Defence against responsive and non-responsive jamming attack in cognitive radio networks: an evolutionary game theoretical approach

Shyamala Bharathi, Dhananjay Kumar, Deepak Ram

Department of Information Technology, Madras Institute of Technology, Anna University, Chennai 600 044, India
E-mail: pshyamala@mitindia.edu

Published in *The Journal of Engineering*; Received on 24th July 2017; Accepted on 6th November 2017

Abstract: An anti-jamming system based on Stackelberg game theory has been used in past to model the sequence of events of a jamming game in cognitive radio network. However, this approach fails to support the improvement of strategy in counteracting responsive and non-responsive attack. The proposed anti-jamming system selects a suitable strategy based on channel availability and jammer type. When channel availability is high, the interaction between cognitive radio and jammer is modelled using hidden Markov process, but when it is low, evolutionary game theory (EGT) is used. Furthermore, in the case of responsive jammer, a distraction strategy is incorporated to deceive the jammer, but Nash equilibrium is attained while dealing with mixed strategy of non-responsive jammer. The simulation results show that the proposed EGT-based anti-jamming system increases the throughput of system while decreasing the probability of bit error at least by 2% compared to the existing Stackelberg game approach.

1 Introduction

Cognitive radio networks (CRN) can play a vital role in accomplishing ubiquitous computing considering the limited availability of spectrum. However, due to the exposed nature of wireless links, CRNs are vulnerable to jamming attack that amounts to denial-of-service [1]. Besides common communication vulnerabilities in wireless, CRNs are liable to other sorts of threats correlated to the intrinsic characteristics of dynamic spectrum access [2]. In recent times, study works have been done in the vicinity of CRN security and especially the issue of opportunistic spectrum access in the presence of jammer.

The jamming attacks are prominently categorised into two types [3], namely (i) responsive jammer and (ii) non-responsive jammer. In the responsive or reactive jamming attack, the adversary targets certain frequency bands depending on cognitive radio (CR) users' activity. However, the attacker should have high sensing and tracking capability to find the user activity in the radio spectrum. When a jammer finds user activity in the channel, they target higher power signal to that specific frequency band which is of interest to override user signal. Here, the jammers will always try to conserve energy by spending power judiciously to achieve specific jamming goals and will not spend energy elsewhere intentionally [4]. The non-responsive jammer has two popular types, the sweep jammer will cover all available frequency band in a fixed duty cycle and the random jammer which remain inactive for certain random time and jams for a certain period with no defined pattern.

Conventionally [5], anti-jamming learning is performed in the physical layer via a few anti-jamming modulations, for instance, spread spectrum, or in the level over MAC via channel switching. Even though, if a CRN have an anti-jam in the PHY-layer transmission system, it may be sensitive to jamming because of a unique character of CRN, that it has to leave a channel even in the existence of minor jamming or interference [6]. This indicates that a jammer can use low energy signals to jam multiple channels at the same time. Additionally, if the CRN can pertain channel hopping to evade jamming, such methods may be expensive because next channel set-up through switching in CRN may be time-consuming due to the required timing/frequency synchronisation, channel estimation, handshaking for information exchange, and network set-up. The key problem is that the available channels may be time-varying, and the information about the available channels may not be identical among the CRN nodes. If not carefully designed, the channel switching procedure can greatly reduce the throughput of the CRN.

The proposed anti-jamming defence module majorly assists the system in the channel selection for frequency hopping to evade jammer. The anti-jamming defence module gets activated only when the number of available idle channels reduces <75% in the radio environment. When channel availability is high, the system uses frequency hopping spread spectrum (FHSS) technique to dynamically access idle frequency bands in the spectrum to avoid any kind of interference. The cognitive radio with anti-jamming module is shown in Fig. 1.

The CRN anti-jamming system model provides us the high-level overview of operations in the cognitive radio environment. Spectrum sensing is being aware of the radio environment in which cognitive radio operates. A cognitive radio must have the capability to sense the spatial and temporal radio environment in its service area [7]. Spectrum analysis is the examination of all cognitive radio parameters sensed in the previous stage. In the analysis stage, cognitive radio will consider all parameters available at its disposal to deduce an optimal channel and protocol for establishing reliable communication in the radio environment at a given time and condition. Some of the important parameters to be considered in the analysis stage are availability of idle channels, transmission power of other users, environmental noise, and local policies.

The decision maker unit is where the inputs from the spectrum sensor, analyser, and anti-jamming defence module are used to compute optimal channel for establishing communication. Though at spectrum analysis stage itself optimal channel identification is achieved, the radio channel specified in the spectrum decision stage is given final preference. As the spectrum decision maker algorithm will consider inputs from anti-jamming defence module, which can provide intelligence and strategy to overcome a jamming attack on CRN. Based on the input from decision maker stage, a cognitive radio system will dynamically adjust its operational radio parameters, such as transmission power and frequency, to ensure the desired connectivity.

The rest of the paper is organised as follows. Section 2 discusses the work in related works, Section 3 provides the system model and design of anti-jamming module and analyses the probability of bit error and throughput calculation. In Section 4, the simulation results are discussed with implementation details. Section 5 presents the conclusion and scope for future work.

