Malicious users control and management in cognitive radio networks with priority queues

Samuel D. Okegbile
Dept. of Electrical, Electronic and Computer Engineering, University of Pretoria, South Africa
samokegbile@gmail.com

B. T. Maharaj
Dept. of Electrical, Electronic and Computer Engineering, University of Pretoria, South Africa
sunil.maharaj@up.ac.za

Attahiru S. Alfa
Dept. of Electrical and Computer Engineering, University of Manitoba, Canada and Dept. of Electrical, Electronic and Computer Engineering, University of Pretoria, South Africa
attahiru.alfa@umanitoba.ca

***Abstract*—Malicious users (MUs) have the tendency to disrupt the activities of honest users in the network if not properly controlled. In a massive cognitive radio network (CRN) with priority queues, malicious secondary users (SUs) can manipulate their priority queue requirements and mislead legitimate SUs to vacate the channels. In this paper, a game theoretic based signal detection approach is proposed to control the presence of MUs in CRN. If the received signal strength is less than the predefined threshold for primary transmissions in the presence of interference and noise, such a user is marked to be malicious and its payoff table is updated. Through the mixed strategy Nash equilibrium method, the payoff table of each user can be updated to aid removal of MUs from the network. The outcome of the simulation results shows that such an approach can reduce the impact of malicious activities in the massive CRN where SUs are expected to be low-power energy-efficient devices.**

***Index Terms*—Cognitive radio, game theory, payoff, point process, queuing.**

I. Introduction

Cognitive radio network (CRN) has been proposed as a suitable paradigm capable of ending the threat of spectrum scarcity caused by the adoption of the fixed spectrum allocation policy, which has proven to be inefficient and insufficient to cope with the next generation of spectrum users. It is, therefore, unsurprising that the area has been receiving substantial attention in the past years. CRN is the paradigm that allows unlicensed users to access the channels belonging to licensed users such as digital TV transmitters, provided that such usage will not disrupt the activities of the licensed users. The channel access requirements of the unlicensed users can thus be met while the operations of the licensed users are not affected. These licensed users are generally called the primary users (PUs), while the unlicensed users are known as secondary users (SUs) or cognitive users.

In order to meet the channel usage constraints, especially at the primary network, all SUs must carry out channel sensing to obtain the state of the channel. When any PU is active (i.e. in the ON state) on a particular channel, such a channel is said to be busy and unavailable for secondary usage. SUs must, therefore, wait until the channel is available or switch to another channel for possible spectrum opportunity. In CRN, a typical SU can secure transmission opportunity based on the time (when a PU is inactive), the frequency (when a PU is transmitting on another frequency band), or space (when a PU is located far away). A transmission opportunity obtained by the SUs based on space encourages spatial reuse and is known to facilitate spectrum usage in a more efficient and effective manner. In such a network, an SU is allowed to transmit when the neighboring PUs are not active, though the transmissions of several SUs, as in a densely populated wireless network, can result in excessive interference with the primary networks. To reduce interference associated with spatial reuse, interference management and control become an important issue if users' quality of service must be satisfied.

Stochastic geometry (SG) has been proposed as a suitable approach to control interference in wireless networks [1]– [3]. In [1], [2], the use of protection zones within which SUs are not allowed to transmit were shown to reduce interference in the network. Subsequent efforts [4], [5] now consider the integration of the queueing model into the system modeling so as to relax the full buffer assumption in the previous works, while also capturing the spatial-temporal dynamic of the network. With the adoption of queueing theory along with SG, PUs are placed in the primary queue, while SUs are placed in the secondary queue. PUs in the primary queue are considered to transmit based on their arrival time following first-come-first-served (FCFS) principle, though PUs' arrivals are well structured owing to their delay-sensitive nature. Because of the pre-emptive priority enjoyed by PUs, no SU can secure access to transmit within a location except when the primary queue in such a spatial location is empty. Similar to the primary queue, SUs gain access to transmit based on their arrival time following the FCFS principle, provided that the primary queue is empty.

With the adoption of the spatiotemporal approach in CRN, malicious SUs (which will be referred to throughout this paper as malicious users (MUS)) can violate the queueing principle to deny other SUs opportunities to transmit by staying on the primary queue, forcing SUs either to switch to another channel or wait for a longer period (an attack similar to

This work was supported by the SENTECH Chair in Broadband Wireless Multimedia Communications (BWMC), Department of Electrical, Electronic and Computer Engineering, University of Pretoria, South Africa.

a denial of service attack). Similarly, MUs can stay in the secondary queue and wait for an appropriate transmission opportunity with the purpose of disrupting the network by selfishly securing more channel opportunities than specified for secondary transmissions. Such attacks are common in all wireless networks and have been subjected to intense research in the past years. In CRN, MUs are commonly studied in the form of PU emulation attackers (PUEA) [6]–[14], jamming attackers [15], jamming learning threats and secondary spectrum data falsification [6], [16] etc. though PUEA is the most frequently studied form of attack in the literature because it is the most dangerous threat to CRN owing to the difficulty of detecting it.

