Spoofing Attack and Surveillance Game in Geo-location Database Driven Spectrum Sharing

Nhan Nguyen-Thanh, Duc-Tuyen Ta, van Tam Nguyen

Spoofing Attack and Surveillance Game in Geo-location Database Driven Spectrum Sharing

Nhan Nguyen-Thanh[1], *Duc-Tuyen Ta*[1], *Van-Tam Nguyen*[1]

[1] *LTCI, CNRS, Télécom ParisTech, Université Paris Saclay, 75013, Paris, France.*
** E-mail: duc-tuyen.ta@telecom-paristech.fr*

Abstract: The geo-location database (GDB) driven is the enforcement method for dynamic spectrum sharing in TV White Space and 3.5 GHz spectrum bands, as well as a preferred option for the other spectrum sharing applications. Although providing accurate and reliable spectrum information services, the GDB driven spectrum sharing suffers from a critical security threat of spoofing attack. Under a spoofing attack, an adversary could spoof either the identification (ID) or the location information in its request messages. This breaks the fairness and reduces the efficiency of the GDB driven spectrum sharing system. In order to counteract the location and ID spoofing attacks, we consider the location verification of request messages and the ID verification of communicating data. Because a resource manager and an adversary are independent and self-interested, we formulate two corresponding surveillance games to analyze the conflict interaction between spoofing attack and the countermeasures. By expressing the surveillance game on requests' location in a strategic form and representing the surveillance game on data ID in a sequence form, we find out Nash equilibrium. The analytical and numerical results show that a resource manager can mitigate the spoofing attack by adequately adapting its penalty policy and surveillance strategy.

1 Introduction

Allocating spectrum resource, which is naturally scarce, in a conventionally static manner can lead to a spectrum underutilization up to 85% [1]. Dynamic spectrum access (DSA) to licensed spectrum bands has been proposed to enhance the spectrum utilization. In order to implement DSA, secondary users must be able to adapt their transmission parameters to exploit the spectrum utilities. Determining accurate and reliable spectrum opportunities is, therefore, essential and still a very challenging problem. Three main approaches for determining spectrum opportunities are beacon signal-based[12], spectrum sensing-based [23], and geo-location database (GDB) driven-based [17]. In the beacon signal-based approach, licensed users broadcast information about spectrum holes in their beacon messages. However, this approach requires considerable changes in the existing primary systems. In the spectrum sensing-based method, primary system's activity is explored by measuring the radio environment spectrum. However, the rapid change and complexity of radio propagation environment due to shadowing and fading bring in too many uncertainties, leading to low sensing accuracy. In the GDB driven-based approach, a coordinator for the coexistence between primary systems and secondary systems is introduced. The coordinator is essentially a database server which contains an online geo-location map of spectrum usage. It is responsible for managing the spectrum allocation to secondary networks. Whenever a network or a user has demand to use spectrum, it will send to the resource manager a request which contains its geo-location information. The spectrum server/coordinator optimizes the allocation as well as the corresponding transmission parameters of the available spectrum bands and provides the detailed configuration to the requester. Compared to other approaches, the GDB driven is more accurate and reliable [17]. Therefore, in 2012, FCC enforces to adopt the GDB driven approach for exploiting DSA in the TV White Space and the 3.5 GHz CR systems [8].

The key point for implementing GDB driven method is the availability and the accuracy of the information of devices' location. Considerable interference on both primary and secondary systems will appear if the location information of the users is inaccurate. Moreover, unfair spectrum allocation will happen if adversaries intentionally spoof request messages with either faked identification (ID) or faked location information. Therefore, spoofing attack is a critical vulnerability of the GDB driven-based DSA system. However, to the best of our knowledge, there is no work systematically examining the impacts of spoofing attacks in GDB driven-based DSA. The most relevant related work which considers the GPS spoofing attacks in a GDB driven cognitive radio (CR) network is presented in [24], but limited due to the impact of false localization from the attacked GPS signals. Other researches on the security problem in database-driven systems mostly focus on location privacy [2, 9, 22].

In this paper, we consider a general view of spoofing attacks in GDB driven DSA, which occur in the ID and the location information of request messages. We classify the request messages consisting of spoofing information into accidental, malicious and selfish categories. An *accidental spoofing request* occurs when the sender is not aware of the incorrectness of its location information due to either a malfunctioning or an attack problem (similar to [24]). A *malicious spoofing request* comes when the sender intentionally provides false location information for causing more interference to the whole system. Finally, a *selfish spoofing request* appears when the sender abusively queries for more spectrum resources under faked ID. In order to counteract these spoofing attacks, we consider two surveillance processes corresponding to the ID and the location information in the request messages. However, implementing surveillance processes in a DSA system, where various networks coexist, is costly and complicated. Thus, a key question that needs to be investigated is when to implement the above surveillance processes.

As a resource manager and an attacker are independent but always have opposing benefits and interactions, to study the problem, we adopt game theory, which is a mathematical tool of conflict analyzing among independent, self-interested players [20] and has been adopted in many similar DSA problem [7, 19]. Two surveillance games on request location verification and data traffic identification will be formulated. Hence, we leverage and amplify our previous work on surveillance game [5, 18] for this work. It has been proven that a relevant strategy for all players of a certain game is the Nash equilibrium (NE) points [10]. Therefore, a resource manager

enforces attacker to reduce the number of spoofing attacks by performing surveillance processes according to NE at an appropriate penalty.

The remainder of the paper is organized as follows. In Section II, we discuss the detailed of the GDB driven based DSA system and the spoofing attack problem. In Section III, we describe the system model of the investigated DSA system. The request location verification game and the data traffic identification game for detecting spoofing attacks are investigated in Section IV and Section V, respectively. Numerical results and the corresponding interpretations are presented in Section VI. Finally, we conclude the paper in Section Section VII.

2 Database-driven spectrum sharing and spoofing attack problem

2.1 The geo-location database-driven CR system

During the last fifteen years, there is a strong effort of wireless communication community on developing a CR for improving spectrum resource utilization which is wasted due to the traditional fixed allocated approach. DSA is the target as a needed capability for a new developed system which satisfies the above desire. Initially, there are several proposals such as spectrum sensing, GDB driven spectrum sharing, etc., considered as the candidates for implementing DSA on TV white space spectrum, an experimental primary goal.

In 2012, the FCC rules [8] have made spectrum sensing optional in white space networks. Instead, the rules require white space devices (WSDs) to learn spectrum availability at their corresponding locations from a central database of incumbents. In general, the database is required to store an up-to-date repository of incumbents, including television stations and in certain cases, wireless microphones, and use this information to determine white space availability at a WSD's location. The system operates based on the location information and the database system, thus is called the GDB driven spectrum sharing. In particular, whenever a user has a demand to use channels it should send a request to Database Service Provider (DSP) to acquire channel resource. The DSP, which plays the important role of a resource manager, will assign the available channels to the user and charge using fee.

Let's consider two famous GDB driven DSA standards, IEEE 802.19 [14] and 802.11af [13]. In IEEE 802.19, DSP is CDIS (coexistence discovery and information server), and a network object (NO), i.e., a device or a group of devices, must includes either a fixed or a mode II-FCC master device. A mode II-FCC device is a portable device that has internal geo-location capabilities and can access a database of channels in use to load availability information for its current location. This loading service can be performed through a direct wireless connection to the server or through a backhaul connection. In mobility use case, the location and mobility information should be updated at least every 60 seconds. In 802.11af, DSP is GDB. This means that the location of users must be known to ensure a good channel assignment such that there is no interference to primary system. Access points and stations determine their position using a satellite positioning system (e.g., Global Positioning System - GPS) and use the Internet to query a GDB provided by a regional regulatory agency to discover which frequency channels are available for use at a given time and position. In summary, the model of GDB driven DSA systems are illustrated in Fig. 1.

2.2 Spoofing attacks and defending strategies in geo-location database-driven spectrum sharing

As location information is a prerequisite for the operation of GDB driven spectrum sharing, any attacks which influence on its accuracy could severely degrade the operation of the whole system. Analyzing such the security threats and their corresponding countermeasures is, therefore, a need.

