathcal{I}_1) \ldots f_m(p_m,\mathcal{I}_m)$) that *m* payoffs jointly achieve form a feasible payoff set ($\mathbb{S}^{SU}$) of SU.

3.2 Interactive Feedback Process for Strategic Resource Allocation

In game theory, each player seeks to maximize his payoff function. To obtain an effective solution, John Nash proposed the NBS solution concept [7]. It is formulated by expected payoff functions over the set of feasible agreements and the outcome that results in the case of disagreement. NBS is an effective tool to achieve a mutually desirable solution by allocating resources optimally. In addition, it does not require global objective functions unlike conventional optimization methods such as *Lagrangian* or dynamic programming. Because of its many appealing properties, the basic concept of NBS has become an interesting research topic regarding a wide range of real-life situations [7]. In the proposed Blotto game model, the $\mathbb{S}^{SU}$ also tries to maximize $\mathcal{U}_{SU}(\mathbb{P},\mathbb{I})$ based on the NBS approach. Therefore, the main goal of SU can be expressed as follows.

$$\max \mathcal{U}_{SU}(\mathbb{P},\mathbb{I}) \cong \max_{g_i} \prod_{1\le i\le m} g_i \cong \max_{g_i} \prod_{1\le i\le m} (g_i - d_i), \text{ where } d_{i,1\le i\le m} \in d \quad (7)$$

where d is a disagreement vector $d = (d_1, .. d_m) \in \mathbb{S}^{SU}$ and a disagreement point $d_{i,1\le i\le m}$ represents a minimum payoff of each channel. Therefore, d is a set of least guaranteed payoffs for a defender.

Usually, the NBS is conventionally found based on an exhaustive search, i.e., all feasible payoff pairs in $\mathbb{S}^{SU}$ are examined. However, the exhaustive search becomes considerably inefficient when the amount of resources and number of m increase. In addition, a solution to security problems should be obtained in real time. Therefore, computing an optimal NBS solution is challenging because of the complexity of exponential computations [11]. Another weak point of traditional NBS is that it requires complete information; game players are assumed to know everything to maximize their payoffs. However, in reality, this assumption rarely holds. Occasionally, game players make decisions irrationally because of limited information about available strategies [11].

To overcome the aforementioned problems, we decompose the feasible payoff set into smaller sub-feasible sets, and then approximate the NBS by iteratively applying the learning approach in each sub-feasible payoff sets. Initially, the SU in the proposed scheme makes a decision based on less-than perfect information. However, under the current system situation, the SU has the capability of deciding intelligently by self-adapting to the dynamics of the IoT environment, while considering the experience gained under past and present system states, and using long term benefit estimations. Therefore, our iterative learning approach can considerably reduce computation complexity compared to that in a conventional method in which the SU bargains over the entire feasible payoff set to approximate the NBS [11]. For these reasons, the proposed scheme can obtain globally desirable properties such as adaptability to approximate an optimal solution, flexibility and effectiveness for real-world IoT system dynamics.

Based on the feedback learning process, the proposed Blotto game model can capture the means by which the SU adapts his strategy to achieve a better payoff. This procedure is defined as a strategic power allocation algorithm to secure IoT communications. At the initial game iteration (t = 1), the power is equally distributed to m fallow channels. The obtained $\mathcal{U}_{SU}^{t=1}(\mathbb{P},\mathbb{I})$ value is considered the disagreement vector for the next sub-solution ($\mathcal{U}_{SU}^{t=2}(\mathbb{P},\mathbb{I})$). Correspondingly, the lth sub-solution ($\mathcal{U}_{SU}^{t=l}(\mathbb{P},\mathbb{I})$) is computed by considering the (l – 1)th sub-solution ($\mathcal{U}_{SU}^{t=l-1}(\mathbb{P},\mathbb{I})$). Based on this iterative learning mechanism, the desirable lth sub-feasible payoff $\mathcal{U}_{SU}^{t=l}(\mathbb{P},\mathbb{I})$ can be defined as follows.