Two common types of PUEA are selfish and malicious users [7]. PUEA in the form of MUs pose denial of service threats [17]. In PUEA, malicious SUs can mislead legitimate SUs to vacate the channels by mimicking PUs' signal features [11]. Accurate detection of a PU is, however, very challenging, hence the need to differentiate between PU and PUEA signals remains an open issue in CRN [10]. One important requirement when detecting MUs in CRN is that such an approach must be energy-efficient, since SUs are expected to be low-power energy-efficient devices or users.

The energy detection approach was considered in [10], [18], though multiple channels were not considered in [18]. Similarly, a trust list table was proposed in [6], while a multipath fading detection approach was used to detect PUEA in [7]. In CRN, PUs are generally TV stations, radars and cellular base stations with signal power strength normally tens to thousands of times higher than what PUEA can produce [19]; hence, the signal power of PUs cannot be mimicked by smart attackers. The detection of PUEA through PU transmission power was thus considered in [9]. In [14], PUs' activity patterns were obtained through the ON and OFF periods of PU signal and were compared with the activity patterns of any active user to detect MUs. Such an approach, however, assumed a similar channel usage pattern (ON and OFF periods) referred to as a signal activity pattern for all PUs.

Detection approaches based on fingerprint/radiometric features, transient pulse shape, geographical information, and propagation channels have been claimed to be computationally intensive, hence, to have restricted deployment [20], while the localization-based approach and fingerprint approach assume that the locations and identities respectively of PUs are known to all SUs. In fact, the localization approach is known to be affected by many factors such as mobility, fading and shadowing [6]. The belief level approach is proposed in [21] in which each node's reputation is obtained through the cluster head of the group to which such node belongs. Each time, all nodes carry out channel sensing and forward the outcome to their neighboring nodes. Such outcomes are also sent to the cluster head to compute each node's belief level. The limitation of such an approach lies in its dependence on the cluster heads to determine the state of a PU. For instance, a smart attacker can first build its belief level until it becomes the cluster head with the aim of compromising the entire network.

In [6], a game theory-based approach is proposed to detect PUEA in CRN following the approach discussed in [8]. The work assumed that the existing pattern of PUs is known to all SUs in the learning phase and that SUs are able to recognize the evacuation signal from the PUEA. Communication between the sending and receiving nodes, however, occurs through the multiple cluster heads - an approach that is not energy-efficient, while interference between PUEAs and SUs is neglected. An advanced encryption scheme was proposed in [13], where PUs were assumed to be uniformly distributed, although the distribution of SUs was not considered. The adoption of authentication and encryption methods has been reported to require a high level of computation and overhead cost [6]. Mitigation of jamming attacks was also considered in [15].

In this paper, we present a game theoretic based signal to interference plus noise ratio (SINR) detection approach to mitigate and detect the activities of MUs in CRN. To the best of our knowledge, detection of MUs, while still capturing the spatiotemporal behavior of users in CRN, has not been considered before. The approach presented in this paper not only captures the information-theoretic interactions in the network, but is also shown to be energy-efficient. The closest effort to our work is [11], in which a queueing game-theoretic solution was introduced. The work studied the effects of malicious misbehavior users and selfish misbehavior users in CRN through the M/M/1 queuing system. The work, however, considered only a single PU band while SUs still vacate bands for malicious misbehavior and selfish misbehavior users.

The rest of the paper is structured as follows: In Section II, we present the details of the network model, while Section III presents the analysis of the proposed approach. Numerical results and simulation are presented in Section IV, while Section V concludes this paper. The following notations are used throughout this paper: (a, b) is the payoff received by the SU and MU respectively, $\bar{x} = 1 - x$ and I represents the identity matrix.

II. Network model

We consider a CRN under malicious attack as shown in Fig. 1, where the network is segmented into different cells or disks of radius $r_{p,max}$, each of which represents the coverage area of PUs. Each of these cells includes PUs and SUs considered to be located on primary and secondary queues respectively, based on their arrival times. MUs can be located in either a primary or secondary queue owing to their malicious features. The distribution of primary transmitters and secondary transmitters is assumed to follow two independent Poisson point processes Ψ_p and Ψ_s with their respective intensity given as λ_p and λ_s, though such distributions are better represented as the Matern hole process (MHP). The approximation was necessary owing to the unavailability of the probability generating functional (PGFL) for MHP. Note that in CRN, we have only two users: PUs and SUs. All MUs that are present can, therefore, be interpreted as SUs with