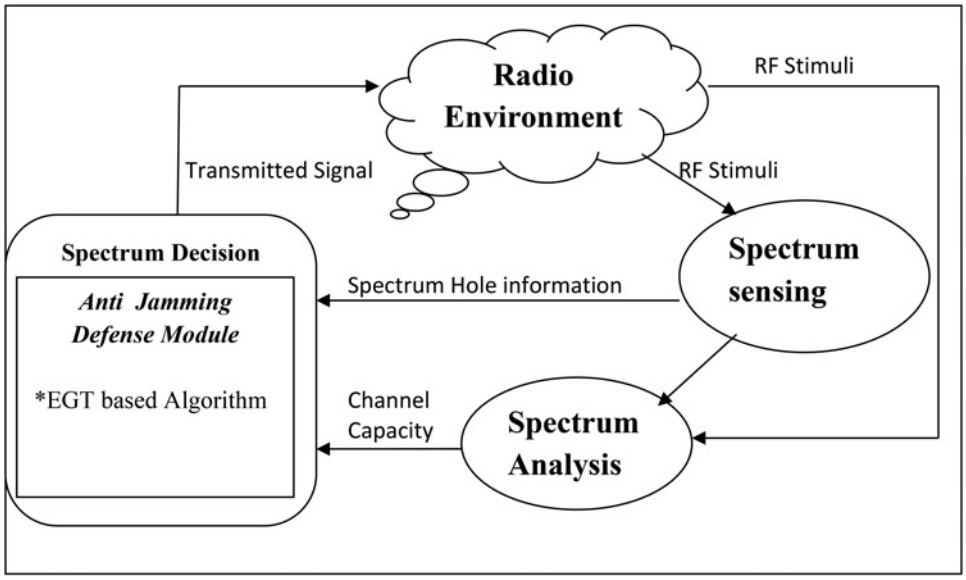

Fig. 1 *CRN anti-jamming system model*

2 Related works

In some cases, the FHSS technique is used as method to evade jammer's signal interference [8]. Having a frequency hopping technique system based on pseudo-random sequence alone would not be sufficient to tackle jamming attacks, because a skilled attacker may find radiofrequency (RF) hopping sequence used in the network at some point in time by carefully studying the transmission pattern. Hence, it is essential to develop a frequency hopping technique which is adaptive in nature to successfully evade a responsive jammer [9]. Many anti-jamming schemes use algorithms based on Markov decision process (MDP) to select the suitable idle available channels for transmission.

The MDP [10] is good at predicting future states with the limited information and works based on Markov chain, but it is found to be linear in logic so in security perspective, it is vulnerable to attack as the attacker can also predict the probable sequence of channels to be used in future for transmission with the same information available to the user and jammer in the cognitive radio environment. Hence, there arises a need to develop an anti-jamming system with adaptive frequency hopping to mitigate the risk of channel prediction by jammer and enhance the performance of the system by decreasing the probability of bit error rate to improve the throughput of system. Given there is a chance, we improve the outputs of both the models, i.e. hidden Markov model (HMM) and evolutionary game theory (EGT), to find most suitable channel for transmission and conserve power at CR node by selecting available low-frequency bands for signal transmission.

The channel state information from sensing unit subjected to further scrutiny using HMM Viterbi algorithm [2]. Two things can be achieved by this action; first, the algorithm will filter out some unfavourable channels. Second, idle channels identified to be suitable for transmission will also have certain degree of randomness when compared with the MDP-based approach. The randomness in channel selection due to HMM provides us an advantage in security scenario, because it makes it difficult for any proactive jammer to rendezvous a CR node transmission using tracking and prediction.

The channel states are deduced with inputs of random initial probability of states, transition matrix, and observation matrix constructed from observed emissions. Here, three emissions can be observed from each state [7]. We consider sensing unit of cognitive radio uses energy detection sensing technique to sense channel availability and this input is fed to the algorithm as one of the emissions, the channel noise condition is taken as second emission, and transmission power required for transmitting in certain frequency bands is the third emission (e.g. if some channels are found to be idle at higher frequency bands, to transmit information in that channel the radio transmitter requires high power to generate the frequencies). Given all these information, we compute the most likely channel states with the algorithm as in [11].

When there exists a strategic situation involving two or more nodes, game theory can be one of the most convenient techniques used to mathematical model and analyse the strategic situation in the system [12], but not all game theoretical concept can be used to model the interaction of cognitive radio node and jammer for anti-jamming capability improvement needs as the cognitive radios are inherently dynamic in nature and the introduction of the jammer will further add complexity to the system. Hence, there is a need to choose an efficient game theoretical concept to assist the cognitive radio system to efficiently counter the jammer's strategy and to improve the system performance.

Game theory provides greater insight into the problem and it can handle all critical variables that influence the course of game. Game theory involves two players the monitor nodes and the jammer. The principle of jammers is to exploit the denial of channel access to the rightful users, while rightful nodes aim to maximise their communication throughput. The game theory help us to find best response for all circumstances encountered in the game and through which a player can maximise their utility and eventually win the game or successfully overcome the challenges posed by making best use of the resources at their disposal. The modelling of anti-jamming system using Stackelberg game [13] describes the interaction between CR and jammer as leader and follower.

In [14], uses the Stackelberg game theoretical modelling i.e. to commit error in measuring channel states to improve SU utility. But, the fact is that the SU has no control over it here, ending up always being chased by jammer and blocked in the majority of situations. Hence, it is essential to explore other game theories that could give SU a chance to improvise strategy at critical conditions in a CR-based anti-jamming system. To overcome these challenges, we propose EGT to model the interaction between the CR node and jammer in the anti-jamming system. Evolutionary games were proposed to adjust the transmit powers of users and mitigate interference. However, instant information

exchange is required between the users, which are hard to realise in practice.