$$\mathcal{U}_{SU}^{t=l}(\mathbb{P},\mathbb{I}) = \left\{ \left(f_{k,1\le k\le m}^{t=l}(p_k,\mathcal{I}_k)\right) \in \mathbb{R}_{+}^{m} \left| \sum_{k=1}^{m} p_k^{t=l} \le \mathcal{P} \text{ and } \mathcal{U}_{SU}^{t=l-1}(\mathbb{P},\mathbb{I}) < \mathcal{U}_{SU}^{t=l}(\mathbb{P},\mathbb{I}) \right. \right\} \quad (8)$$

s.t., $\mathcal{U}_{SU}^{t=l}(\mathbb{P},\mathbb{I}) \in \mathbb{S}^{SU}$ and $\mathbb{R}_{+}^{m}$ denotes a set of non-negative real number.

where $f_k^{t=l}(\cdot)$, $p_k^{t=l}$ are the *l*th iteration payoff and allocated power of the *k*th channel, respectively. From the feasible payoff set ($\mathbb{S}^{SU}$) of all possible SU's payoff pairs, $\mathcal{U}_{SU}^{t=l}(\mathbb{P},\mathbb{I})$ is decided. However, the exact information regarding $(\mathcal{I}_1^{t=l},\mathcal{I}_2^{t=l},\cdots,\mathcal{I}_m^{t=l}) \in \mathbb{I}$ is not known at the $(p_1^{t=l},p_2^{t=l},\cdots,p_m^{t=l}) \in \mathbb{P}$ decision time. Therefore, under dynamically changing IoT environments and limited information, the SU's optimal solution according to (7) cannot be obtained. To solve this problem, we apply an iterative learning approach in a step-by-step manner. At the end of each game iteration, the SU evaluates his current payoff ($\mathcal{U}_{SU}(\mathbb{P},\mathbb{I})$) in each sub-feasible payoff sets, and the disagreement vector *d* is updated as follows.

$$\begin{cases} d = (d_1,..d_m) = \left(p_1^{t=l},p_2^{t=l},\cdots,p_m^{t=l}\right), & \text{if } \mathcal{U}_{SU}^{t=l-1}(\mathbb{P},\mathbb{I}) < \mathcal{U}_{SU}^{t=l}(\mathbb{P},\mathbb{I}) \\ d = (d_1,..d_m), & \text{otherwise, } d \text{ is not changed} \end{cases} \quad (9)$$

Therefore, the obtained $\mathcal{U}_{SU}(\mathbb{P},\mathbb{I})$ is used to generate a power allocation decision for the next game iteration. This interactive feedback process continues iteratively until the equilibrium status is obtained. It may be the only realistic approach to solve complex and dynamic IoT security problems.

In the proposed model, the SU's payoff $\mathcal{U}_{SU}^{t=l}(\mathbb{P},\mathbb{I})$ at the *l*th iteration is obtained through online computations where decisions must be generated in real time without securing information about the future. According to our online method, the $\mathcal{U}_{SU}^{t=l}(\mathbb{P},\mathbb{I})$ is strongly influenced by the SU's and jammer's previous strategies such as $S_{jammer}^{t=l-1} = (\mathcal{I}_1^{t=l-1},\mathcal{I}_2^{t=l-1},\cdots,\mathcal{I}_m^{t=l-1})$ and $S_{SU}^{t=l-1} = (p_1^{t=l-1},p_2^{t=l-1},\cdots,p_m^{t=l-1})$. It means that the jammer's strategy ($S_{jammer}^{t=l-1}$) is the factor in the SU's decision for the next iteration. In this study, we employ the *higher weighted, more preferential* rule for the power resource allocation problem. To implement this rule, five steps in each game iteration are employed. First, the SU calculates his payoff $\mathcal{U}_{SU}(\mathbb{P},\mathbb{I})$ according to (6) and then selects the lost channels (e.g., $f_{k,1\le k\le m}(p_k,\mathcal{I}_k) = 0$). Second, these selected channels are decreasingly sorted according to their weighted factors (α). Third, the allocated power resource for each selected channel is dynamically re-allocated; the adjusted power amount for the channel with the highest α value is given by.

