International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Revue d'Intelligence Artificielle
Vol. 36, No. 4, August, 2022, pp. 615-620
Journal homepage: http://iieta.org/journals/ria

Jamming Attack Mitigation in CR-IoT Using Game Theory

Nallarasan Venkatachalam*, Kottilingam Kottursamy

School of Computing, SRM Institute of Science and Technology, Kattankulathur, Chengalpattu 603203, Tamil Nadu, India

Corresponding Author Email: nallarav@srmist.edu.in

https://doi.org/10.18280/ria.360414

Received: 20 June 2022
Accepted: 18 August 2022

Keywords:
cognitive radio internet of things, game theory, cognitive radio network, jammer received signal strength, internet of things

ABSTRACT

Jamming attack is Cognitive radio Internet of thing network disables the spectrum sharing and reduces the spectrum utilization .detection and mitigation of such attacks is the main component in realizing cognitive radio-based spectrum sharing in cognitive radio-based internet of thing network this work proposes a game theory-based jamming attack mitigation strategy. The problem of jamming attack mitigation is modeled as a zero-sum game and solved by finding Nash equilibrium. The cognitive node which tries to share the spectrum pays the zero-sum game with the jamming attacker and selects the best strategy of selecting the best frequency without getting into the jamming attack. The result of the proposed mechanism proves that the gaming mechanism can tackle the jamming attack.

1. INTRODUCTION

The article examines the defense system, which is associated with game theory. While the jammers lower the signal's quality of appropriate users, and the intruder focuses on reducing the privacy rates, especially in virtual wireless networks where Mobile Virtual Network Operator (MVNO) users' goal is to boost their Signal to Interference plus Noise Ratio (SINR). Where the jammers aim to indiscriminately advance their Jammer Received Signal Strength (JRSS), and the intruder's target is to decrease the overall privacy rate. In comparison to old strategies, a numerical number of outputs have verified and proven that the implemented game strategies are successful against the attackers with reference to data rate, secrecy rate and latency [1-3].

Defensive Path Selection (DPS) is implemented in this framework on the basis of inter-institutional reinforcement learning in order to choose a flawless choice against the smart invader and also to increase the performance of SSE's transmission. The aptitude of DPS is evaluated and the efficiency of the implemented method is proved theoretically [4].

In the study of Signori et al. [5], we consider an environment where jamming attacks, lowering the quality of communication of battery-powered submerged nodes, are performed by a harmful node. To increase the probabilities of correct delivery of the packet, packet-level coding is used in the legitimate transmitter. The jammer has a dual objective due to the node's energy restriction. The objectives are interrupting the communication and making the target to send more no. of redundancy in order to reduce its lifespan. They derived the best tactics from their model, where the jammer and the transmitter are players in a multi-stage game. The evaluation of the performance is done in both model-based environments by using the actual experimental data and in order to evaluate the strategy's performance, a sensitivity analysis is performed to ensure if, by chance, the actual channel model differs from the one they use [6, 7].

In the study of Thien et al. [8], in Cognitive Radio Network (CRN) they aim to increase the safety of multi-channel communication. In the meantime, several jammers try to access the important channels to avoid the Secondary Users (SUs) from using them. In order to overcome that, they have implemented a game–based schemes by using the concepts of game theory and defining the position, actions, and players' rewards. Which seems to be the supreme channel for the SUs so that they could evade the jammer's attacks in their communication channels. Respectively the difficulty is to find the best channel to increase the long-term reward of the SU. Since the Primary Users (PUs) don't use the communication channels, so jammer attacker doesn't target them. A Transfer Game-Actor-Critic (TGACT) scheme is implemented by recommending applied transfer learning. For quickening the learning progress and to deliver improved performance, TGACT utilizes the transmitted information in a double-game period in channel selection. In the end, with a different configuration, the implemented scheme's performance is imitated. The imitated outputs prove that the implemented scheme is resistant to the jammer attack, and improved performance is achieved while comparing to other schemes for channel selection.

In the study of Taggu et al. [9], in order to diminish or to reduce the jamming attack, a metamorphic game-theory approach is used. The Secondary Users (SUs) can get fair usability of the channels by the implementation of the metamorphic game, even though the malicious SU is present in the channel. The implemented algorithm works well, as shown by the obtained results of this study.

In Cognitive Radio Network (CRN), in order to prevent the Radio Frequency (RF) jamming attack, an anti-jamming system was implemented with an adaptive frequency jumping method [10]. In considering a reactive jammer presence, two methods are implemented to accomplish adaptive frequency jumping. Those two methods are: An algorithm is used on the basis of the Hidden Markov Model (HMM) if the channel availability is lower than 75% and the communication between the Cognitive radio node and the jammer is exhibited using the Evolutionary Game Theory (EGT) if the system reaches the critical state (where the channel availability is lower than 25%). From these two models, the results are obtained and developed more in order to discover a capable channel. It was found that this anti-jamming system reduced the probability of bit error by 48% even in the presence of reactive jammer and verified through a VR demonstration