In [15] the evolutionary game, every player with passion adjusts his/her strategy through observing the utilities in different strategies. An effective move towards for a group of players join to a stable equilibrium after a period of strategic communications, and such a stable equilibrium is called as an evolutionarily stable strategy (ESS). In a distributed system, all players tentative about others behaviour and utilities. To improve their own utility, every player will attempt different strategies in dissimilar rounds of play and study from the communications using the methodology of understanding-by-building. In this method, the part of players using an assured pure strategy may differ with time. In the evolutionary game, replicator dynamics are used to model such a population evolution

An ESS is a strategy when all members in a population adopt will make the conditions difficult for a mutant to invade it successfully [16]. In the operations environment of our system, sometimes certain conditions may arise, where there is a need to switch between two strategies. We find mixed strategy Nash equilibrium (NE) to determine the type of jammer. In the case of responsive jammer, we use distraction strategy to counter jammer and with non-responsive jammer we do not use distraction which will help us save power in CR node. The switching between two alternatives makes our strategy a mixed ESS; these conditions are explained in detail here.

3 Design and methodology

In this work, we assume that jammer either in reactive or proactive method is always present in the radio environment. The working procedure of anti-jamming module indicates that all the decisions and state changes happen only based on channel availability, rather than the type of jammer. The anti-jamming capability improvement in the CRN is achieved through three-step process as follows:

- The FHSS technique is used when channel availability is CA ≥ Ut.
- HMM-assisted adaptive frequency hopping is applied when channel availability range is Lt> CA < Ut
- EGT-assisted adaptive frequency hopping is used when channel availability range is CA ≤ Lt.

Where CA is the channel availability, Ut the upper threshold, and Lt the lower threshold of idle channel availability.

The anti-jamming defence module helps decision-making in the cognitive radio under jamming attack, they are implemented between spectrum analyser and decision-making component in the cognitive radio architecture and the working procedure of the module is given below.

1. Initialize CA, U_T, L_T // Channel availability, lower and upper threshold
2. Sense channel availability in the network
3. If channel availability is ($CA > U_T$)
4. Initiate transmission using frequency hopping spread spectrum technique
5. If transmission is successful Go to Step 6
6. Else, if channel availability ($L_T > CA < U_T$)
7. Initiate Anti-jamming defence module (responsive jamming)
8. Continuously sense channel availability
9. If channel availability improves to ($CA > U_T$), Go to Step 3
10. Else, if channel availability is (CA < UT)
11. Initiate Anti-jamming defence module (non-responsive) based on
12. Evolutionary game theory for optimal channel selection
13. If transmission is successful go to Step-6
14. Continuously sense channel availability
15. If channel availability improves i.e. ($L_T > CA < U_T$), goto Step-4.
16. Else if channel availability improves further i.e. (CA U_T), goto Step-3
17. Stop

The system is designed in that way because when a system is under jamming attack, it is not possible for us to identify the type of jammer, i.e. whether it is a responsive or non-responsive at the initial stages itself, only upon certain interactions between CR and jammer in a transmission window, the type of jammer can be determined. This act of profiling jammer nature will help us make some strategy changes at critical state (CA ≤ Lt) to improve the performance of anti-jamming module.

3.1 Hidden Markov model and Viterbi algorithm-based channel selection

The Viterbi algorithm based on HMM is used to deduce the most likely channel states when (Lt > CA <Ut). The HMM is preferred over the conventional Markov model process is because the HMM is a doubly embedded stochastic process, where one state is always hidden and can be found by only observing another state. This set-up provides a good framework for modelling an anti-jamming system and the channel state prediction in the CRN scenario as the channel state information we get is mostly ambiguous.

The Viterbi algorithm output based on the random transition and emission probabilities will compute a channel condition to be any one of the following three states, i.e. channel idle, not favourable, or channel busy. The channels states deduced based on the algorithm are filtered further with below condition to choose most suitable channel for data transmission considering the jammer in the network. The main criterion for choosing the most suitable channel lies in the proximity of the idle channel to other currently used frequency bands either by primary or by secondary user. That is, if the HMM Viterbi deduced idle or favourable channel for transmission was found to be within the range of ±1 kHz frequency currently used for transmission by primary user/other secondary users, that channel will not be considered for transmission as it has high probability of getting sensed and jammed by responsive jammer with low reaction time [17]. To explain this scenario, let us suppose if the jammer is trying block adjacent frequency bands used by primary or secondary user, then there is a chance that jamming signal may cause interference to our transmission in nearby frequency bands due to spill over. This stringent channel selection helps the adaptive frequency hopping to avoid jamming-related interference when channel availability range is Lt > CA <Ut in the radio spectrum.