In a GDB driven DSA system, when a user wants to register for operation or to update new location or to query for spectrum bands, it must send a request to a resource manager. The request

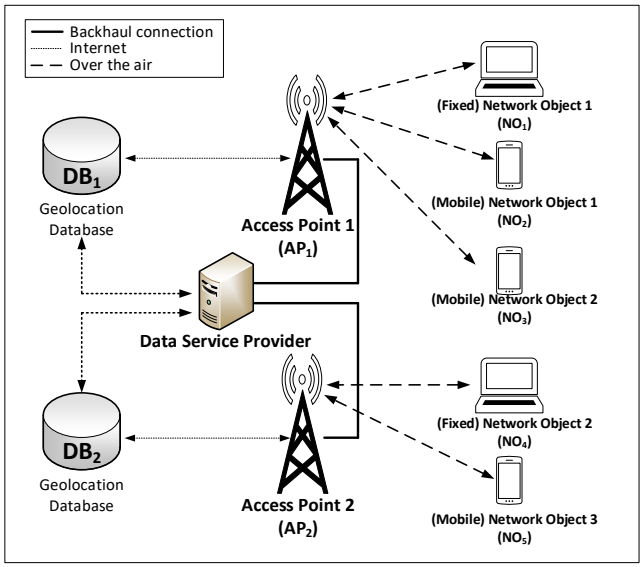
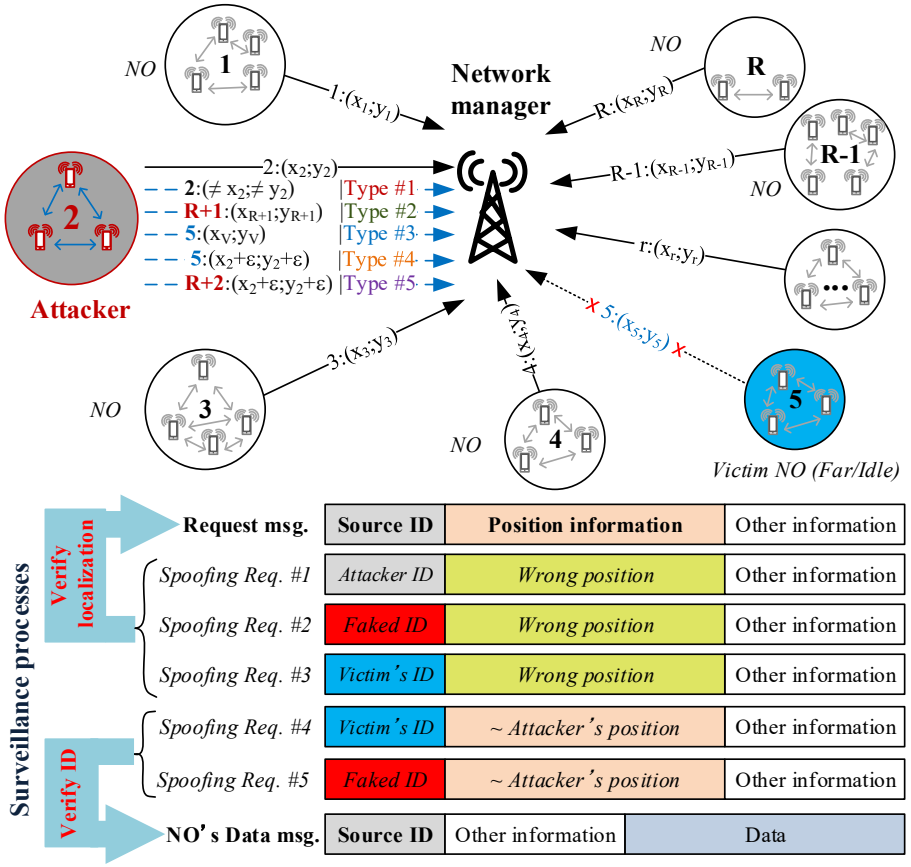


Fig. 1: Example of GDB Driven based DSA system.

messages usually contain the physical/network ID and the location of the user. The general format for a request message is presented in Fig. 2. Due to the flexibility of the software-defined radio, either ID or location information could be spoofed. For example, the attacker can use the GPS spoofing attack by broadcasting incorrect GPS signals or by rebroadcasting genuine signals captured elsewhere or at a different time to fake the estimated location of other users [24]. In addition, some communication protocols do not provide mechanisms for authenticating the source or destination of a message, such as the protocols in the TCP/IP suite or the Voice over IP (VoIP), then allow users/callers to forge ID information and present false names and numbers [3, 6]. The attacker hence can spoof the ID (ie.e, uses a fake ID or uses the ID of other users) to attack the network. According to spoofed contents, we categorize the spoofing requests into five types as illustrated in Fig. 2. Due to the variety of purposes and contents of spoofing requests, there are possibly several countermeasures. To achieve a systematical approach, we remark that the spoofing attack only locates at the location and the ID information. Therefore, we propose a surveillance process which includes two complementing steps: the *request location verification* and the *spectrum user's identification* to deal with the location and ID spoofing attacks, respectively (Fig. 3). The 2-steps verification process is issued in details as follows:

- **Request location verification**: for the location spoofing attack, we propose to implement a location verification process. Positioning methods based on receive signal strength, time of arrival, added sensor networks, etc., can be used to determine the deriving position of the request. If there is a mismatch between the estimated location and the location information in the request message, the location spoofing attack is detected. The request will be ignored and a further penalty is imposed on the attacker. In practice, because of the variation of radio environment and the characteristic of positioning methods, there is always a limitation on localization accuracy. Hence, the efficiency of this surveillance step is limited to a distance, called an *undetectable radius*. Any difference distance between the real position and the location information in the request smaller than the undetectable radius cannot be discovered.
- **Spectrum user's identification**: in order to provide complementing counteractions for the above step, we propose to perform a second surveillance process. The extra surveillance at a small area inside an undetectable radius is conducted by scanning allocated spectrum bands to determine who is using the resource. The reason is that the user must reveal it physical ID to transmit its own data through any communication links. If the spectrum bands are not occupied, then the attack is malicious and the frequency resource is



Attack type	Details	Objectives	Spoofing	Surveillance Process
Type 1	A user which has a localizing malfunction or suffers from an outside adversary localizing attack, e.g., the spoofing attack on GPS signals.	**Malicious spoofing request**: reduces the probability of receiving spectrum allocation at the attacked location. Selfish attacking request. **Selfish spoofing request**: queries spectrum bands at a specific location for using in future.	Location	Verify location
Type 2	An adversary spoofs a registration for anew ID at an arbitrary location.	**Malicious spoofing request**: reduces spectrum resource opportunity at a specific location. **Selfish spoofing request**: illegally occupies spectrum resource if the wrong location is close to its real location.	Location	Verify location
Type 3	An attacker overlaps and replaces the request of a (victim) user by a spoofed location one.	**Malicious spoofing request**: causes interference to the victims. **Selfish spoofing request**: virtually moves the position of the victim in the database to a position outside the area of the attacker and increases the spectrum opportunity for the attacker.	Location	Verify location
Type 4	An attacker overlaps and replaces the request of a far or idle user to query fora spectrum band at the location of the attacker	**Selfish spoofing request**: thieves spectrum resource of a victim user who can be either afar (outside the area of the attacker) or an idle(inactive) user.	ID	Verify ID
Type 5	An attacker uses faked IDs for registering and querying for spectrum bands.	**Selfish spoofing request**: registers and queries for spectrum bands through a fake ID could help the attacker occupies more resources.	ID	Verify ID

Fig. 2: Types of spoofing attack and surveillance process in geo-location database-driven spectrum sharing

rearranged for other requests. If the spectrum bands are occupied by mismatching users, the selfishly spoofing attack (i.e., type 4 and 5), therefore, can be detected and punished accordingly.

3 System model

We consider a GDB driven spectrum sharing system which supports the coexistence among several independently controlled cognitive radio networks. By using geo-location awareness and maintaining information databases, the system could perform licensed bands sharing for local CR networks. The operation of the considered system is similar to that proposed in the standard IEEE 802.19.1 which manages CR wireless networks operating in TV White Space. The proposed system includes two separating sets: 1) a resource manager (RM) and 2) network objects (NOs). The resource manager is responsible for i) collecting spectrum usage information, ii) gathering registrations, geo-location information and requests of NOs, iii)