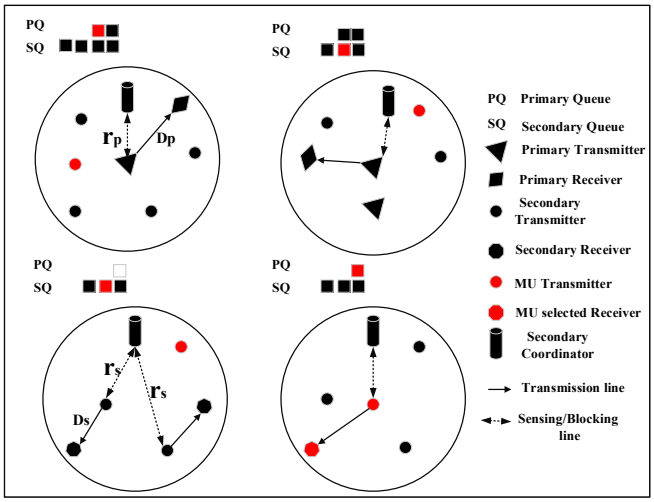

Fig. 1. Users' distribution in CRN under malicious attacks.

malicious intentions and their distributions are captured within SUs' distribution.

For any active primary transmitter (PT), its paired primary receiver is located at a maximum distance $D_p \leq r_{p,max}$. Similarly, for any active secondary transmitter (ST), its paired secondary receiver is located at a maximum distance of $D_s, \forall D_s \ll D_p$. Since $D_s \ll D_p$, more than one ST can be granted access within any cell, depending on the channel requirements if no PT is active. Each secondary user coordinator (SC) is assumed to be distributed uniformly within each cell and is capable of accessing the signal strength and location of each active user within such a cell at any time slot via smart channel sensing. Any active PT is located at a distance $r_p \in [0, r_{p,max}]$ from its closest SC. Similarly, any active ST is located at a maximum distance of $r_s \in [0, r_{s,max}], \forall r_{s,max} \leq r_{p,max}$ from the SC located within its spatial location. The deployment of SCs is useful in the detection of MUs and is responsible for user verification in the network.

The use of a vacation-based Geo/PH/1 discrete-time Markov chain queuing model was employed for each cell owing to its simplified memoryless inter-arrival process and its general departure process that can account for the interference-based interactions between the primary and secondary queues in the network [5]. Each PT arrival rate follows a Bernoulli process with parameter ξ_p, while each ST arrival rate follows an independent Bernoulli process with parameter ξ_s. With such a model, we considered inter-arrival time at each primary queue to follow a geometric distribution with parameter $\xi_p \in [0, 1]$ transmitter per time slot, while inter-arrival time at each secondary queue is considered to follow an independent geometric distribution with parameter $\xi_s \in [0, 1]$ transmitter per time slot.

We assumed that both queues have infinite capacities and that each PT requires a random number of slots to complete its transmission. STs requiring multiple slots to complete their transmissions must carry out channel sensing at the beginning of each time slot.

Owing to the requirement of CRN, a typical ST is required to vacate the band upon arrival of any user in the primary queue (because of its low power and processing capabilities, legitimate STs assume any user in the primary queue is a PU). The interrupted ST is returned to the head of the secondary queue. Both primary and secondary priority queues' vacation periods can be characterized using PH type distribution. When the primary queue is not empty, the channel is unavailable for secondary transmission, hence, to all users in the secondary queue, the channel is said to be on vacation. However, when the primary queue is empty, all users in the secondary queue perceive the channel to have returned from vacation and hence in the state of absorption.

The detection of malicious activities on the network is thus discussed as follows: an MU can either be a selfish MU or a destructive MU. A typical MU is destructive if such a user secures access to a channel (usually through a secondary queue) with the purpose of causing interference to neighboring users. On the other hand, a selfish MU joins the primary queue with the aim of preventing legitimate SUs from accessing the channels (an attack known as a denial of service). As shown in Fig. 2, an SC located within each cell verifies each user on the channel using the received SINR and the estimated distance to decide whether such a user is legitimate or an MU. Through channel sensing, the SC is aware of the SINR pattern of PTs within its assigned cell under the Rayleigh fading assumption and unbounded path loss propagation model.

At the beginning of each slot, any ST $y_k \in \Psi_s$ at the head of the secondary queue senses the channel for a window cycle c_w to obtain channel information in the primary queue. If the primary queue is empty, such an ST proceeds to transmit on the channel, else the ST waits until the channel becomes available or switches to other cells with faster transmission opportunities. Similarly, any typical SC within such a cell performs channel sensing to obtain the SINR credentials and the estimated distance of the current channel user. This sensing is done during a window cycle $v_w < c_w$. If the set of the received SINR during v_w falls within the known SINR of PTs, no ST is allowed to access the channel. However, if the received SINR does not fall within the known SINR for PTs, such a user is considered to be malicious. MUs are denied access by the SC, providing more spectrum opportunities for the legitimate SUs. With $v_w < c_w$, the SC considers any user besides PUs transmitting within v_w to be malicious, since only PUs are allowed to transmit without sensing. We provide more details in the next section.