3.1.1 Hidden Markov model: Viterbi algorithm: The dynamic programming-based Viterbi algorithm is used to deduce the most likely channel state based on observations of emissions from each channel. The channel state is deduced with inputs of initial probability of states, transition matrix, and observation matrix constructed from observed emission of each channel state

$$\delta_{n+1}(j) = b_j(y_{n+1}) \max_{1 \le i \le M} \left[\delta_n(i) \boldsymbol{a}_{ij} \right], \quad 0 \le j \le M \tag{1}$$

$$\psi_{n+1}(j) = \arg\max \left[\delta(i) \boldsymbol{a}_{ij} \right], \quad 0 \le j \le M \tag{2}$$

where b is the initial probability, δ the hidden state sequence, δ_n stores the probability of the most likely path and it forms transition matrix, $\boldsymbol{a}_{ij}$ the observation matrix, and ψ_n stores the probability of the most likely path the arg max value of δ_n. After the maximisation, the termination and backtracking takes place.

1. Initialise the value $\delta_0(i)$
2. Initialise n, where $n=0$

(a) for $n=0, 2,\ldots,N-1$.
Compute the most likely path using (1)
Calculate the maximisation by using (2)
end for

3. Initialise termination with the equation given below

$$\hat{x} = \arg \max_{1 \le i \le M} \delta_N(i)$$

4. Initialise backtracking with the equation given below

for $n=N-1, N-2,...,0$

$$\hat{x}_n = \psi_{n+1}\left(\hat{x}_n + 1\right)$$

end for

The Viterbi algorithm output based on the random transition and emission probabilities will compute a channel condition to be any one of the following three channel states, i.e. channel idle, not favourable, and channel busy.

3.2 Problem formulation using EGT

The interaction between the cognitive user and the jammer is modelled as an evolutionary game with constant resources in which the cognitive user being the controller, seek out to prevent the jamming attack by distributing its power in a smart method to decrease the cumulative bit error rate (BER) caused by the jammer. The jammer, alternatively, aims at troublesome the system performance by assigning jamming power to dissimilar frequency bands. To resolve the game, an evolutionary algorithm is proposed which can discover a mixed-strategy NE of the evolutionary game. The effect of jamming can be measured by the CRN's receiver side signal to interference noise ratio (SINR) which can be evaluated by the constraint

$$\Gamma_i = \frac{P_i T_i}{P_j T_j + N T_i} = \frac{P_i}{P_j(T_j/T_i) + N_0} \tag{3}$$

We assume that the cognitive user CR user i and the jammer J have a limited power budget, denoted by P_i and P_J, respectively. T_i and T_j be the channel sensing and transmission capability period of time cognitive user and jammer, N_0 is the signal noise, and we assume that there is an SINR threshold Γ_0 such that, then the cognitive user transmission is jammed. The jammer challenges at compromising the system performance by distributing its power over the channels so as to humiliate the effective SINR and enhance the BER. Suppose, to successfully transmit data over the channels, the received effective SINR must exceed a threshold Γ_0, the condition that a user having a successful transmission over a channel is given as

$$\Gamma_i < \Gamma_0, \tag{4}$$

If the jammer cannot attack the cognitive users perfectly, assume next transmission will be successful. h the CU is jammed then the CU need to spend time T_s to switch to a new position for transmission. As the jammer could not track properly, assume that the next transmission be successful and the throughput of CU transmission is subject to

$$R_{\mathrm{CU}} = \frac{1 - P[J]P[\Gamma_i < \Gamma_0]}{1 + (T_s/T_i)P[J]P[\Gamma_i < \Gamma_0]} \tag{5}$$

where $P[J]$ denotes the jamming probability that it successfully inferred the channel avail by the CU, $P[\Gamma_i<\Gamma_0]$ is the probability that the received SINR is less than the threshold value Γ_0 and it insists CU to switch channel.

To prevent the jamming attack, the SU must share out its power over the set of frequencies in optimal manners which reduce the effect of jamming and remains the SINR above for as many channels as possible. On the other hand, the SU does not have any prior information about which channel the jammer may decide to jam and thus it has to act proactively based on the past observations of the jammer's behaviour. Analogous to [18], we define the SU's payoff as the number of successful transmissions over M available channels

$$U_{\mathrm{CU}}(P_i, J_i) = \frac{1}{N} \left\| \{ i | \Gamma i \ge \Gamma_0 \} \right\|, \tag{6}$$

where $\|.\|$ indicates cardinality of the set. Similarly, also compute the jammer's payoff as the number of failed transmissions over N existing channels

$$U_J(P_i, J_i) = \frac{1}{N} \left\| \{ i | \Gamma_i < \Gamma_0 \} \right\|. \tag{7}$$

The utility functions in (4) and (5) expose that the payoff of every player depends on equally of its own power allocation strategy and that of its challenger. Therefore, we model it as the evolutionary game framework that provides the fundamental of mixed strategic resource allocation in multiple dimensions, where two players contend over a number of independent trials and the player with effective SINR that allocated higher level of SINR wins.

3.3 Evolutionary stable strategies

The proposed EGT based anti-jamming module is developed with three strategy S1, S2, and S3, where S3 is the final strategy of CR chosen from S1 and S2 (i.e. a strategy logically opposite to that of jammer strategy).

(i) The CR user will transmit (frequency hopping sequence to receiver) in channel 1 (S1 – best response strategy of CR node).
(ii) Sensing activity in channel 1 responsive jammer will transmit in the same frequency with higher power to block channel (S1 – best response strategy of jammer).
(iii) The CR user begins transmission of frequency hopping sequence and data to receiver in channel 2, by the time jammer sense the activity in channel 2 and introduces interference to block it, most of or all the data transmission would have completed (S2 – final best response strategy of CR node).