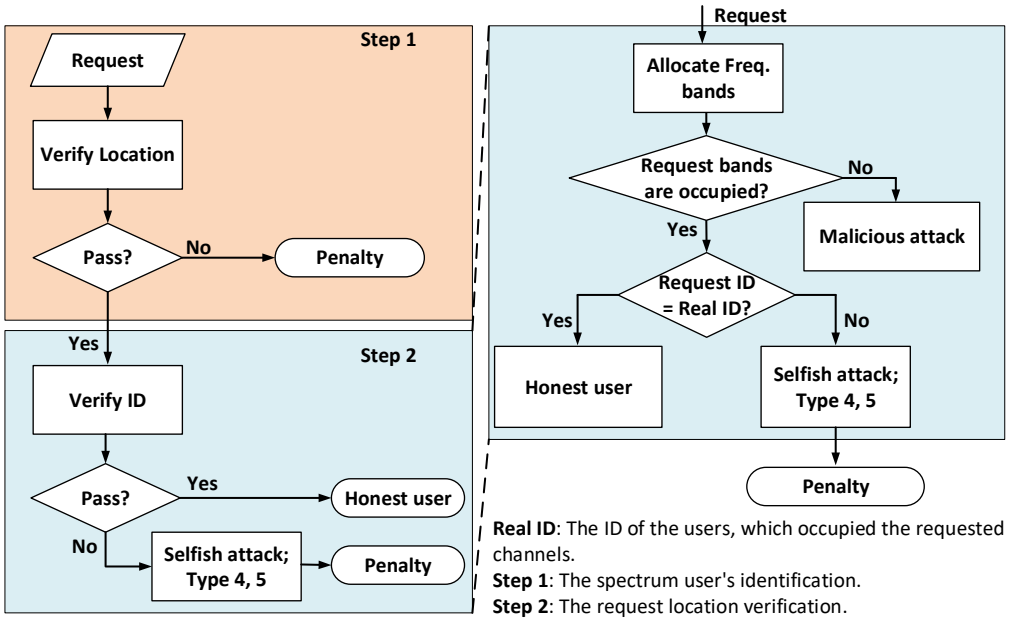


Fig. 3: The 2-steps verification process to deal with the location and ID spoofing attacks on the GDB spectrum sharing system.

managing and allocating spectrum bands and the transmitting configurations to NOs, and iv) monitoring and controlling to ensure the correctness of the system operation. An NO could be either a CR device or a local network of CR devices. The accesses to spectrum bands of NOs is under the control of the resource manager. Location information of NOs is the prerequisite for RM to allocate spectrum and corresponding transmitting configurations. Hence, each NO must include either a fixed master device which is location-aware and able to query RM database frequently to retrieve spectrum allocated to their location, or a portable master device which has an internal geo-location capability, i.e., similar to an FCC mode II TV band device, and frequently updates its geo-location to RM. We aim at a geo-location database-driven spectrum sharing system which supports mobile NOs. Therefore, the registering, location updating and spectrum band querying requests are performed frequently through wireless connections. After receiving NOs' requests, RM will optimize and assign the spectrum bands and transmitting configurations for NOs. Without loss of generality, we assume that the quality of spectrum bands is the same and only one spectrum band is allocated to one NO. Due to the flexibility of cognitive radio, an NO or an attacker could easily spoof their requests in both ID and location fields as shown in Fig. 2. Thus, we assume that there are attackers in the spectrum sharing system who want to perform the ID and location spoofing attacks for different purposes as described in the previous subsection. In order to simplify the analysis and focus on the effects surveillance process, we assume that the attacker performs the spoofing attack for selfish purpose.

To combat these spoofing attacks, the RM utilize its infrastructures, which include base stations, additional sensor networks, etc., for monitoring the control channel to localize sending locations of requests, and to scan data traffic on assigned spectrum bands to detect illegal occupations. The surveillance process includes a data traffic identification and a location verification steps, which support each other so that the spoofing attack is eliminated as much as possible. Since there are the trade-off between the objective of the attacker and the network manager, game theory, which mathematically studies the interaction among independent, self-interested players, helps to formulate our problem. In the next two sections, we formulate two games that describe the interaction of the two surveillance steps with attacking strategies. The details of these formulations will be presented as follows.

4 Request Location Verification Strategies

For the spectrum sharing systems, mobile NOs sent the request messages to RM over the wireless connections. Hence, it is possible to estimate the location of requesters. The estimated location then use to verify the request is location spoofing (i.e., type 1, 2 and 3) or not by comparing it with the location information in the request message. Since the number of active NOs locating in the system can be recorded in history data, we assume that it is a common knowledge of both RM and attacker before a requesting time. The question here is that, for both attacker and RM, what is the optimal number of attacking requests and verification processes?

4.1 Game formulation

To analyze the interaction between the location verification process and the request spoofing attack, we formulate a two players game between a defender and an attacker as follows.

4.1.1 Players:

- **Attacker**, who also is a cognitive user, can spoof and send up to N spoofing requests.
- **Defender**, who represents the resource manager, can perform surveillance up to M locations/request slots (depending on the supporting infrastructure).

4.1.2 Strategies: The pure strategy set of attacker and defender are defined by $\{n, n = 0, 1, ..., N\}$ and $\{m, m = 0, 1, ..., M\}$. Throughout the paper, n denotes the number of spoofing attacks and m represent the number of surveillance. If $n = 0$, attacker does not attack and $m = 0$, defender does not defend.

4.1.3 Payoffs: Let r denote the number of active NOs in the verified area. For each pair of (m, n) given r, the payoff of attacker Π^A and defender Π^D are calculated by:

$$\Pi^A_{m,n,r} = n\,(G - C_A) - \pi_{m,n,r} \tag{1a}$$

$$\Pi^D_{m,n,r} = -mC_S + \pi_{m,n,r} \tag{1b}$$

where G is the benefit of using one allocated band, C_S and C_A denote the costs of implementing the surveillance process and the spoofing attack on one band, and $\pi_{m,n,r}$ represents the expected penalty.

In practice, instead of keeping one pure strategy, attacker and defender could choose their strategy randomly. This forms a mixed strategy for each player. The mixed strategy sets of the attacker and defender are defined by $\{\alpha_n\}$ and $\{\delta_m\}$ where α_n and δ_m are the probabilities of spoofing n users and monitoring m locations. The game between spoofing attacker and defender is now equivalent to a strategic bi-matrix form game with size $N \times M$ as shown in Table 1.

Table 1 Strategic bi-matrix game

		Defender			
		0	***1***	...	***M***
Attacker	***0***	$\left[\Pi^A_{0,0,r}, \Pi^D_{0,0,r}\right]$	$\left[\Pi^A_{1,0,r}, \Pi^D_{1,0,r}\right]$	...	$\left[\Pi^A_{M,0,r}, \Pi^D_{M,0,r}\right]$
	1	$\left[\Pi^A_{0,1,r}, \Pi^D_{0,1,r}\right]$	$\left[\Pi^A_{1,1,r}, \Pi^D_{1,1,r}\right]$	...	$\left[\Pi^A_{M,1,r}, \Pi^D_{M,1,r}\right]$
	...	...	...	...	...
	N	$\left[\Pi^A_{0,N,r}, \Pi^D_{0,N,r}\right]$	$\left[\Pi^A_{1,N,r}, \Pi^D_{1,N,r}\right]$	...	$\left[\Pi^A_{M,N,r}, \Pi^D_{M,N,r}\right]$

The expected payoffs of players are given by:

$$U_A = \boldsymbol{\alpha}^T \boldsymbol{\Pi}_A \boldsymbol{\delta} = \sum_n \alpha_n U_{A|n} = \sum_n \alpha_n \left(\sum_m \delta_m \Pi^A_{m,n,r} \right) \tag{2a}$$

$$U_D = \boldsymbol{\alpha}^T \boldsymbol{\Pi}_D \boldsymbol{\delta} = \sum_m \delta_m U_{D|m} = \sum_m \delta_m \left(\sum_n \alpha_n \Pi^D_{m,n,r} \right) \tag{2b}$$

Obviously, the attacker's payoffs depends not only on its own strategy but also on the defender's strategy, and vice versa. The presence and interaction of defender strongly affect the selection of attacker to optimize its outcome. In turn, the adjustment on attacker's strategies leads to the corresponding reaction of defender's ones. The reasoning of these interactions introduces the equilibrium point which is the intersection of both best response functions of the players. Therefore, NE of the game will be investigated in the next subsection. Also, since the main impact of the network manager on the attackers is the punishment for the captured spoofing attack, penalty policies will be considered as well.

4.2 Penalty policy and Nash equilibrium

4.2.1 Penalty policy: After performing verification process for a request message, if there is a mismatch between the localized position of the sender and the indicated location of the request message content, RM firstly must consider the request as a spoofing one and ignore it. A further penalty time P where spectrum allocation to the attacker is banned should be imposed. Location and ID are the two optional bases for a penalty extracting from a spoofing request. Executing a location-based penalty and an ID-based penalty means that a ban on spectrum resource allocation for a penalty time P is imposed to the localized area of the spoofing request, and to the ID contained in the spoofing request, respectively.

For the location-based penalty option, apparently, RM always ensures that the attacker sending the detected spoofing request must be suffered from a punishment regardless its attack in type 1, or type 2, or type 3. However, other normal NOs located inside the penalized area would be affected. Unfortunately, since an attacker could generate several spoofing requests with different IDs (type 2 and type 3) at one requesting period, it is difficult to distinguish between spoofing IDs and honest IDs. Consequently, the penalty should not be too large for this option. We propose to use a *constant penalty* for a detected area regardless the amount of the detected spoofing requests.