$$p_k^{t=l} = \frac{\alpha_k}{\sum_{j\in\mathbb{F}}\alpha_j} \times T_R \times \beta, \text{ s.t., } T_R = \sum\nolimits_{j\in\mathbb{F}} p_j^{t=l-1} \text{ and } \beta = 1 + \frac{(\mathcal{I}_k^{t=l-1} - p_k^{t=l-1})}{p_k^{t=l-1}} \quad (10)$$

where $\mathbb{F}$ is the set of lost channels. T_R is the total allocated power resource in $\mathbb{F}$ and β is a control factor to adjust the allocating power amount. Fourth, the next higher α value channel in $\mathbb{F}$ is selected for the power reallocation. During the sequential power reallocation, it is possible that some lower α value battlefields cannot get the enough power resource due to the resource scarcity. Finally, after the power resource reallocation process, the SU's payoff of next iteration ($\mathcal{U}_{SU}^{t=l}(\mathbb{P},\mathbb{I})$) is obtained according to (8).

3.3 The Main Steps of the Proposed Algorithm

As the sophistication of the attacks as well as the cost of their prevention increase, security problems in IoT systems become increasingly pressing each year. Several jamming detection techniques have been developed to increase the security of sensitive CR-based IoT communications, and many studies have sought methods to optimize the use of available security resources [12], [13]. In this study, we examine the problem of adaptive power resource allocation to detect potential jamming attacks in CR fallow channels. In the proposed scheme, a jammer attempts to harm these CR fallow channels and the SU dynamically allocates his power resources to protect these fallow channels. Based on the interactive feedback process, the SU adaptively re-allocates these limited power resources in a step-by-step manner. The main steps of the proposed strategic power allocation scheme are given next.

Step 1: At the initial game iteration, the power resource of SU is equally distributed. This starting guess guarantees that each fallow channels enjoys the same benefit at the beginning of the game.

Step 2: The iterative sub-solution algorithm begins by considering the previous sub-feasible payoff set $\mathcal{U}_{SU}$. In the lth iteration, the disagreement vector ($\boldsymbol{d}$) is the obtained sub-solution ($\mathcal{U}_{SU}^{t=l-1}(\mathbb{P},\mathbb{I})$) at the previous ($l$– 1) iteration.

Step 3: Each game iteration, the SU calculates his payoff $\mathcal{U}_{SU}(\mathbb{P},\mathbb{I})$ according to (6), and selects the lost channels (e.g., $f_{k,1\leq k\leq m}(p_k,\mathcal{I}_k)=0$).

Step 4: The selected lost channels are decreasingly sorted according to their weighted factors (α).

Step 5: Based on the α, β and T_R values, the allocated power resource for each selected lost channel is dynamically re-allocated according to (10).

Step 6: After the resource reallocation process, the $\mathcal{U}_{SU}$ for next iteration is obtained according to (6). If the currently estimated $\mathcal{U}_{SU}$ is better than the previous iteration $\mathcal{U}_{SU}$, $\boldsymbol{d}$ vector is adjusted according to (9).

Step 7: To adapt the IoT system dynamics, the dynamic power allocation process is iteratively applied in each sub-feasible payoff sets in a step-by-step manner. This interactive approach is suitable in real world operations to approximate an optimal solution of the Equation (7)

Step 8: If a new obtained $\mathcal{U}_{SU}$ is a status quo (i.e., the change of $\mathcal{U}_{SU}$ is within a pre-defined minimum bound (ε)), we assume that the security level of IoT system reaches to an efficient stable state; the game process is temporarily stop.