Though the final best response strategy of the CR user in the game uses either S1 or S2 as its second strategy to evade jammer, it is identified to be a separate new third strategy (S3) adopted by a player in the game. So, the low key CR's frequency hopping sequence transmission in the first strategy (S1) will effectively distract jammer to buy some time for data transmission in strategy (S3). We also suppose all communication between transmitter and receiver are being secured with efficient encryption standards to prevent eavesdropping. The payoff matrix for above sample EGT anti-jamming game is shown in Table 1.

Let us consider the sample payoff of EGT game as given in Table 1, based on this payoff matrix, it is seen that CR user and jammer are gaining one unit for success and should any player fail, they will earn nothing that is zero. For the detailed mathematical analysis of the interaction between CR user and jammer, we consider for any failure, the player will lose one unit. The modified, payoffs of both jammer and CR user will look like the one as given in Table 2.

The mathematical analysis of EGT payoff reveals that the interaction between CR user and reactive jammer was a zero-sum game, with equal probability of success for both CR user and responsive jammer. Suppose, if we happen to encounter a non-

Table 1 EGT payoff matrix of sample anti-jamming game

Strategy of CR user and jammer	CR user (S3)	
	S1	S2
S1, S1	0, 1	1, 0
S1, S2	1, 0	0, 1
S2, S1	0, 1	1, 0
S2, S2	1, 0	0, 1

Table 2 EGT payoff matrix of CR and jammer

Strategies CR user and jammer	CR user	Jammer
S1S1S1	—	1
S1 S1S2	1	—
S1 S2S1	1	—
S1 S2 S2	—	1
S2 S1 S1	—	1
S2 S1 S2	1	—
S2 S2S1	1	—
S2 S2S2	—	1
Total	0	0

responsive jammer be it sweep jammer or random jammer, the strategy of transmitting a decoy signal, which we adopt to distract jammer, is useless here, because the non-responsive jammer may not be looking out for user activity as opposed to the responsive jammer. A random or sweep jammer will have its own agenda to introduce interference in the channel. Hence, to improve our utility in the non-responsive jamming scenario, i.e. chance to successfully evade jammer and to conserve transmission power at CR node, we are mixing strategies of CR user and jammer to get insight on channels that are frequently blocked by jammer. To determine both the CR user and jammer preference on channels based on their interaction, we find mixed strategy NE.

3.4 *Subgame perfect Nash equilibrium*

To find subgame perfect Nash equilibrium (SPNE), let us suppose we have eight idle channels in the cognitive radio environment at an instance. Eight channels are split into two halves, namely left side and right side as shown in Fig. 2.

The payoff matrix of a game will look like the one as given in Table 3, where the rows and columns hold information about the percentage of channel utilisation by both CR user and jammer in a region.

Both CR user and Jammer have equal success rate and it shows that there is no pure NE. Since the game is symmetric, we analyse the mixed strategy NE using strategies played by both players. Suppose, the available spectrum is split into two halves, i.e. left and right. The NE for CR user $(p, (1-p))$, using jammer's payoff

$$L_p = JL_1(p) + JL_2(1-p) \tag{8}$$

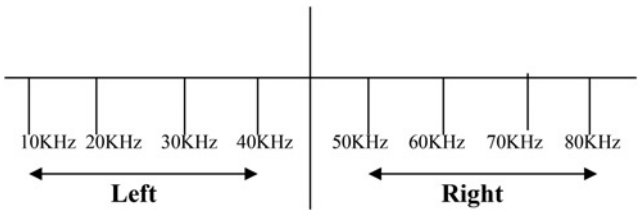

Fig. 2 *Radio spectrum split into two regions*

Table 3 EGT payoff matrix of sample for mixed strategy

CR user	Jammer		
	Left, in %	Right, in %	
left	CL_1, JL_1	CL_2, JR_1	$\boldsymbol{P}$
right	CR_1, JL_2	CR_2, JR_2	$(1-p)$
	Q	$(1-q)$	

$$R_p = JR_1(p) + JR_2(1-p) \tag{9}$$

Since it is a mixed strategy, we equate (8) and (9) and we get

$$J_1(p) + J_2(1-p) \tag{10}$$

Simplifying the above constraint

$$p = \frac{J_1(p) + J_2}{J_2} \tag{11}$$

$$\mathrm{CR} = \big(p, (1-p)\big) \tag{12}$$

NE for jammer $(q, (1-q))$ using CR user's payoffs

$$L_q = \mathrm{CL}_1(q) + \mathrm{CL}_2(1-q) \tag{13}$$

$$R_q = \mathrm{CR}_1(q) + \mathrm{CR}_2(1-q) \tag{14}$$

Since it is a mixed strategy, we equate (13) and (14), then we get

$$C_1(q) + C_2(1-q) \tag{15}$$

By simplifying, (10) becomes

$$q = \frac{C_1(q) + C_2}{C_2} \tag{16}$$

$$J = \big(q, (1-q)\big) \tag{17}$$

$$\mathrm{NE} = \mathrm{CU}\big(p, (1-p)\big), J\big(q, (1-q)\big) \tag{18}$$

In EGT, fitness of the player is calculated using (19) and (20) as given in [19]

$$F(\sigma) = F_0 + q\Delta F(\sigma, \sigma) + p\Delta F(\sigma, m) \tag{19}$$

$$F(m) = F_0 + q\Delta F(m, \sigma) + p\Delta F(m, m) \tag{20}$$

where σ is the strategy of a player in the game and m a mutant strategy which invades the population, $q = (1-p)$, where p is the percentage of the population following the strategy m. The $\Delta F(S1, S2)$ denotes the change in fitness. Furthermore, each player in the population has an initial fitness of F_0.