For the ID-based penalty option, a penalty of pending spectrum allocation is imposed on the IDs contained in the detected spoofing requests. Therefore, this kind of punishment will not affect the other honest NOs located inside the undetectable area of an attacker, and the totally nominal penalty on an attacker varies according to the amount of the detected spoofing requests. As the spoofing requests' IDs could not be associated with the attacker, the penalty based on sender's ID is, however, too severe to NOs sending malfunctioning/adversary-attacked requests of type 1, meaningless to the faked IDs in the spoofing type 2, and unfair to the IDs of the victims in the spoofing type 3. In order to validate this penalty option, we propose that RM, instead of explicitly imposing an access-banning time P, performs a further location-reconfirming and authenticating process during a time P. By this way, a malfunctioning/adversary-attacked NO could rapidly correct its location information and receive the allocated spectrum band, whereas an attacker would be busy for answering the location-reconfirming and authenticating process for all of its detected spoofing requests. As a result, the penalty for this option is a detected *amount-related penalty* delay.

In order to determine the expected penalty $\pi_{m,n,r}$, we define $\gamma^{(k)}_{m,r,r}$ the probability of k detected spoofing messages $(0 \le k \le \min(m,n))$ over n attacks. Since the number of combinations for monitoring m requests is $\binom{n+r}{m}$, and the number of having k spoofing attacks in m surveillances is $\binom{n}{k}\binom{r}{m-k}$ for $r \ge m-k$, we have

$$\gamma^{(k)}_{m,n,r} = \begin{cases} 1, & \text{if } m = 0 \\ 0, & \text{if } m > r + k \\ \binom{n}{k}\binom{r}{m-k} \Big/ \binom{n+r}{m}, & \text{otherwise} \end{cases} \tag{3}$$

The probability of capturing at least one attack is the complement of the probability of capturing nothing, i.e., $1 - \gamma^{(0)}_{m,n,r}$. Furthermore, the penalty in the constant policy when capturing spoofing attacks is P, and the penalty in the amount-related policy when capturing k attack is kP. Therefore, the expected penalty is given by:

$$\pi_{m,n,r} = \begin{cases} P\left(1 - \gamma^{(0)}_{m,n,r}\right), & \text{constant pentalty} \\ P \sum\limits_{k=1}^{\min(m,n)} k\gamma^{(k)}_{m,n,r}, & \text{amount-related penalty} \end{cases} \tag{4}$$

4.2.2 Nash Equilibrium: In order to find a solution for the best strategy of attacker and defender in such the interactive game, we explore NE in which each player has selected the best response to opponents' strategies, and no player gains anything by solely changing their own strategy. The NE of the formulated game (α^*_n, δ^*_m), therefore, must satisfy the following conditions:

$$\begin{cases} U_A\left(\alpha^*_n, \delta^*_m\right) \ge U_A\left(\alpha_n, \delta^*_m\right) \\ U_D\left(\alpha^*_n, \delta^*_m\right) \ge U_D\left(\alpha^*_n, \delta_m\right) \end{cases} \tag{5}$$

And, the problem for finding NE is equivalent to a bi-optimization problem as follows.

$$\begin{aligned} \underset{\boldsymbol{\alpha}}{\text{maximize}} \quad & \boldsymbol{\alpha}^T \boldsymbol{\Pi}_A \boldsymbol{\delta} \\ \underset{\boldsymbol{\delta}}{\text{maximize}} \quad & \boldsymbol{\alpha}^T \boldsymbol{\Pi}_D \boldsymbol{\delta} \\ \text{subject to} \quad & \mathbf{1}^T \boldsymbol{\alpha} = 1, \boldsymbol{\alpha} \ge 0 \\ & \mathbf{1}^T \boldsymbol{\delta} = 1, \boldsymbol{\delta} \ge 0 \end{aligned} \tag{6}$$

The optimization problem given in (6) can be solved by Lemke-Howson algorithm[16].

Proposition 1. *For constant penalty case, attacker only selects its attacking strategies from the two numbers of attack 0 and N.*

Proof: For constant penalty case, from (1a), (2a) and (4), the expected payoff of attacker corresponding to each selected number

of attacks n is calculated by:

$$U_{A|n} = \sum_m \delta_m \Pi^A_{m,n,r} = \sum_m \delta_m \left[n\left(G - C_A\right) - \left(1 - \gamma^{(0)}_{m,n,r}\right) P \right] \tag{7}$$

Then, the second derivative $U_{A|n}$ is determined by

$$\Delta\left(\Delta U_{A|n}\right)_{|n} = \Delta U_{A|n+1} - \Delta U_{A|n} = \frac{P \sum\limits_m \delta_m \left(m^2 + m\right) \gamma^{(0)}_{m,n,r}}{(n+r+1)(n+r+2)} \tag{8}$$

where $\Delta F_{|n} = F_{|n+1} - F_{|n}$ denotes the derivative of a discrete function $F_{|n}$ of variable n. Since $\Delta\left(\Delta U_{A|n}\right)_{|n} \geq 0, \forall m$, $U_{A|n}$ is a convex function of n regardless m, and hence,

$$U_{A|n} \leq \left(1 - \frac{n}{N}\right) U_{A|0} + \frac{n}{N} U_{A|N}, \forall m \text{ and } 0 < n < N.$$

In other word, the strategy n, $0 < n < N$, is dominated by either the strategies 0 or N. □

Corollary 1. *For constant penalty case, the formulated game given in Table* 1 *is equivalent to the* $2 \times M$ *bi-matrix game where attacker has only two strategies: not attack and attack with the full capacity of* N *spoofing requests.*

Proposition 2. *For constant penalty case,*

(i) $\exists m_{\max} \leq r : U_{D|m_{\max}} \geq U_{D|m}, \forall m > m_{\max}$.
(ii) $m_{\max}$ *is upper-bounded by*

$$m_0 = \max \left\{ \arg\max_m \left(\Pi^D_{m,n,r} \right) \right\}_{n=0}^{N} \tag{9}$$

(iii) the formulated game given in Table 1 *reduces to a* $2 \times (m_0 + 1)$ *bi-matrix game.*

Proof: (i) From (1b), (2b) and (4), the expected payoff of defender verifying m request in constant penalty case is computed by:

$$U_{D|m} = \sum_n \alpha_n \Pi^D_{m,n,r} = \sum_n \alpha_n \left(-mC_S + \left(1 - \gamma^{(0)}_{m,n,r}\right) P \right) \tag{10}$$

From (3), we have $\gamma^{(0)}_{m,n,r} = 0$ when $m > r$. Thus,

$$U_{D|r} \geq U_{D|m}, \forall m > r$$

This means that the feasible value of $m_{\max}$ is in $[0, r]$. Besides, the second derivative of $U_{D|m}$ is calculated by:

$$\begin{aligned} \Delta\left(\Delta U_{D|m}\right)_{|m} &= \Delta U_{D|m+1} - \Delta U_{D|n} \\ &= -P \sum_n \alpha_n \frac{n(n-1)\gamma^{(0)}_{m,n,r}}{(n+r-m-1)(n+r-m)} \end{aligned} \tag{11}$$

Obviously, $\Delta\left(\Delta U_{D|m}\right)_{|m} \leq 0$ for $0 \leq m \leq r$. Thus, $U_{D|m}$ is a concave function of m in $[0, r]$. This means that there exists $m_{\max} \leq r$ so that $U_{D|m_{\max}} \geq U_{D|m}, \forall m > m_{\max}$.

(ii) One can easily check that $\Delta\left(\Delta(\Pi^D_{m,n=k,r})_{|m}\right)_{|m} \leq 0$, $\forall 0 \leq k \leq N$ and $0 \leq m \leq r$. Hence, $\Pi^D_{m,n=k,r}$ is a concave function of m in $[0, r]$, $\forall 0 \leq k \leq N$. This means $\Pi^D_{m_0,n=k,r} \geq \Pi^D_{m,n=k,r}$, or $U_{D|m_0} \geq U_{D|m}$, $\forall m \geq m_0$.

(iii), One can easily check from (ii) that the formulated game (Table 1) reduces to a $2 \times (m_0 + 1)$ bi-matrix game. □

5 Data Traffic Identification Strategies

If the request passes the first verification step, the network manager then allocates the spectrum resource for the user. However, the ID spoofing attacks and even the location spoofing attacks could pass through due to the imperfect localization. Therefore, it is necessary to conduct a further surveillance process to verify if the allocated spectrum resource is used by the right/registered NO through an ID verification. The proposed ID verification can be considered as an appropriate complement for the request location check.

5.1 Game formulation

In order to analyze the interaction between the spoofing attack of an attacker and the ID surveillance process of the network manager, we formulate a non-cooperative extensive-form game as follows.