Step 9: Under widely diverse environments, the SU is self-monitoring constantly to estimate the current IoT system situation; If $(\mathcal{I}_1,\mathcal{I}_2,\cdots,\mathcal{I}_m)\in\mathbb{I}$ is thoroughly changed and the currently estimated $\mathcal{U}_{SU}$ decreases by more than ε, the power re-allocation algorithm is re-triggered, and back to the Step 2 to obtain a new solution.

4. Performance Evaluation

In this section, we describe the effectiveness of the proposed scheme based on a conducted simulation. Using a simulation model, we compared the performance of the proposed scheme with the existing schemes described in [2], [4], [9] to validate the superiority of our approach. For our performance evaluation, experimental scenarios of the analyzed problem depend on a set of parameters that affect both the performance of the algorithm as well as the quality of the generated solution. The assumptions implemented in the simulation model are described as follows.

- The simulated model assumes that one attacker (i.e., jammer) and one defender (i.e., secondary user) exist.
- The amount of power resources for the attacker and defender ($\mathfrak{T}$ and $\mathcal{P}$) are 100 mW and 300 mW, respectively.
- We set ε = 0.1× max ($\mathcal{U}_{SU}$) and, for simplicity, Γ and σ are set as 1.
- The number of fallow channels (m) is varied from 5 to 20.
- Performance measures obtained based on 50 simulation runs are plotted as a function of the offered number of fallow channels (m).
- At each iteration, $\mathbb{P}$ and $\mathbb{I}$ are dynamically changeable.
- To simplify analysis, we assume the absence of any outbreak situation in the experiments.

Performance measures obtained through simulation are normalized values of SU's payoff, security efficiency and the percentage of payoff decrease. The recently developed, the *BGPA* [2], *CRAJ* [4], and *RLAJ* schemes [9] have introduced unique challenges for solving security problems in CR communications. To confirm the superiority of our proposed approach, we compare the performance of the proposed scheme with those of existing schemes.

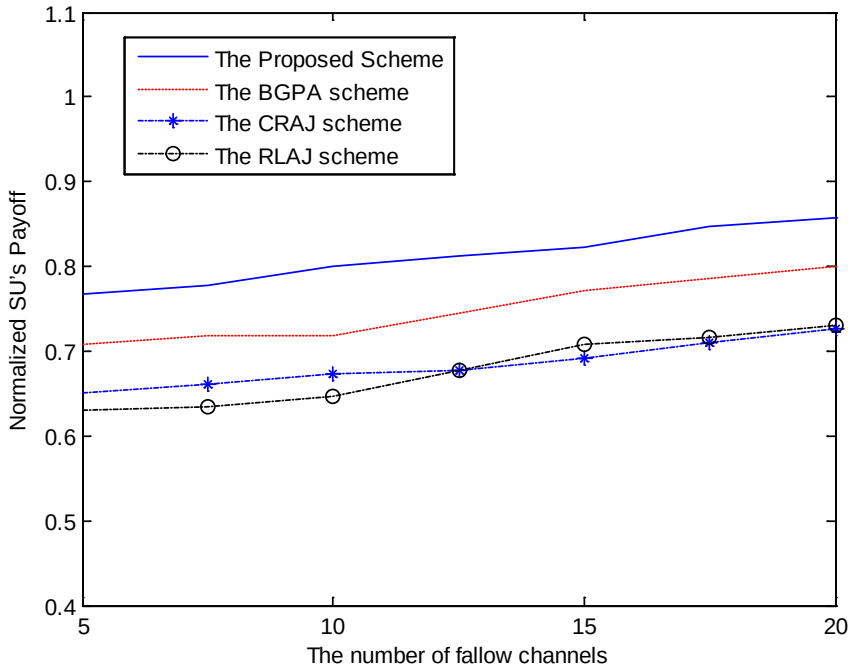

Fig. 1. Normalized SU's Payoff

Fig. 1 shows the performance comparison for the normalized SU's payoff. This is the $\mathcal{U}_{SU}(\mathbb{P}, \mathbb{I})$ value for each CR communication in IoT systems. To estimate the system's performance, SU's payoff is an important metric. In widely diverse IoT environments, our game-based strategic power allocation approach can result in a higher payoff for the SU. **Fig. 1**, shows that our proposed scheme effectively manages the damage caused by the jammer and maintains a better SU' payoff than do other existing schemes.