The mathematical analysis of CR user and jammer interaction in an anti-jamming game helped us understand that the CR user's channel preference based on sides (i.e. the probability of choosing channels in the left and right side of spectrum). When we analysed the jammer's interaction with CR user, we find jammer's channel preference (i.e. the probability of choosing channels in the left and right side of spectrum). The results obtained from mathematical analysis can have a direct effect on the strategy adopted by CR user in the future interactions because, now that we know the jammer's side preference by studying some interactions, the CR user can make use of the information in future and lean more towards the favourable side (i.e. choose channels on sides which is less likely to be used by jammer) to evade jammer successfully. The EGT

doi: 10.1049/joe.2017.0285

1. Initialization: State each player i {1, 2.., K} outcome-based matrix
2. For all player i {1,2,..K} do
3. break the sequential games of all player into subgames
4. SG_{ij} $i \rightarrow 1,2,...K$ & $j \rightarrow 1,2,...K$
5. If i = 2, then player's subgame isolated payoff vectors (SGIPV) for all are calculated
6. { for all $\{i \rightarrow 1,2,...K$ & $j \rightarrow 1,2,...K$ {
7. Calculate player 1 (CR node's) fitness using (4.24)
8. Calculate player 2 (Jammer's) fitness using (4.25)}
9. else
10. end for
11. Each player's best action must now be determined, given player 1 and 2's choice of initial actions for all $i \rightarrow 1,2,...K$ & $j \rightarrow 1,2,...K$
12. Player two's best action given $p_i, p_j = \{i, j\}$, is computed as $\lfloor sgbr_{ij} \rfloor \leftarrow \max(SGIPV_{ij})$
13. end for
14. The outcomes for both players must be determined for all subgames $i \rightarrow 1,2,...K$ & $j \rightarrow 1,2,...K$
15. Outcome vector $O_{ij} \leftarrow [sgbr_{ij}, p_i(j, sgbri_{ij})]$
16. Outcome matrix is created $OM_{ij} \leftarrow [O_{ij}]$
17. end for
18. The Subgame Perfect Nash Equilibrium (SPNE) is determined for all $i \rightarrow 1,2,..K$ & $j \rightarrow 1,2,..K$
19. player's best initial action is determined by finding the maximum values in the first row of the outcome matrix $[bri_{ij}] \leftarrow \max(OM_{ij})$
20. end for
21. The matrix of Subgame Perfect Nash Equilibrium $SPNE \leftarrow [bri_i, sgbri_{ij}, sgbri_i]$
22. The final equilibrium strategy vector is calculated $ES \leftarrow [bri_i, bri_{ij}, bri_j]$, where bri_i is the initial best response of player 1 (CR node), bri_{ij} is the best response of player 2 (Jammer) and is the final best response player 1 (CR node)

Fig. 3 *Anti-Jamming EGT algorithm*

algorithm for modelling CR user and reactive jammer interaction is given in Fig. 3.

4 Results and discussion

The results of the proposed anti-jamming system are analysed using the MATLAB simulation. The inferences from graphs are discussed for different conditions. The signal level analysis of jamming scenario with initial distraction transmission with payload having hopping sequence is shown on top in Fig. 4. In the bottom, frequency hopping sequence and original data transmission is shown. Here, the neat periodic signal at background is original BPSK modulated signal at transmitter and distorted signal is the transmitted signal with channel and jammer noise. Fig. 5 presents the demodulated signal at receiver.