The theme of this paper is to examine and give a dependable and adaptive CR safeguarding method against jamming attacks [11]. Thereby advancing the bandwidth, increasing the wireless network of IoT technology's performance and cracking the problem of vestry of the frequency bands. The above aims are achieved through an anti-jamming game, which was designed with the help of game theory and also achieved by the adaptation of the Multi-Arm Bandit (MAB) strategy. Few MAB strategies are adapted to overcome the problem of the vestry in cognitive radio's frequency band spectrum like Upper Confidence Bound (UCB), Thompson Sampling and Kullback-Leibler Upper Confidence Bound (KL-UCB). There are some increments and advancements in solving the problem of the vestry in frequency band spectrum is verified by the obtained outputs. It concludes that Thompson Sampling MAB policy with lower regrets and highest rewards is best to solve these issues in adaptation while comparing with other MAB policies.

In the study of Wang et al. [12], reducing the damage effect issue on the frequency jump spread spectrum satellite is solved by the usage of a game framework called two-player asymmetric zero-sum. The reward is designed as the channel capacity of a guardian under a white additive Gaussian noise. The capacity to spreading their signals all over a pre-determined frequency band are possessed by both invader and guardian. They consider two environments are: (i) both of their strategies are known to both the invader and the guardian and (ii) the invader's strategies are known to the guardian but not the other way round. They also examined that the players whether they have the knowledge about the scenarios of these environments or not. If so not they have provided some guidelines for the players to logically define the best strategies in each of these environments and it is verified by a simulation

In the study of Kakalou and Psannis [13], in order to study the Primary User Emulation Attack (PUEA) on cognitive radio nodes, a game theory-based framework is implemented as a game of incomplete information between the SUs. The game information is not shared by the Secondary User (SU) against the opponents, who are causing the PUEA and with the minimum requirement of computation, the SU can define the best strategies. After successfully challenging the PU emulator by the SU, the information is updated in a cloud database so that the remaining network can identify the identities of PUE. In the meantime, the game evolves, a splendid alliance of secondary users is made to group together as one and they don't work against the live PU emulator a victory strategy. The performance of the alliance approach for PUEA detection is equal to the performance of the game's best strategy.

Li and Wang [14], Vijayakumar and Malarvihi [15], Nallarasan and Kottursamy [16] contemplate the misbehavior user into two types, namely MMU and SMU. First, the SUs non-supportive behavior is examined, which increases their own advantage and thereby, we can get an exclusive strategy called individual Nash equilibrium joining strategy. Then according to the social organizer, they implemented a strategy called socially optimal joining strategy. In order to remove the gap between these two strategies (individual equilibrium and socially optimal strategies), they implemented a fee is charged on the SUs. A sensitive analysis is carried out for joining the strategies of SUs and social prosperity with respective to few important system parameters. Remarkably the increment of individual equilibrium and socially optimal joining chances alongside with social welfare is observed when the system is attacked by MMUs.

The security tactic is on the basis of playing Nash Equilibrium (NE) to prevent worst-case network utility [17]. There are three different steps in this tactic those are: (i) a separate control set is established, where the space of security tactics increases with respect to the network size. In order to yield a security strategy, a measurable degradable approach is utilized whose performance is almost equivalent to the non-degradable game, (ii) to allocate the power levels, a marginal tactic is proposed in order to satisfy reported restrains so that combinatory complication with enormous no. of pure actions could be dogged, (iii) in considering the both player's constant action space marginal-based strategy is simplified. The availability of an exclusive NE is proven for this setting. The effect of this security approach against several attacks is shown by the obtained results and a demonstration is done in the real-life scenario wireless network deployed in a three-story building

Laszka et al. [18] is to give a theoretical fundamental for safeguarding transportation networks from attacks. So a model is introduced on the basis of game theory for launching, detecting, and mitigating these attacks, which interferes with traffic-signal plans. It was found out that defining the best tactics or strategies is a challenging one and they implemented an experimental algorithm in order to find close optimal tactics. An abnormality detector is proposed on the basis of the Gaussian process to warn the operators about the current attack. Through the numerical number of experiments, the evaluations of the experimental algorithm and the implemented detector are done on the basis of the SUMO traffic simulator.

A Stackelberg game is designed. Where the commanders are jammers and the followers are dispatchers [19-21]. In order to achieve the splendid defense level, an enhanced encryption scheme is implemented to prevent the intruder situation, where the primary spectrum is accessed by the intruder. By the implementation of this technique, the privacy rate is maximized and it also reduces the power consumption. Aside from the power scheme, the most important apprehension is the intruder, where the transmission products create an optimal scheme in CRN. This optimization is spot lighted with a fuzzy-based mathematical method. In order to eliminate the intruder presence in CRN with an optimal solution Markov Decision Process Outcome Prediction (MDPOP) a Q learning algorithm is utilized.

2. PROPOSED METHOD

The system model for the jamming attack mitigation is given in Figure 1. The system model consists of n primary user and one CRIoT node, and one jamming node. The CRIoT node is applying an auto encoder for the detection of the jamming attack. This detection result is used on the gaming model for the mitigation of the jamming attack.