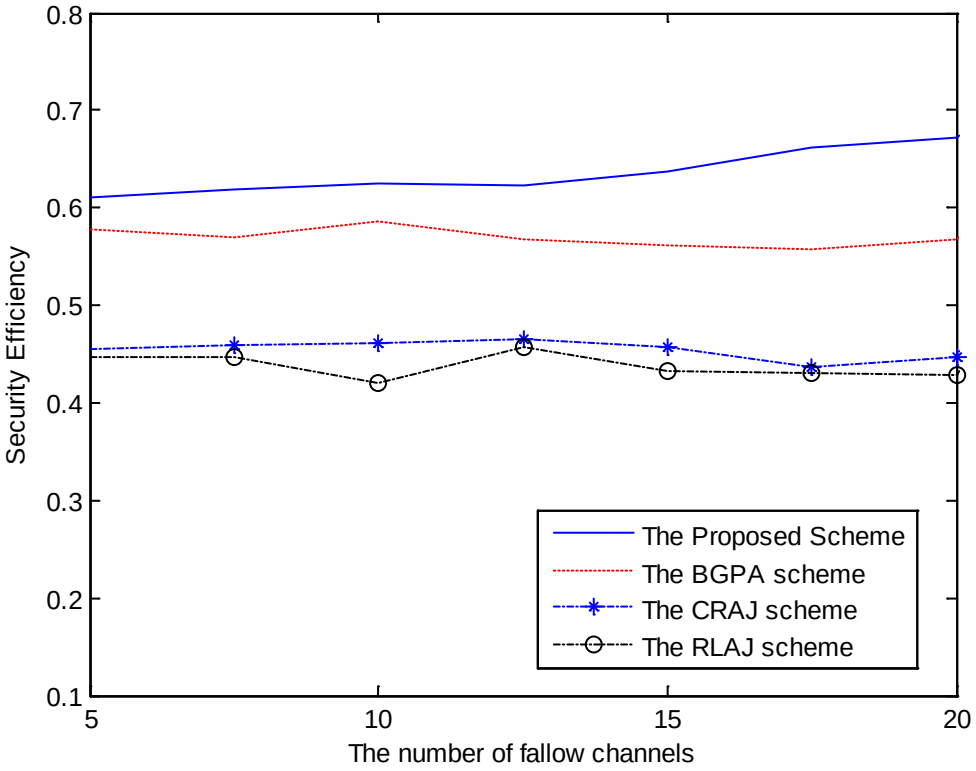

Fig. 2. Security Efficiency

Fig. 2 presents a performance comparison in terms of security efficiency. Usually, security efficiency is quantified as the congruence between requested security levels and obtained security levels. In this study, it is quantified as the ratio between total requested weighted factor values (α) for channels and totally obtained weighted factor values of fallow channels. All the schemes show similar trends. However, considering various numbers of fallow channels, the security efficiency of the proposed scheme is considerably better than in other existing schemes.