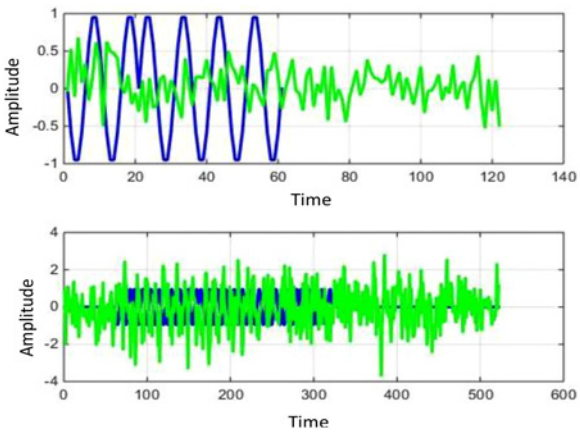

Fig. 4 *Distraction signal and data signal, both with jammer interference*

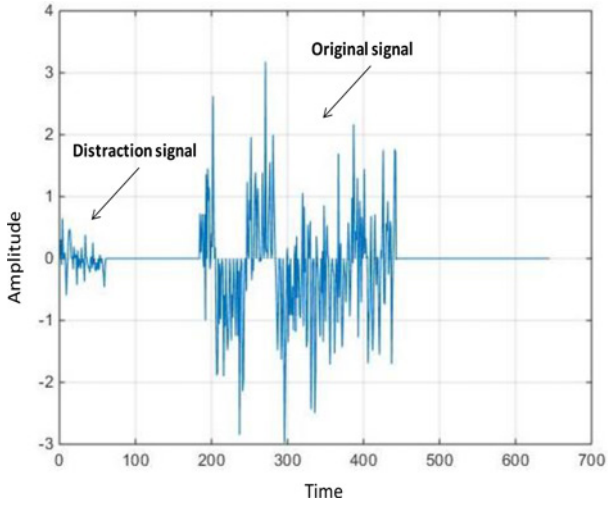

Fig. 5 *Demodulated signal at receiver*

doi: 10.1049/joe.2017.0285

Table 4 Simulation parameters and results

Parameters	When (CA > 75%) value	When (CA ≤ 75%) value
number of channels in RF environment	8	8
number of bits in data	1000	1000
available frequency bands	10, 20, 30, 40, 50, 60, 70, 80 kHz	10, 20, 30, 40, 50, 60, 70, 80 kHz
wireless channel	Rayleigh fading channel	Rayleigh fading channel
max percentage of PU occupancy	52% (total channels used by PU 4)	77% (total channels used by PU 6)
channels BW used by PU – random, kHz	40, 20, 80, 10 kHz	50, 70, 20, 80, 30, 10 kHz
idle channel BW, kHz	30, 50, 60, 70 kHz	10, 40 kHz
channel availability in percentage for SU	50%	23%
anti-jamming module status	active – HMM Viterbi Activated	system condition critical-EGT activated
HMM deduced current channel state	30 kHz – not_favourable 50 kHz – channel_busy 60 kHz – channel_idle 70 kHz – channel_busy	—
channel BW used by SU, kHz	60 kHz	40, 10 kHz

Table 5 Payoff matrix of player 1 (CR) for strategies S1, S2, and S3

0	1
1	0
0	1
1	0

Table 6 Payoff matrix of player 2 (jammer) for strategies S1, S2, and S3

1	0
0	1
1	0
0	1

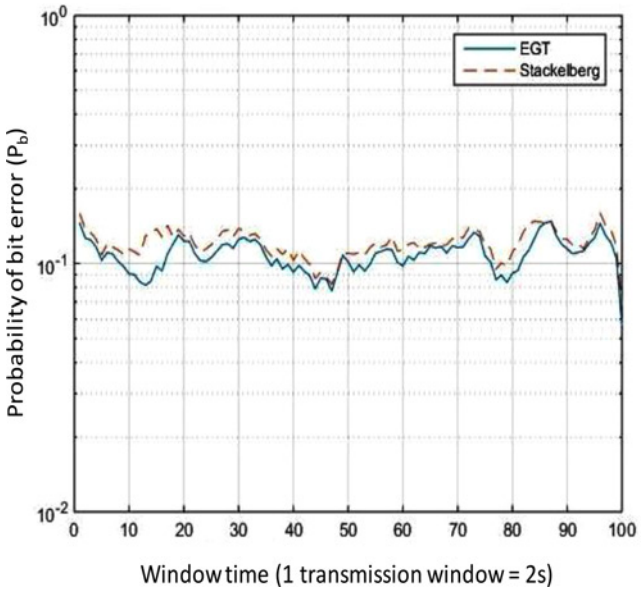

Fig. 6 *Probability of bit error (P_b)*

Table 4 presents the instantaneous parameters and results of simulation of the CRN with the anti-jamming system having channel availability of upper threshold (Ut) <75% with jammer.

Table 5 presents the instantaneous parameters and results of simulation of the CRN with the anti-jamming system having channel availability as (CA ≤ Lt) with reactive jammer, where Lt = 25%.

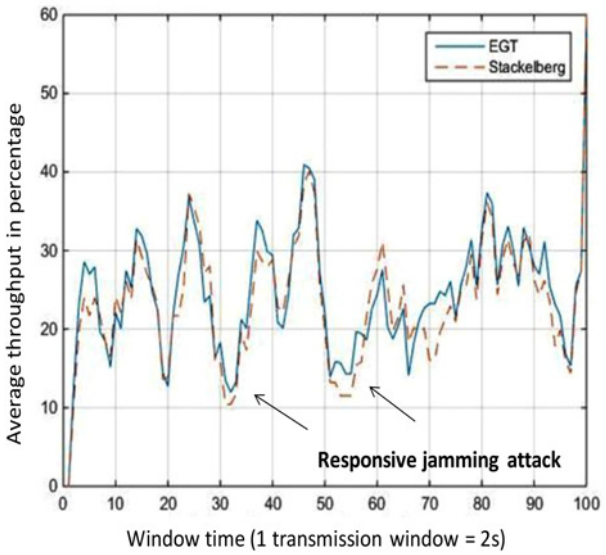

Fig. 7 *Throughput (EGT and Stackelberg game)*

The parameters listed in Table 4 are obtained with for channel availability <75 and 25% and channel availability is <25% with jammer. Tables 5 and 6 infer the strategies obtained during channel availability is <25%. When the channel availability is >75%, the FHSS technique is used with pseudo-random sequence for channel selection, dwell time: 10 ms and channel spacing: 10 kHz. The graph comparing the system performance of EGT and Stackelberg game theoretical modelling of interaction between the CR node and jammer in terms of probability of bit error is shown in Fig. 6.