5.1.1 Players and Strategies:

- **Step 1**: Attacker, i.e., the user which perform the spoofing attack, sends n , $0 \leq n \leq N$ spoofing requests in either type 4 or type 5 for getting more spectrum resource.*
- **Step 2**: The network manager allocates $n + r$ spectrum band for n requests from attacker and r requests from real/normal users.
- **Step 3**: Defender scans m, $0 \leq m \leq \min(M, n + r)$ allocated spectrum bands to detect and penalize defender.†

Notice that attacker sends n requests without knowing the true value of r, while defender chooses m with the knowledge of the total allocated spectrum bands $n + r$. Hence, the pure behavioral strategy set of attacker is defined by

$$\mathbf{S}_A = \{n, 0 \leq n \leq N\},$$

and the pure behavioral strategy set of defender depending on $n + r$ is given by

$$\mathbf{S}_{D|n+r} = \{m|(n+r), 0 \leq m \leq \min(M, n+r)\}.$$

The corresponding mixed strategy sets of attacker and defender is defined by: $\boldsymbol{\alpha} = \{\alpha_n, 0 \leq n \leq N\}$ and $\boldsymbol{\delta}_{|n+r} = \{\delta_{m|n+r}, 0 \leq m \leq \min(M, n+r)\}$ where α_n is the probability of spoofing n requests and $\delta_{m|n+r}$ is the probability of monitoring m spectrum bands given that $n + r$ requests have been allocated.

5.1.2 Payoffs: Since both defender and attacker could have the historical records of the amount of the real NOs located in the area of attacker, we assume that the distribution of the real requests number r is a common knowledge. Without loss of generality, we assume that r follows Poisson distribution. The probability mass function (pmf) of r is given by: $f_{\mathfrak{R}}(r, \lambda) = \frac{\lambda^r e^{-\lambda}}{r!}$, where λ is Poisson distribution parameter, which equals to the mean value of r. To simply the game, we assume that r is truncated by a maximum value R where $Pr[r \leq R] \geq \theta$ (θ denotes a probability threshold, e.g., $\theta = 0.99$). This assumption is acceptable because the game is formulated for a small area where the difference in locations of NOs is undetectable by the request senders' locations verification process (Section 4), and hence the number of NOs could be limited. Then the probability of r is given by normalizing $f_{\mathfrak{R}}(r, \lambda)$ as follows.

$$\rho_r = \frac{f_{\mathfrak{R}}(r, \lambda)}{\sum_{r=0}^{R} f_{\mathfrak{R}}(r, \lambda)} \tag{12}$$

For providing a clear example, we depict the formulated game in a tree form when $M = 3$, $N = 2$ and $R = 2$ in Fig 4. It can be seen that, at each terminal node, i.e., the leaf of the game tree corresponding to a certain set of m, n and r, there is a pair of payoffs for both

** N denotes the maximum spoofing attack capability.*
† M represents the maximum surveillance capability.

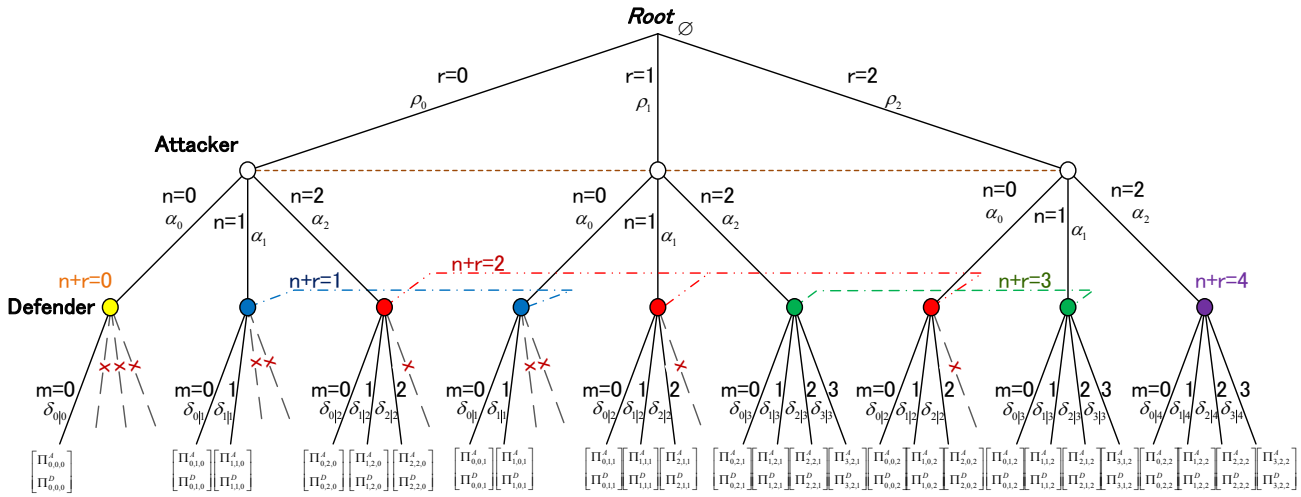


Fig. 4: The identification surveillance game for mitigating spoofing attack when $N = 2, M = 3$ and $R = 2$.

attacker and defender $\left[\Pi^A_{m,n,r}, \Pi^D_{m,n,r}\right]$ which are calculated as similarly as (1a) and (1b). Notice that the expected penalty $\pi_{m,n,r}$ is also calculated by (4) for either constant or amount-related penalty policy.

In principle, we can consider the formulated game given in Fig. 4 as an Bayesian game and adopt Harsanyi transformation [11] to convert it to a strategic-form game. This means the pure strategy set of defender can be built upon the combinations of all possible conditional pure strategy sets, i.e., $\mathbf{S}_D = \mathbf{S}_{D|0} \times \mathbf{S}_{D|1} \times \cdots \times \mathbf{S}_{D|n+r} \times \cdots \times \mathbf{S}_{D|N+R}$. However the number of the elements of $\mathbf{S}_D$ increases exponentially with M, N,and R ($|\mathbf{S}_D| = M!(M+1)^{N+R-M+1}$). E.g., $|\mathbf{S}_D| = 96$ with $M = 3, N = 2$ and $R = 2$ (the game in Fig. 4), but $|\mathbf{S}_D| = 24576$ with $M = 3, N = 2$ and $R = 6$. Therefore, it is too complicated to solve the game by Harsanyi transformation. Instead, we leverage our previous work [5] using the sequence form representation to express the formulated game.

5.2 *Sequence-form representation and Nash equilibrium*

In game theory, an extensive game can be represented by the sequence-form representation, which follows the tree-form of the game. The sequence-form representation is similar to the normal strategic-form one except that pure strategies are replaced by sequences of players, but with the lower complexity [15, 21]. In general, a player with perfect recall has the same sequence σ_u of choices at all nodes in an information set u. Consequently, each choice c at u is the last choice of a unique sequence $c|\sigma_u$, and the set of sequence of a player is given by $\mathbf{\Sigma} = \{\emptyset\} \cup \{c|\sigma_u\}$.

Since both players have perfect recall, the formulated game can be described in the sequence-form representation, in which the sequence sets of attacker and defender are defined by:

$$\mathbf{\Sigma}_A = \{\emptyset\} \cup \{n, n = 0, 1, ..., N\} \tag{13}$$

$$\mathbf{\Sigma}_D = \{\emptyset\} \cup \{m|n+r, m = 0, 1, ..., \min(M, n+r)\} \tag{14}$$

When attacker plays a mixed strategy, the realization probabilities for its sequences, called a *realization plan*, is represented by a non-negative vector $\boldsymbol{\alpha}$, $\boldsymbol{\alpha} = [\alpha_\emptyset, \alpha_0, \alpha_1, ..., \alpha_n, ..., \alpha_N]^T$.

The realization plan of attacker is characterized by: $\alpha_\emptyset = 1$ and $\sum_{n=0}^{N} \alpha_n = \alpha_\emptyset$. Similarly, the realization plan of defender is defined by a non-negative vector $\boldsymbol{\delta}$,

$$\boldsymbol{\delta} = \left[\delta_\emptyset, \delta_{0|0}, \delta_{0|1}, \delta_{1|1}, ..., \delta_{m|n+r}, ..., \delta_{\min(M,N+R)|N+R}\right]^T$$

which $\delta_\emptyset = 1$ and $\sum_{m=0}^{\min(M,n+r)} \delta_{m|n+r} = 1, \forall n, r$.