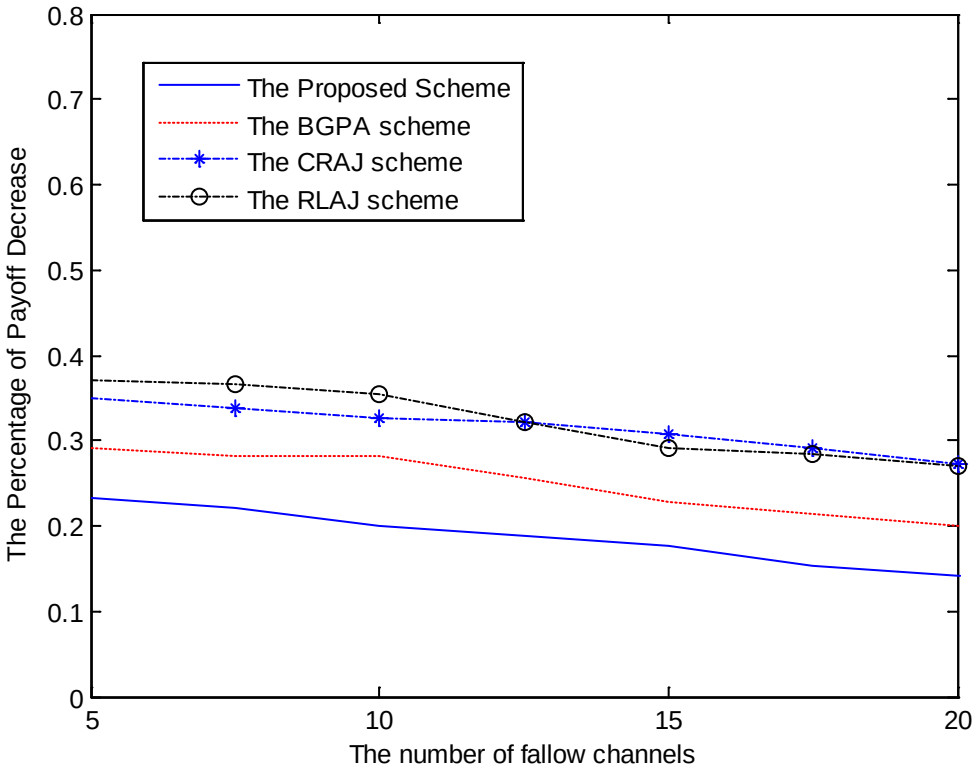

Fig. 3. The Percentage of Payoff Decrease

The curves in **Fig. 3** show the percentage of payoff. This result rationally represents that the ratio of SU's payoff decreases because of jamming attacks. It helps explain the effectiveness of each scheme in minimizing damage from an attacker. To approximate an optimal solution, the proposed scheme adaptively re-allocates the power resource in a step-by-step manner. From the simulation result, we can observe that the proposed scheme perform extremely well compared to other schemes.

Simulation results obtained from **Fig. 1-3** show that the proposed scheme generally exhibits superior performance compared with the other schemes when many different fallow channels are involved. Because of our adaptive game approach, the proposed algorithm constantly monitors current IoT system conditions and iteratively adapts the system dynamics more effectively than the other schemes in [2], [4], [9].

In this study, we do not emphasize obtaining an optimal solution based on the traditional approach. Instead, an adaptive interactive learning model is proposed. This approach can dramatically reduce computational complexity and overhead. Usually, the traditional optimal solutions require exponential time complexity. However, our proposed approach only requires polynomial time complexity. This feature means our model is practical in real-world operations.

5. Summary and Conclusions

In this study, we investigated the cognitive radio anti-jamming problem in IoT systems. By considering the interaction between the SU and jammer, we converted the anti-jamming power allocation problem to a two-player Blotto game. To approximate the efficient system equilibrium status, the iterative NBS technique was adopted to solve the developed Blotto game model. By constantly monitoring the current IoT system condition, the proposed scheme dynamically re-negotiates the current strategy in a step-by-step manner and can re-allocate the SU's power as efficiently as possible to ensure IoT communication security. In this manner, we can obtain a feasible and efficient solution to provide secure CR communications in IoT systems. Finally, simulation results verified the excellent performance of the proposed scheme. By analyzing simulation results, we conclude that the proposed scheme can address the strategic power allocation problem more effectively than other existing schemes. For future research, our iterative game approach can be generalized to model various defense mechanisms, and can be extended to address different security provisioning problems in dynamic environments.