The average probability of bit error P_b for EGT modelling with jammer was around 0.12 and the average probability of bit error P_b for Stackelberg game with jammer was around 0.14. This shows that on an average, there is 2% reduction in probability of bit error for EGT-based model when compared with Stackelberg game theory model under similar conditions. The simulation graph comparing the system performance of EGT and Stackelberg game theoretical modelling of interaction between the CR node and jammer in terms of throughput is shown in Fig. 7.

The throughput of the system in terms of average percentage of successful bit transfer per unit time was observed in the range of 30% for EGT modelling with jammer, and the average percentage of successful bit transfer per unit time for Stackelberg game with jammer was around 27%. This shows that on an average, there is

doi: 10.1049/joe.2017.0285

a 3% improvement in throughput for EGT-based model when compared with the Stackelberg game theoretical model under similar conditions. In both the cases, one unit time is the window of transmission and is equal to 2 s.

5 Conclusion

An anti-jamming system with adaptive channel frequency hopping was proposed using HMM and EGT to counteract jamming attack. Based on channel availability, the adaptive frequency hopping were implemented using inputs from HMM-based channel state selection and final strategy results of the EGT to evade jammer. The simulation results show that the proposed EGT-based anti-jamming system increases the throughput of system significantly by decreasing the probability of bit error at least by 2%, when compared with an anti-jamming system which uses Stackelberg game theory to model the interaction between cognitive radio node and jammer. The anti-jamming system performance can be further analysed in terms of power conservation at CR nodes in detail. Also, the performance and efficiency of the anti-jamming system for CRN can be investigated under multiple jammer scenarios.

6 References

[1] Pelechrinis K., Iliofotou M., Krishnamurthy S.V.: 'Denial of service attacks in wireless networks: the case of jammers', *IEEE Commun. Surv. Tuts.*, 2011, **13**, (2), pp. 245–257

[2] Slimeni F., Scheers B., Chtourou Z., *ET AL.*: 'Cognitive radio jamming mitigation using Markov decision process and reinforcement learning', *Procedia Comput. Sci.*, 2015, **73**, pp. 199–208

[3] Xiao L.: 'Anti-jamming transmissions in cognitive radio networks' (Springer, NY, USA, 2015)

[4] Sen C.: 'Digital communications jamming' (Storming Media, Middlesex, UK, 2000)

[5] Chen C., Song M., Xin C., *ET AL.*: 'A game-theoretical anti-jamming scheme for cognitive radio networks', *IEEE Netw.*, 2013, **27**, (3), pp. 22–27

[6] Marinho J., Granjal J., Monteiro E.: 'A survey on security attacks and countermeasures with primary user detection in cognitive radio networks', *EURASIP J. Inf. Secur.*, 2015, **2015**, (1), p. 4

[7] Grover K., Lim A., Yang Q.: 'Jamming and anti-jamming techniques in wireless networks: a survey', *Int. J. Ad Hoc Ubiquit. Comput.*, 2014, **17**, (4), pp. 197–215

[8] Min A.W., Zhang X., Shin K.G.: 'Detection of small-scale primary users in cognitive radio networks', *IEEE J. Sel. Areas Commun.*, 2011, **29**, (2), pp. 349–361

[9] Popper C., Strasser M., Capkun S.: 'Anti-jamming broadcast communication using uncoordinated spread spectrum techniques', *IEEE J. Sel. Areas Commun.*, 2010, **28**, (5), pp. 703–715

[10] Hanawal M.K., Abdel-Rahman M.J., Krunz M.: 'Joint adaptation of frequency hopping and transmission rate for anti-jamming wireless systems', *IEEE Trans. Mob. Comput.*, 2016, **15**, (9), pp. 2247–2259

[11] Dabcevic K., Betancourt A., Marcenaro L., *ET AL.*: 'Intelligent cognitive radio jamming-a game-theoretical approach', *EURASIP J. Adv. Signal Process.*, 2014, **2014**, (1), p. 171

[12] Arunkumar B.R., Raghu M.S.: 'Simulation study of Markov chain models with an application in cognitive radio networks', *Simulation*, 2015, **5**, (07), pp. 53–68

[13] Hossain E., Niyato D., Han Z.: 'Dynamic spectrum access and management in cognitive radio networks' (Cambridge University Press, Cambridge, UK, 2009)

[14] D'Oro S., Galluccio L., Morabito G., *ET AL.*: 'Defeating jamming with the power of silence: a game-theoretic analysis', *IEEE Trans. Wirel. Commun.*, 2015, **14**, (5), pp. 2337–2352

[15] Xiao L., Chen T., Liu J., *ET AL.*: 'Anti-jamming transmission Stackelberg game with observation errors', *IEEE Commun. Lett.*, 2015, **19**, (6), pp. 949–952

[16] Jiang C., Chen Y., Gao Y., *ET AL.*: 'Joint spectrum sensing and access evolutionary game in cognitive radio networks', *IEEE Trans. Wirel. Commun.*, 2013, **12**, (5), pp. 2470–2483

[17] Smith J.M.: 'Evolution and the theory of games' (Cambridge University Press, Cambridge, UK, 1982)

[18] Bednarczyk W., Gajewski P.: 'Hidden Markov models based channel status prediction for cognitive radio networks'. Session 4P6 RF and Wireless Communication, 2015, p. 2088

[19] Namvar N., Saad W., Bahadori N., *ET AL.*: 'Jamming in the internet of things: a game-theoretic perspective'. 2016 IEEE Global Communications Conf. (GLOBECOM), 4 December 2016, pp. 1–6