These constraints can be rewritten in matrix form by:

$$\begin{cases} \mathbf{E}\boldsymbol{\alpha} = \mathbf{e} \\ \boldsymbol{\alpha} \geq 0 \end{cases}, \quad \text{and} \quad \begin{cases} \mathbf{F}\boldsymbol{\delta} = \mathbf{f} \\ \boldsymbol{\delta} \geq 0 \end{cases}, \tag{15}$$

where $\mathbf{e} = [1, 0]^T$, $\mathbf{f} = [1, 0, ..., 0]^T$, and $\mathbf{E}$ and $\mathbf{F}$ are constraint matrices which are given by:

$$\mathbf{E} = \begin{bmatrix} 1 & 0 & ... & 0 \\ -1 & 1 & ... & 1 \end{bmatrix} \tag{16}$$

$$\mathbf{F} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & ... & 0 \\ -1 & 1 & 0 & 0 & 0 & 0 & ... & 0 \\ -1 & 0 & 1 & 1 & 0 & 0 & ... & 0 \\ ... & & & & ... & ... & & \\ -1 & 0 & 0 & 0 & 0 & 1 & ... & 1 \end{bmatrix} \tag{17}$$

In the sequence-form representation, the payoff of attacker and defender is represented by matrices $\mathbf{\Phi}_A$ and $\mathbf{\Phi}_D$, respectively. Each sequence of attacker corresponds to a row and each sequence of defender corresponds to a column. The payoff values for a pair of sequences defined by a leaf of the game tree are equal to the payoff values of the leaf. Otherwise, the payoff values are equal to zero. For example, the payoffs of attacker and defender at $(\emptyset, m|n+r)$ are zero, and at $(n, m|n+r)$ are $\Pi^A_{m,n,r}$ and $\Pi^D_{m,n,r}$. The expected utility of the attacker and the defender in sequence-form are calculated by:

$$U_A = \boldsymbol{\alpha}^T \mathbf{\Phi}_A \boldsymbol{\delta} \tag{18a}$$

$$U_D = \boldsymbol{\alpha}^T \mathbf{\Phi}_D \boldsymbol{\delta} \tag{18b}$$

The problem for finding NE is given by:

$$\max_{\boldsymbol{\alpha}} \quad \boldsymbol{\alpha}^T \mathbf{\Phi}_A \boldsymbol{\delta} \tag{19a}$$
$$\text{s.t.} \quad \mathbf{E}\boldsymbol{\alpha} = \mathbf{e}, \boldsymbol{\alpha} \geq \mathbf{0}$$

$$\max_{\boldsymbol{\delta}} \quad \boldsymbol{\alpha}^T \mathbf{\Phi}_D \boldsymbol{\delta} \tag{19b}$$
$$\text{s.t.} \quad \mathbf{F}\boldsymbol{\delta} = \mathbf{f}, \boldsymbol{\delta} \geq \mathbf{0}$$

The duality problems of (19) are given by:

$$\min_{\mathbf{x}} \quad \mathbf{e}^T \mathbf{x} \tag{20a}$$
$$\text{s.t.} \quad \boldsymbol{\alpha}^{\mathbf{T}} \left(-\mathbf{\Phi}_A \boldsymbol{\delta} + \mathbf{E}^T \mathbf{x}\right) = 0, \mathbf{E}^T \mathbf{x} \geq \mathbf{\Phi}_A \boldsymbol{\delta}$$

$$\min_{\mathbf{y}} \quad \mathbf{f}^T \mathbf{y} \tag{20b}$$
$$\text{s.t.} \quad \boldsymbol{\delta}^{\mathbf{T}} \left(-\mathbf{\Phi}_D^T \boldsymbol{\alpha} + \mathbf{F}^T \mathbf{y}\right) = 0, \mathbf{F}^T \mathbf{y} \geq \mathbf{\Phi}_D^T \boldsymbol{\delta}$$

The feasible solutions of $\boldsymbol{\alpha}$ of (19a) and $\boldsymbol{x}$ of (20a) are optimal if and only if the two objective function values are equal, i.e., $\boldsymbol{\alpha}^T \boldsymbol{\Phi}_A \boldsymbol{\delta} = \mathbf{e}^T \mathbf{x}$. This means that $\boldsymbol{\alpha}^{\mathbf{T}} \left(-\boldsymbol{\Phi}_A \boldsymbol{\delta} + \mathbf{E}^T \mathbf{x} \right) = 0$. Similarly, $\boldsymbol{\delta}$ of (19b) and $\boldsymbol{y}$ of (20b) are optimal if and only if $\boldsymbol{\delta}^{\mathbf{T}} \left(-\boldsymbol{\Phi}_D^T \boldsymbol{\alpha} + \mathbf{F}^T \mathbf{y} \right) = 0$. In summary, the equilibrium $\{\boldsymbol{\alpha}, \boldsymbol{\delta}\}$ is determined through:

$$
\begin{array}{ll}
\text{find} & \boldsymbol{\alpha}, \boldsymbol{\delta}, \mathbf{x}, \mathbf{y} \\
\text{s.t.} & \mathbf{E}^T \mathbf{x} \geq \boldsymbol{\Phi}_A \boldsymbol{\delta}, \mathbf{F}^T \mathbf{y} \geq \boldsymbol{\Phi}_D^T \boldsymbol{\delta} \\
& \boldsymbol{\alpha}^{\mathbf{T}} \left(-\boldsymbol{\Phi}_A \boldsymbol{\delta} + \mathbf{E}^T \mathbf{x} \right) = 0 \\
& \boldsymbol{\delta}^{\mathbf{T}} \left(-\boldsymbol{\Phi}_D^T \boldsymbol{\alpha} + \mathbf{F}^T \mathbf{y} \right) = 0 \\
& \boldsymbol{E\alpha} = \mathbf{e}, \boldsymbol{F\delta} = \mathbf{f} \\
& \boldsymbol{\alpha} \geq 0, \boldsymbol{\delta} \geq 0
\end{array}
\tag{21}
$$

We introduce a non-negative vector $\mathbf{z} = \left(\boldsymbol{\alpha}, \boldsymbol{\delta}, \mathbf{x}', \mathbf{x}'', \mathbf{y}', \mathbf{y}'' \right)^T$ where $\mathbf{x}', \mathbf{x}''$, $\mathbf{y}'$, and $\mathbf{y}''$ are also non-negative vectors with the same dimension so that $\mathbf{x} = \mathbf{x}' - \mathbf{x}''$ and $\mathbf{y} = \mathbf{y}' - \mathbf{y}''$. The values of $\mathbf{x}, \mathbf{y}, \boldsymbol{\alpha}$, and $\boldsymbol{\delta}$ which satisfy the constraints of (21) can be found by solving a standard Linear Complementary Programing (LCP) which is given by [4]:

$$
\begin{array}{ll}
\text{find} & \mathbf{z} \\
\text{s.t} & \mathbf{Hz} + \mathbf{b} \geq \mathbf{0} \\
& \mathbf{z}^{\mathbf{T}} (\mathbf{Hz} + \mathbf{b}) = 0 \\
& \mathbf{z} \geq 0
\end{array}
\tag{22}
$$

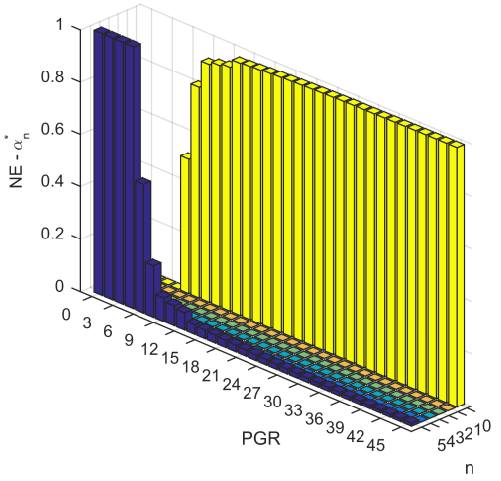
where $\mathbf{b}^T = \left(0,\ 0,\ \mathbf{e},\ -\mathbf{e},\ \mathbf{f},\ -\mathbf{f} \right)^T$ and

$$
\mathbf{H} = \begin{bmatrix}
\mathbf{0} & -\boldsymbol{\Phi}_A^T & \mathbf{E^T} & -\mathbf{E^T} & \mathbf{0} & \mathbf{0} \\
-\boldsymbol{\Phi}_D^T & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{F^T} & -\mathbf{F^T} \\
-\mathbf{E} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\
\mathbf{E} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\
\mathbf{0} & -\mathbf{F} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\
\mathbf{0} & \mathbf{F} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0}
\end{bmatrix}
\tag{23}
$$

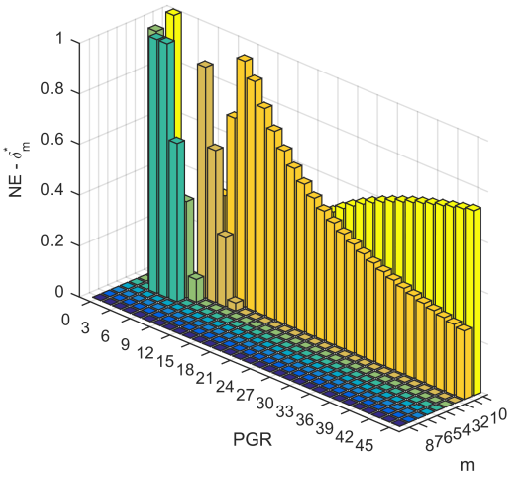
Lemke algorithm [4, 15, 21], a general version of the L-H algorithm, is an efficient mean on solving LCP problem. Therefore, we adopt it for dealing with the problem (22). Feasible points achieved from Lemke algorithm is then used to find the optimal solution of (21) which is the NE point of the game. The existence of a feasible solution of (22) is provided in [15] through a simple trick that subtracting a constant from the payoffs of the players that these become non-positive to ensure Theorem 4.1 (pp. 254-255, [15]).