III. Analysis

The analysis for the proposed CRN followed a two-level PH type distribution of the initial probability vector β_n and transient matrix S_n, where $n \in [p, s]$ for PUs and SUs. The transient matrix S_n is defined as the sub-stochastic matrix representing the transient states' transitions and it captures transitions until service completion [22]. For any real-life queuing system modeled in discrete time, it is possible to come up with quasi-birth-and-death (QBD) types of Markov

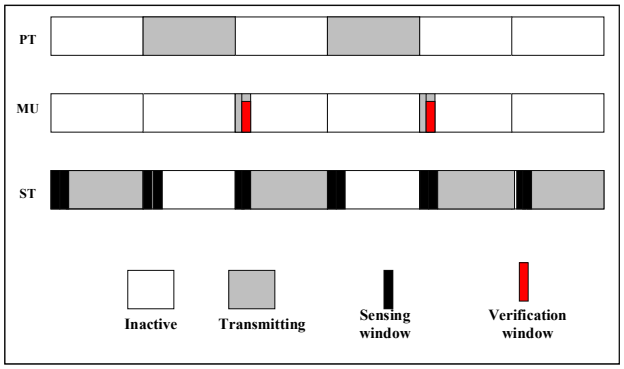

Fig. 2. Users' distribution in CRN under malicious attacks.

chains for such a system [23]. The QBD model suitable to characterize such a model can be derived as

$$P_n = \begin{pmatrix} B_{1,n} & C_n & & & \\ E_n & A_{1,n} & A_{0,n} & & \\ & A_{2,n} & A_{1,n} & A_{0,n} & \\ & & A_{2,n} & A_{1,n} & A_{0,n} \\ & & \ddots & \ddots & \ddots \end{pmatrix}, \quad (1)$$

where $B_{1,n} = 1 - \xi_n$, $E_n = (1-\xi_n)s_n$, $C_n = \xi_n\beta_n$, $A_{0,n} = \xi_n S_n$, $A_{1,n} = \xi_n s_n \beta_n + (1-\xi_n)S_n$, $A_{2,n} = (1-\xi)s_n\beta_n$ and $s_n = \mathbf{1} - S_n\mathbf{1}$. $\mathbf{1}$ is the column vector of ones. From [22], we know that

$$R_n = A_{0,n}[I - A_{1,n} - A_{0,n}\mathbf{1}\beta_n]^{-1}. \quad (2)$$

The stationary distribution of this system can be obtained, knowing that

$$x_n = x_n P_n, x_n\mathbf{1} = 1, \quad (3)$$

with the boundary equations given as

$$x_{n,0} = x_{n,0}(1-\xi_n) + x_{n,1}(1-\xi_n)s_n,\ x_{n,1} = x_{n,0}\xi_n\beta_n + x_{n,1}(A_{1,n} + R_n A_{2,n}), \quad (4)$$

and the normalization equation

$$x_{n,0} + x_{n,1}(I - R_n)^{-1}\mathbf{1} = 1. \quad (5)$$

In order to control the presence of MUs within a spatial location, verification of users' identities is important. Let z_k be the SC located on the cell C_k, then at z_k, the SINR pattern of PTs within the cell $C_k \in R^2$ can be obtained from

$$SINR_{z_k} = \frac{P_p G_X |z_k^x|^{-\mu}}{\varphi + I_{pc} + I_{sc}}, \quad (6)$$

where P_p is the PTs' transmit power, φ is the thermal noise signal power, G_X is the channel gain between any tagged PT $x_k \in \Psi_p$ and the SC within C_k and $|z_k^x|^{-\mu}$ gives the Euclidean distance between the tagged PT and the SC with path loss exponent μ. I_{pc} and I_{sc} are the inter-cell interference from other active PTs and interference from active STs (including possible active MUs) respectively at the z_k. The probability that the user currently transmitting in C_k is a PT is the probability that the SINR received at the SC z_k is greater than the pre-defined threshold T_p. This can be obtained as

$$P(P_T) = P\left(\frac{P_p G_X |z_k^x|^{-\mu}}{\varphi + I_{pc} + I_{sc}} > T_p\right), \quad (7)$$

$$= P\left(G_X > \frac{T_p(\varphi + I_{pc} + I_{sc})}{P_p |z_k^x|^{-\mu}}\right).$$

With Rayleigh fading assumption,

$$P(P_T) = \exp\Big(-\varphi\frac{T_p}{P_p|z_k^x|^{-\mu}}\Big)\mathcal{L}_{I_{pc}}\Big(\frac{T_p}{P_p|z_k^x|^{-\mu}}\Big)\mathcal{L}_{I_{sc}}\Big(\frac{T_p}{P_p|z_k^x|^{-\mu}}\Big), \quad (8)$$

where $\mathcal{L}_I(s)$ is the Laplace transform of I at point s.
Under the scenario considered, the interference from other PTs is generated from PTs located outside C_k of radius $r_{p,max}$. Let $s = \frac{T_p}{P_p r_p^{-\mu}}$, by applying the PGFL of PPP,

$$\mathcal{L}_{I_{pc}}(s) = \exp\left\{\frac{-2\pi^2\lambda_p\xi_p(sP_p)^{\frac{2}{\mu}}}{\mu\sin(\frac{2\pi}{\mu})}\right\}. \quad (9)$$