References

[1] Aijaz, A. and Aghvami, A.H., "Cognitive Machine-to-Machine Communications for Internet-of-Things: A Protocol Stack Perspective," *IEEE Journal of Internet of Things, Accepted for publication in 2015*. Article (CrossRef Link).

[2] Yongle Wu, Beibei Wang and Liu, K.J.R., "Optimal power allocation strategy against jamming attacks using the Colonel Blotto game," *IEEE GLOBECOM'2009*, pp.1-5, 2009. Article (CrossRef Link).

[3] Beibei Wang, Yongle Wu, Liu, K.J.R. and Clancy, T.C., "An Anti-Jamming Stochastic Game for Cognitive Radio Networks," *IEEE Journal on Selected Areas in Communications*, vol.29, no.4, pp.877-889, 2011. Article (CrossRef Link).

[4] Yongle Wu, Beibei Wang, Liu, K.J.R. and Clancy, T.C., "Anti-Jamming Games in Multi-Channel Cognitive Radio Networks," *IEEE Journal on Selected Areas in Communications*, vol.30, no.1, pp.4-15, 2012. Article (CrossRef Link).

[5] A. H. Fares, M. I. Sharawy and H. H. Zayed, "Intrusion Detection: Supervised Machine Learning," *Journal of Computing Science and Engineering, vol.5, no.4*, pp.305-313, 2011. Article (CrossRef Link).

[6] Taeho Kang, Xiang Li, Chansu Yu, and Jong Kim, "A Survey of Security Mechanisms with Direct Sequence Spread Spectrum Signals," *Journal of Computing Science and Engineering*, vol.7, no.3, pp.187-197, 2013. Article (CrossRef Link).

[7] Sungwook Kim, "Cellular network bandwidth management scheme by using Nash bargaining solution," *IET Communications*, vol. 5, Issue 3, pp. 371 – 380, 2011. Article (CrossRef Link).

[8] M. D. Wittman, "Solving the Blotto Game: A Computational Approach," *MIT working paper*, 2011. Article (CrossRef Link).

[9] Singh, S. and Trivedi, A., "Anti-jamming in cognitive radio networks using reinforcement learning algorithms," *IEEE WOCN'2012*, pp.1-5, 2012. Article (CrossRef Link).

[10] D. Korzhyk, V. Conitzer and R. Parr, "Security Games with Multiple Attacker Resources," *IJCAI'11*, pp.273-279, 2011. Article (CrossRef Link).

[11] E. Kim, H. Park and P. Frossard, "Low complexity iterative multimedia resource allocation based on game theoretic approach," *IEEE ISCAS*, pp.1099-1102, 2012. Article (CrossRef Link).

[12] O. Vanek, Z. Yin, M. Jain, B. Bosanský, M. Tambe, and M. Pechoucek, "Game-theoretic resource allocation for malicious packet detection in computer networks," *AAMAS'2012*, pp.905-912, 2012. Article (CrossRef Link).

[13] Jungwoo Ryoo and Eun-A Park, "Internet Security Readiness: The Influence of Internet Usage

Level and Awareness on Internet Security Readiness Capital, Skill, and Actual Uptake/Use of Infrastructure," *Journal of Computing Science and Engineering*, *vol.5*, *no.1*, pp.33-50, 2011. Article (CrossRef Link).

Sungwook Kim received the BS, MS degrees in computer science from the Sogang University, Seoul, in 1993 and 1995, respectively. In 2003, he received the PhD degree in computer science from the Syracuse University, Syracuse, New York, supervised by Prof. Pramod K. Varshney. He has held faculty positions at the department of Computer Science of ChoongAng University, Seoul. In 2006, he returned to Sogang University, where he is currently an associate professor of department of Computer Science & Engineering, and is a research director of the Internet Communication Control research laboratory (ICC Lab.). His research interests include resource management, online algorithms, multimedia network management, bandwidth allocation, adaptive QoS control and game theory for wireless network management.