6 Numerical Results

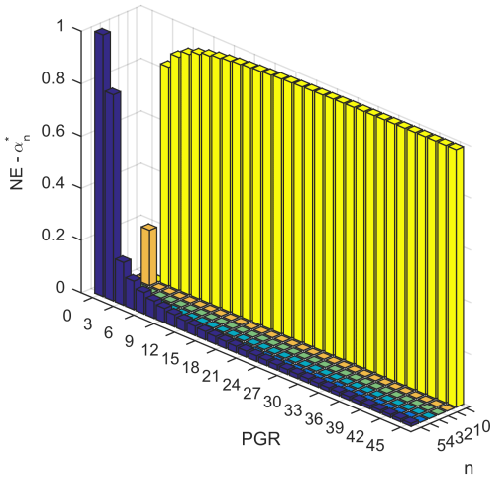
In this section, we use numerical simulation to demonstrate the performance of the proposed algorithm for mitigating the influence of location and ID spoofing attacks in the GDB driven spectrum sharing systems.



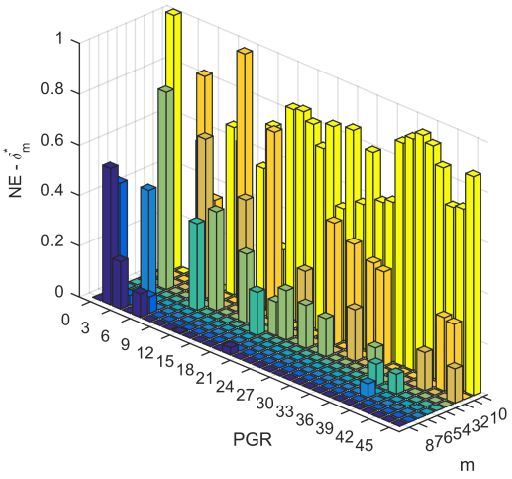
(a) Attacker - Constant penalty



(b) Defender - Constant penalty



(c) Attacker - Amount-related penalty



(d) Defender - Amount-related penalty

Fig. 5: Nash Equilibrium vs. penalty gain ratio when $r = 6$, $N = 5$, and $M = 8$.

6.1 Request location verification strategies

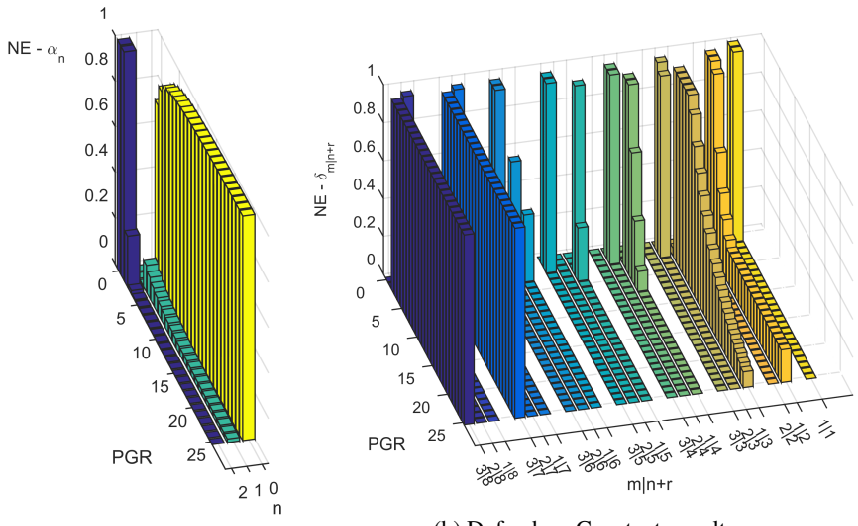
Figure 5 depicts the NE of the formulated game for the two penalty policy cases according to different values of penalty gain ratio (PGR) when $r = 6$, $N = 5$, and $M = 8$. The PGR is defined by:

$$PGR = P/G \tag{24}$$

G is the gain of using a spectrum band in a requesting interval, i.e., the interval between two adjacent requesting times. Therefore, PGR is equivalent to the number of banning time interval on an captured attacker. Assume that $G = 10$, $C_S = 2$ and $C_A = 1$. It should be noted that C_A is the cost of sending a request to the network manager on a control channel, whereas C_S is the cost for localizing the request sender. Thus, it is reasonable to assume that $C_A \ll G$ and $C_A < C_S$. The results are achieved by adopting L-H algorithm on the original game with the size $N \times M$.

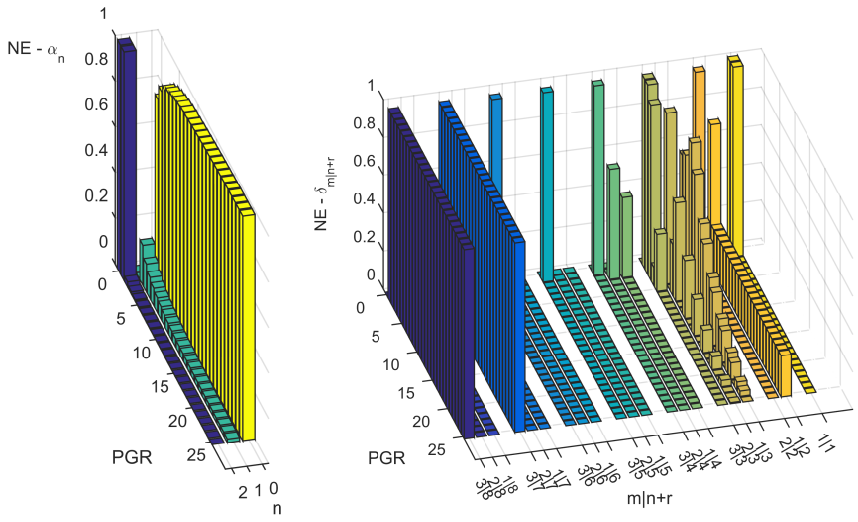
For the effect of the penalty policies, on the one hand, as shown in Fig. 5a, an attacker in constant penalty case only selects between no attack $n = 0$ and attack with full capability $n = N$. The other attacking strategies are dominated. This result is in accordance with the statement in Proposition 1. As shown in Fig. 5c, an attacker in amount-related penalty case has almost the same behavior as an attacker in constant penalty case, expect for the small PGR case where strategies $n, n > 0$ appear. Complicated surveillance behaviors of defender in this case is the reason for this result. On the other hand, there is a big difference, when comparing the NE of defender between the two penalty policies. For the constant penalty policy, in accordance with the state in Corollary 2, defender does not select to verify more than the number of real users. In Fig. 5b, the largest n is 4 which smaller than $r = 6$, whereas in Fig. 5d, the largest n is 8 which is larger than $r = 6$. The reason is that in the proportional penalty policy, the more the spoofing attacks has been captured, the more the benefit from penalties has been gained. Hence, the defender has to optimize the number of verification of request messages in its full range of monitoring capability, i.e., $\min(M, r + n)$. In brief, these results mean that the penalty policies do affect the selection of the NE strategies of both defender and attacker.

For the effect of PGR, we observe that there is the same decreasing trend of both attacking and defending probabilities when PGR increases. With a large PGR, defender in constant penalty only needs to maintain a small monitoring probability in one location while defender in amount-related penalty may need to monitoring many requesting locations. Consequently, for the formulated game between the spoofing attack and the requests' location verification, it is favorable to select the constant penalty policy with a large PGR. However, as analyzed in the penalty policy issue, the PGR should



(a) Attacker - Constant penalty

(b) Defender - Constant penalty



(c) Attacker - Amount-related penalty

(d) Defender - Amount-related penalty

Fig. 6: Nash Equilibrium vs. penalty gain ratio when $M = 3$, $N = 2$, $R = 4$, and $\lambda = 2$.

not be too large because of the possible influence on other normal NOs located inside the monitoring area. Therefore, a reasonable PGR should be selected, e.g., $PGR = 15$ as in Fig. 5a and 5b.