Similarly, interference from STs is generated from STs located outside C_k given as

$$\mathcal{L}_{I_{sc}}(s) = \exp\left\{-2\pi\lambda_s\xi_s\chi_i\int_{r_{p,max}}^{\infty}\frac{T_p P_s}{T_p P_s + r^{\mu}P_p r_p^{-\mu}}rdr\right\}, \quad (10)$$

where $\chi_i = x_{p,0}$ is the probability that the primary queue in cell C_i is empty, obtained from the solutions of (2)–(5), a parameter that depends on the service completion rate of PTs. $P_s \leq P_s^{max} \ll P_p$ is the SUs' transmit signal power, with P_s^{max} being the maximum allowable transmit power for any secondary node. Under the Rayleigh fading assumption and with the path loss propagation model, the SINR pattern of PTs within the cell $C_k \in R^2$ is obtained within the range $r_p = [0, r_{p,max}]$. Hence, the upper bound of $P(P_T)$ is obtained when $r_p = 0$ while the lower bound of $P(P_T)$ is obtained at $r_p = r_{p,max}$. The probability received at each $r_p = [0, r_{p,max}]$ forms the reference value R_p for future verifications.

In a typical slot t, the z_k verifies whether the SINR pattern received from any transmitting user is from PT or MU. The average SINR pattern of such an unknown user $u \in \Psi, \forall\Psi = \{\Psi_p \cup \Psi_s\}$ within the cell $C_k \in R^2$ can be obtained within the cycle v_w as

$$SINR_u = \frac{1}{B}\sum_{b=1}^{B}\left(\frac{P_u G_x |z_k^u|^{-\mu}}{\varphi + I_{pc} + I_{sc}}\right), \quad (11)$$

where B is the number of times SINR was sampled during v_w, $P_u \ll P_p$ is the transmit power and G_x is the channel gain between user u and the SC within C_k. The probability

that the SINR received at z_k is greater than the pre-defined threshold T_p, and hence, from the PT is given as

$$P(P_u) = P\left(\frac{1}{B}\sum_{b=1}^{B}\left(\frac{P_u G_x |z_k^u|^{-\mu}}{\varphi + I_{pc} + I_{sc}}\right) > T_p\right). \quad (12)$$

At $B = 1$, such a probability is simplified as

$$P(P_u) = \exp\Big(-\varphi \frac{T_p}{P_u |z_k^u|^{-\mu}}\Big)\mathcal{L}_{I_{pc}}\Big(\frac{T_p}{P_u |z_k^u|^{-\mu}}\Big)\mathcal{L}_{I_{sc}}\Big(\frac{T_p}{P_u |z_k^u|^{-\mu}}\Big). \quad (13)$$

If $P(P_u) \in R_p$ at the estimated r_p, then the presence of PT is determined, else the presence of MU is confirmed. Such a user is denied access, while the payoff table for such a user is updated. A time-invariant channel is assumed during v_w.

At the beginning of any time slot and within a typical cell, only the ST at the head of such a secondary queue performs channel sensing, while other STs in the queue reduce their energy consumption while waiting. Since STs and MUs are not aware of the arrival rate of PTs, only the received SINR during the sensing window slot is used to determine the state of the channel. While the primary intention of any SU is to maximize the usage of the available white space, any typical MU is interested in disrupting the network or deny SUs service opportunities. We hence incorporated a game theory approach via the mixed strategy Nash equilibrium to aid the removal of MUs from the network. Based on the received SINR pattern at the SCs, users' payoff tables are updated at every attempt to transmit and every completed transmission. Users with lower payoff are malicious and can be removed from the network. Following the analysis presented in [8], the game constraints for any typical SU are derived as,

$$C_Q > C_I > G > c_s;\ R_Q > R_I > c_s, \quad (14)$$

where C_Q is the penalty for either joining the primary queue or violating queue constraints, C_I is the penalty for causing excessive interference on the network, while G is the gain received for accessing the channel. Also, R_Q is the benefit received by the SU for obeying the queueing constraints, R_I is the benefit received for managing interference in the network by vacating the channel upon arrival of any PU and by transmitting with the recommended signal power $P_s \leq P_s^{max}$ for secondary transmission and c_s is the cost of switching channels to access the unused channels (or cost of staying and waiting for spectrum opportunity).

For any typical MU, the game constraints can be expressed as

$$G > c_m;\ C_A > c_m, \quad (15)$$

where c_m is the cost of emulating PUs' behavior for the purpose of deceiving SUs or causing interference by generating signal power $P_m > P_s$ and C_A is the benefit of causing interference in the network. The condition $C_Q > C_I$ is necessary to discourage violation of queueing constraints by the SUs, $C_I > G$ is necessary to prevent SUs from causing inference in the network, encouraging them to transmit at the specified transmit power while vacating the channel upon arrival of any PU. $G > c_s$ is useful to encourage SUs to switch between channels so as to occupy the unused spaces in the network. Also, the condition $R_Q > R_I$ is useful to reward SUs that obey queueing principles, while $R_I > c_s$ is necessary to encourage SUs to switch channels or withhold transmission upon arrival of any PU.

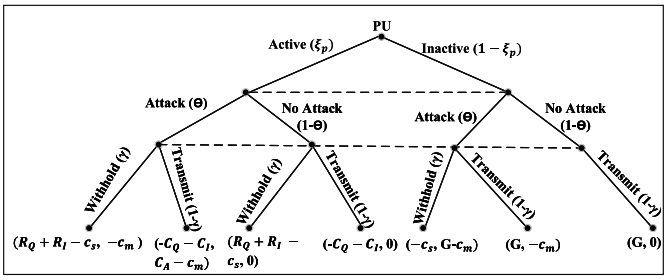

Fig. 3. Game tree in a typical slot.

Similarly, the constraint $G > c_m$ shows that an MU benefits more from securing access to a channel through deceptive means than the cost of emulating PUs' behavior, while $C_A > c_m$ shows more reward for an attacker when causing interference in the network. Generally, the benefit is in the form of spectrum opportunity, while the penalty is in the form of removal or blockage from the network.

Considering a typical slot, users' actions can be depicted using payoff chat, as shown in Table I.

TABLE I
PAYOFF MATRIX FOR THE GAME IN A TYPICAL SLOT

Case 1: PU active (ξ_p)

(SU, MU)	Attack	No Attack
Transmit	$-C_Q - C_I, C_A - c_m$	$-C_Q - C_I, 0$
Withhold	$R_Q + R_I - c_s, -c_m$	$R_Q + R_I - c_s, 0$

Case 2: PU inactive ($1 - \xi_p$)

(SU, MU)	Attack	No Attack
Transmit	$G, -c_m$	$G, 0$
Withhold	$-c_s, G - c_m$	–

Table I can be summarized as shown in Fig. 3. Let μ_s and μ_m represent the service completion rate of any typical ST and MU respectively. The expected reward of such an ST and MU in the absence of PU is given in (16) and (17) respectively.

$$E[R_{ST}] = \mu_s G + (1 - \mu_s)(-c_s). \quad (16)$$

$$E[R_{MU}] = \mu_m (G - c_m). \quad (17)$$

As shown in Fig. 3, the actions of all users are not predictable, hence, the mixed strategy Nash equilibrium method can be used to analyse the expected payoff of SUs and MUs

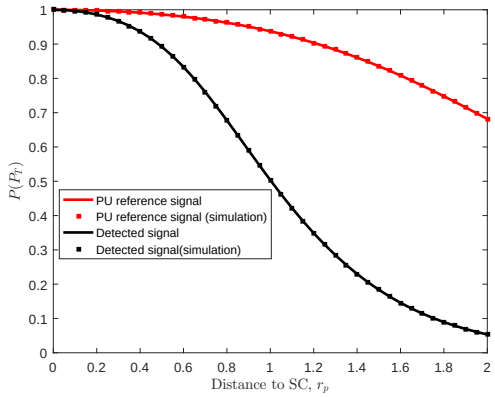

Fig. 4. Received signal probability, $\xi_p = 0.2$, $\xi_s = 0.5$.

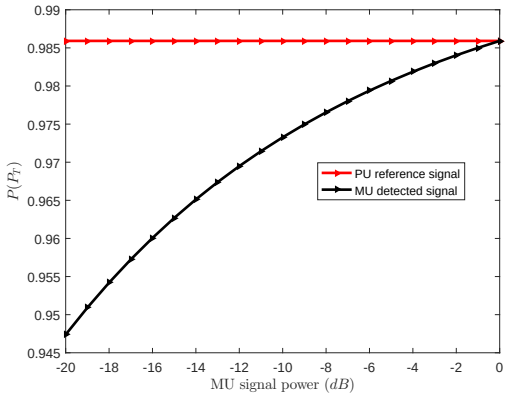

Fig. 5. Received signal probability, $\xi_p = 0.2$, $\xi_s = 0.8$.