6.2 Data Traffic Identification Strategies

Fig. 6 illustrates the NE of the surveillance game with difference values of PGR when $M = 3$, $N = 2$, $R = 4$, and $\lambda = 2$*. Two penalty policies are also considered. The cost and gain parameters are the same as the simulation of the location verification case. In order to provide a clear view of NE points, we only depict the strategies of defender where $m \neq 0$. The probability $\delta_{0|n+r}$ at NE can be inferred from the others because $\sum_m \delta_{m|n+r} = 1$. We can see that the NE points in two penalty cases are quite similar for the attacker and not much different for defender. From attacker side, the NE/best strategies of attacker in the two penalty policies is to attack with a high number of requests when PGR is low and either to attack with a low number of requests or not when PGR is high. It is obvious that the penalty value does affect the attacking behavior of attacker.

For defender side, the best behaviors depend on the values of both PGR and the total request number $n + r$. At low PGRs, defender performs surveillance in all case of $n + r$ since attacking probability is very high in these points. However, when PGR is high, defender only monitors spectrum bands at very low and very high $n + r$ cases. The reason is that the probabilities of having very low or very high number of real requests are lower than the middle range. This means that if conducting surveillance process at these extreme cases, the possibility of capturing attacker will be higher.

Fig. 7 depicts the average delay penalty that attacker has to suffer when it considers NE, uniform (i.e., attacker perform its pure strategies equally), and full attacking strategies (i.e., attacker always attacks with full capability). A Monte Carlo simulation with 10^6 samples is adopted, when $(M, N, R) = (3, 2, 6)$, and $\lambda = 2$. Two penalty policies are considered. We see that attacker is severely delayed if it tries to increase their attacking rate and there is an optimal point for setting PGR for both penalty cases, i.e., 8 for the constant penalty and 3 for captured amount-related penalty, where attacker suffers the highest delays. This means that, by using NE and setting appropriate penalty, defender could impose a stronger enforcement of reducing the selfish spoofing attack.

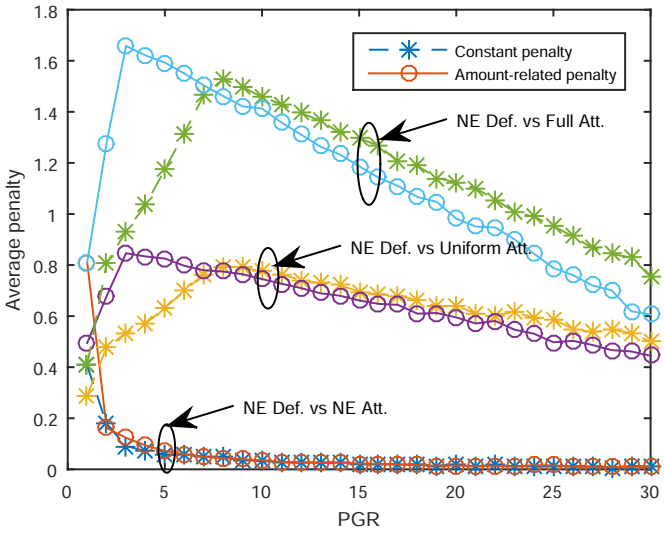


Fig. 7: Average delay penalty vs. PGR.

*We select a small value of R to provide a clearer presentation of the results

7 Conclusion

We have presented a study of critical security threats of various spoofing attacks and their countermeasures in the geo-location database-driven spectrum sharing system. Depending on the structure of the spoofing request, there are five spoofing types for the three accidentally, maliciously and selfishly attacking purposes. Under a spoofing attack, an attacker could spoof either the ID or the location information. The requests' location verification and the data identification processes are the countermeasures for the spoofing attacks. We have formulated two corresponding games for modeling the conflict interaction between the attack of an adversary and the surveillance processes on a resource manager. The surveillance game of the requests' location verification and the spoofing attack is expressed by the strategic form, and the game of the data identification and the spoofing attack is built upon by the sequence-form representation. NE points of the formulated games are determined through Lemke-Howson and Lemke algorithms. The results show that a resource manager mitigates the spoofing attack by changing its penalty policy and surveillance strategies.

8 References

1 Akyildiz, I.F., Lee, W.Y., Vuran, M.C., Mohanty, S.: Next generation/dynamic spectrum access/cognitive radio wireless networks: A survey. Computer Networks 50(13), 2127 – 2159 (2006), http://www.sciencedirect.com/science/article/pii/S1389128606001009

2 Bahrak, B., Bhattarai, S., Ullah, A., Park, J.M., Reed, J., Gurney, D.: Protecting the primary users' operational privacy in spectrum sharing. In: IEEE International Symposium on Dynamic Spectrum Access Networks (DYSPAN). pp. 236–247 (April 2014)

3 Benco, D.S., Kanabar, P.C., Nguyen, J.C., Song, H.: Caller id spoofing (Oct 16 2006), uS Patent App. 11/581,634

4 Cottle, R.W., Pang, J.S., Stone, R.E.: The linear complementarity problem, vol. 60. Siam (1992)

5 Duc-Tuyen, T., Nguyen-Thanh, N., Maille, P., Ciblat, P., Nguyen, V.T.: Mitigating selfish primary user emulation attacks in multi-channel cognitive radio networks: A surveillance game. In: IEEE Globecom'16 (2016)

6 Ehrenkranz, T., Li, J.: On the state of ip spoofing defense. ACM Transactions on Internet Technology (TOIT) 9(2), 6 (2009)

7 Etkin, R., Parekh, A., Tse, D.: Spectrum sharing for unlicensed bands. IEEE Journal on Selected Areas in Communications 25(3), 517–528 (April 2007)

8 FCC12-36: Third memorandum opinion and order. Tech. rep., Federal Communications Commission (May 2012), http://transition.fcc.gov/Daily_Releases/Daily_Business/2012/db0405/FCC-12-36A1.pdf

9 Gao, Z., Zhu, H., Liu, Y., Li, M., Cao, Z.: Location privacy in database-driven cognitive radio networks: Attacks and countermeasures. In: IEEE INFOCOM. pp. 2751–2759 (April 2013)

10 Gibbons, R.: Game theory for applied economists. Princeton University Press (1992)

11 Harsanyi, J.: Games with Incomplete Information Played by "Bayesian" Players, I-III. Manage. Sci. 50(12), 1804–1817 (Dec 2004)

12 Hossain, E., Niyato, D., Han, Z.: Dynamic Spectrum Access and Management in Cognitive Radio Networks. Cambridge University Press (2009), http://dx.doi.org/10.1017/CBO9780511609909, cambridge Books Online

13 IEEE: 802.11af-2013: Part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications amendment 5: Television white spaces (tvws) operation (December 2013)

14 IEEE: 802.19-2014:part 19: Tv white space coexistence methods (May 2014)

15 Koller, D., Megiddo, N., Von Stengel, B.: Efficient computation of equilibria for extensive two-person games. Games and Economic Behavior 14(2), 247–259 (1996)

16 Lemke, C., Howson Jr, J.: Equilibrium Points of Bimatrix Games. Journal of the Society for Industrial and Applied Mathematics 12(2), 413–423 (1964)

17 Murty, P.: SenseLess: A Database-Driven White Spaces Network. IEEE Transactions on Mobile Computing 11(2), 189–203 (Feb 2012)

18 Nguyen-Thanh, N., Ciblat, P., Pham, A.T., Nguyen, V.T.: Surveillance strategies against primary user emulation attack in cognitive radio networks. IEEE Transactions on Wireless Communications 14(9), 4981–4993 (2015)

19 Peng, Q., Cosman, P.C., Milstein, L.B.: Spoofing or jamming: Performance analysis of a tactical cognitive radio adversary. IEEE Journal on Selected Areas in Communications 29(4), 903–911 (April 2011)

20 Shoham, Y., Leyton-Brown, K.: Multiagent systems: Algorithmic, game-theoretic, and logical foundations. Cambridge University Press (2008)

21 von Stengel, B., Van Den Elzen, A., Talman, D.: Tracing equilibria in extensive games by complementary pivoting. Tilburg University (1996)

22 Wang, W., Zhang, Q.: Location Privacy Preservation in Cognitive Radio Networks. Springer (2014)

23 Yucek, T., Arslan, H.: A survey of spectrum sensing algorithms for cognitive radio applications. IEEE Communications Surveys Tutorials 11(1), 116–130 (First 2009)

24 Zeng, K., Ramesh, S., Yang, Y.: Location spoofing attack and its countermeasures in database-driven cognitive radio networks. In: IEEE Conference on Communications and Network Security (CNS). pp. 202–210 (Oct 2014)