[6], [8]. Let γ be the probability that a tagged ST withholds its transmission on a typical channel and $\bar{\gamma}$ be the probability that such an SU transmits; we can similarly define θ as the probability that a tagged MU attacks the typical channel or $\bar{\theta}$ if it decides not to attack the channel. The expected payoff of the SU is given as

$$E[S] = \xi_p[\gamma(R_Q + R_I + C_Q + C_I - c_s) - C_Q - C_I] + (1 - \xi_p)[G - \theta\gamma(c_s + G)]. \quad (18)$$

Similarly, the expected payoff of the MU is given as

$$E[M] = \xi_p\theta[C_A(1 - \gamma) - c_m] + (1 - \xi_p)\theta[\gamma G - c_m]. \quad (19)$$

IV. Numerical Results and Simulation

We now present the simulations of the analysis presented in this paper. Except when stated otherwise, the following parameters were used for simulations: $\lambda_s = 0.3$, $\lambda_p = 0.03$, $T_p = 10dB$, $r_{p,max} = 1.2m$, $P_p = 0dB$, $P_s = -32dB$, $\mu = 4$ and $\varphi = -180dB$. Also, for the mixed strategy Nash equilibrium obtained during one slot, we used $G = 50$, $C_Q = 65$, $C_I = 60$, $C_A = 40$, $R_Q = 25$, $R_I = 20$, $c_s = 15$ and $c_m = 25$. We carried out Monte Carlo simulation averaged over 10 000 simulations to validate our analysis.

Fig. 4 shows the relationship between the received signal probability and the distance of the active user from the SC. At each estimated distance, the SC confirms whether the estimated distance and the obtained SINR signal correspond with their respective values in the reference table. If such values correspond, a PU is detected, else a malicious operation is detected. Fig. 5 shows that under the considered scenario, it is difficult for any typical MU to match the known reference signal at the SC. The PU signal can only be matched when MU transmits with a transmit power equal to that of PU, a situation which is unlikely, owing to the transmission capability of PUs in CRN.

The expected SU and MU payoffs are presented in Fig. 6 and Fig. 7. In Fig. 6, the expected payoff is shown to increase when legitimate SUs desist from transmitting either by waiting

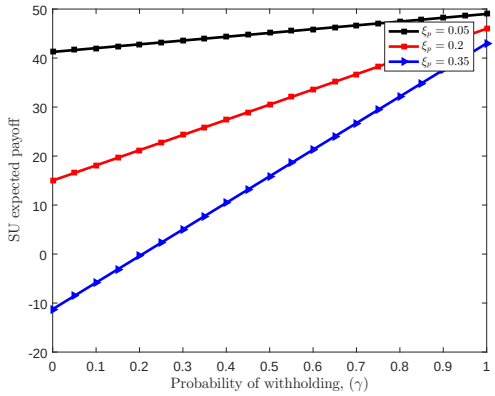

Fig. 6. The expected SU payoff.

until the primary queue is empty or by switching to another channel with an empty primary queue. With an increase in PTs' arrival rate, SUs are penalized for transmitting on a busy channel, as that will generate interference in the primary network. The low expected payoff of the MUs signifies the level of penalty suffered by MUs for not obeying queue and transmission requirements. With more attacks launched, the SC updates the MU payoff table and can make subsequent decisions to remove or block such a user from future access to the channel.

Users' payoff serves as a good metric for channel access. Any legitimate SU can be marked as malicious if its activities suggest a turn away from the required activities for legitimate users. Our approach similarly prevents spectrum sensing data falsification attack - an attack in which an MU sends false sensing results to the other nodes in the network in order to either deny them spectrum opportunities or increase interference in the network.

V. Conclusion

In this paper, we present a game theoretic based SINR detection approach to control the presence of MUs in CRN. The spatiotemporal behavior of the system was captured using

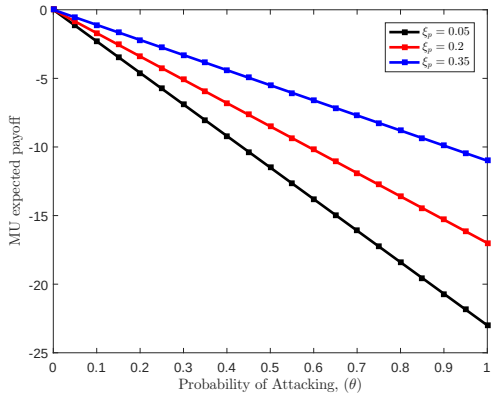

Fig. 7. The expected MU payoff.

the tools of SG and queueing models. The use of a vacation-based Geo/PH/1 discrete-time Markov chain queuing model was employed for each cell owing to its simplified memoryless inter-arrival process and its general departure process that can account for the interference-based interactions between the primary and secondary queues in the network. MUs were penalized for violating queuing and interference requirements in the network. Through SCs, the activities of every active user can be verified through the reference table, containing the reference PU SINR and the corresponding distances. We assumed that SC is able to estimate the location of each active user while also capturing the SINR received. In the proposed approach, SUs can go into hibernation when they are not at the head of the secondary queue in order to reduce energy-wasting while waiting.

REFERENCES

[1] C. H. Lee, and M. Haenggi, "Interference and outage in Poisson cognitive networks," IEEE Transactions on Wireless Communications, vol. 11, no. 4, pp. 1392–1401, Feb. 2012.

[2] U. Tefek, and T. J. Lim, "Interference management through exclusion zones in two-tier cognitive networks," IEEE Transactions on Wireless Communications, vol. 15, no. 3, pp. 2292–2302, Nov. 2015.

[3] X. Song, X. Meng, X. Shen, and C. Jia, "Cognitive radio networks with primary receiver assisted interference avoidance protocol," IEEE Access, vol. 6, pp. 1224–1235, Nov. 2017.

[4] H. H. Yang, and T. Q. Quek, "Spatio-temporal analysis for SINR coverage in small cell networks," IEEE Transactions on Communications, vol. 67, no. 8, pp. 5520–5531, May 2019.

[5] M. Gharbieh, H. ElSawy, A. Bader, and M. S. Alouini, "Spatiotemporal stochastic modeling of IoT enabled cellular networks: Scalability and stability analysis," IEEE Transactions on Communications, vol. 65, no. 8, pp. 3585–3600, May 2017.

[6] S. Yazdi, and M. Ghazvini, "Countermeasure with primary user emulation attack in cognitive radio networks, Wireless Personal Communications, vol. 108, no. 4, pp. 2261–2277, Oct. 2019.

[7] Y. Li, X. Ma, M. Wang, H. Chen, and L. Xie, "Detecting Primary User Emulation Attack Based on Multipath Delay in Cognitive Radio Network," Springer Science, Smart Innovations in Communication and Computational Sciences, vol. 669, pp.361–373, June 2018.

[8] Y. Tan, S. Sengupta, and K. P. Subbalakshmi, "Primary user emulation attack in dynamic spectrum access networks: a game-theoretic approach," IET Communications, vol. 6, no. 8, pp. 964–973, May 2012.

[9] Q. Dong, Y. Chen, X. Li, K. Zeng, and R. Zimmermann, "An adaptive primary user emulation attack detection mechanism for cognitive radio networks," in International Conference on Security and Privacy in Communication Systems, Springer, pp. 297–317, Aug. 2018.

[10] D. Das, and S. Das, "Intelligent resource allocation scheme for the cognitive radio network in the presence of primary user emulation attack," IET Communications, vol. 11, no. 15, pp. 2370–2379, Aug. 2017.

[11] K. Li, and J. Wang, "Optimal joining strategies in cognitive radio networks under primary user emulation attacks," IEEE Access, vol. 7, pp. 183812–183822, Dec. 2019.

[12] B. Naqvi, S. Murtaza, and B. Aslam, "A mitigation strategy against malicious primary user emulation attack in cognitive radio networks," in IEEE international Conference on Emerging Technologies, Islamabad, Dec. 2014, pp. 112-117.

[13] A. Alahmadi, Z. Fang, T. Song, and T. Li, "Subband PUEA detection and mitigation in OFDM-based cognitive radio networks," IEEE Transactions on Information Forensics and Security, vol. 10, no. 10, pp. 2131–2142, Jun. 2015.

[14] C. Xin, and M. Song, "Detection of PUE attacks in cognitive radio networks based on signal activity pattern," IEEE Transactions on Mobile Computing, vol. 13, no. 5, pp. 1022-1034, May 2014.

[15] R. Di Pietro, and G. Oligeri, "Jamming mitigation in cognitive radio networks," IEEE Network, vol. 27, no. 3, pp. 10–15, Jun. 2013.

[16] A. Sivakumaran, A. S. Alfa, and B. T. Maharaj, "An empirical analysis of the effect of malicious users in decentralised cognitive radio networks," in IEEE Vehicular Technology Conference, Kuala Lumpur, April 2019, pp. 1-5.

[17] R. Chen, and J. M. Park, "Ensuring trustworthy spectrum sensing in cognitive radio networks, in IEEE Workshop Networking Technology and Software Defined Radio Networks, Reston, pp. 110-119, Sept. 2006.

[18] Z. Chen, T. Cooklev, C. Chen, and C. Pomalaza-Rez, "Modeling primary user emulation attacks and defenses in cognitive radio networks," in IEEE International Performance Computing and Communications Conference, Scottsdale, Dec. pp. 208–215.

[19] F. Paisana, N. Marchetti, and L. DaSilva, "Radar, TV and cellular bands: Which spectrum access techniques for which bands?," IEEE Communications Surveys and Tutorials vol. 16, no. 3, pp. 1193–1220, 2014.

[20] Q. Dong, "Primary User Emulation Attack Detection in Cognitive Radio Networks," Doctoral dissertation, State University of New York at Binghamton, 2018.

[21] M. Khasawneh, and A. Agarwal, "A collaborative approach for monitoring nodes behavior during spectrum sensing to mitigate multiple attacks in cognitive radio networks," Security and Communication Networks, vol. 2017, Oct. 2017.

[22] A. S. Alfa, "Applied discrete-time queues," Springer New York, 2016.

[23] A. S. Alfa, "Discrete time queues and matrix-analytic methods, Top, vol. 10, no. 2, pp. 147–185, Dec. 2002.