Figure 2 shows the flow diagram of the process which is happening at the CRIoT node. The CRIoT node receiver element receives the signal which is processed by the autoencoder for detection of the jamming attack. The characteristics of jammer are: 1) The jammer will randomly introduce an attack signal into the primary user frequency; 2) The intention of jammer attacks is to mimic of the primary user and make illustration that the frequency of primary user in use. It will deny the use of free frequency of the primary user to be used by CR user; 3) The attacker will randomly inject a high amplitude jam signal at the frequency of the primary user.

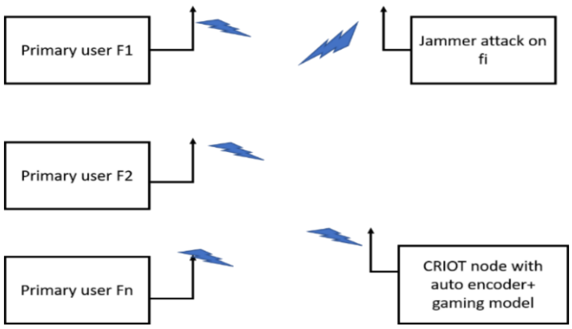
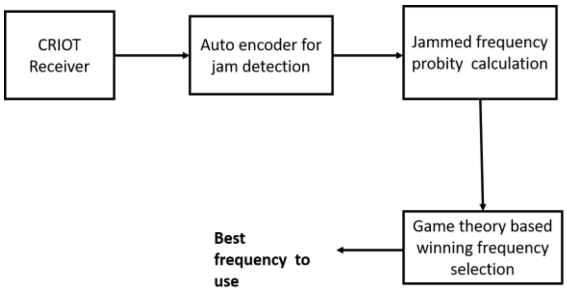


Figure 1. Jamming attack mitigation



CRIOT Receiver
Auto encoder for jam detection
Jammed frequency probity calculation
Game theory based winning frequency selection
Best frequency to use

Figure 2. Flow diagram of the process

From the outcome of the detected jamming attack at a particular frequency fi the probability of being to be attacked is calculated. This probability information is fed to the gaming model, where the zero-sum game is formulated between the CRIoT node and the jammer node.

Generally, the mathematical representation of the zero-sum gaming model is:

$$\text{zero} - \text{sum game} = \sum_{i=1}^{n} p(Ucr) = 0 \qquad (1)$$

where, the utility matrix of the CRIoT node of this zero-sum game is:

$$U_{cr} = \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix} \qquad (2)$$

Row player is considered as cognitive radio, and the Colum player is the jammer Similarly, the Utility matrix of jammer of this zero-sum game is:

$$U_{jam} = \begin{bmatrix} -1 & 1 \\ 1 & -1 \end{bmatrix} \qquad (3)$$

So, a probability model is used to decide which strategy to select and play at the given time.

The game is played between the jammer and CRIoT node for finding Nash equilibrium conditions. Once the Nash equilibrium has been solved, the game is reached. The strategy under the Nash equilibrium is taken as the solution. Here, the strategy of the CRIoT node is to select a free frequency that is not attacked by the jammer. Jammer also keeps on changing his strategy of attacking the frequency randomly such that the CRIoT node will not use the free frequency of the primary user.

Once the Nash equilibrium of the game is reached, the best frequency to be used by the CRIoT node is obtained. In Nash equilibrium, both the competitive players will not deviate from their strategy because, in that equilibrium, both players will have a benefit. If they deviate, all the players will be punished or their award will be reduced.

In the state of the system in a Nash equilibrium, none of the players will change their strategy. They will stick to the same strategy in which the nash equilibrium is achieved. Under our system CR will not change the frequency of selected to transmission and jammer also not change the jamming frequency.

This game is played multiple times at a specific period of T such that at any time over the period of T, the CRIoT node will get the free frequency to use without jamming attack. Since the game is played over period T. The spectral efficiency of the CRIoT is limited by this interval which is given by:

$$S_{EFF} = \frac{T-T_{att}}{T} log_2(1+SNR) \qquad (4)$$

where, T_{att} is the period with which the frequency used by the CRIoT node is being attacked by the jammer.

During jamming with jamming over a period, T_{att} the spectral efficiency is given below:

$$S_{effjam} = log_2(1+\frac{P_{cr}}{P_n+P_{jam}}) \qquad (5)$$

where, P_{cr} is the transmit power of the CRIoT node; P_{jam} is the transmit power of the jammer; P_n is the channel noise power.

When the CRIoT node use the M number of different frequency, the spectral efficiency is given as:

$$S_{effjam} = \sum_{f=1}^{M} log_2(1+\frac{P_{crf}}{P_{nf}+P_{fjam}}) \qquad (6)$$

where, P_{crf} is the transmit power of the CRIoT node at frequency f; P_{fjam} is the transmit power of the jammer at frequency f; P_{nf} is the channel noise power at frequency f.

When the CRIoT node uses the strategy of using the frequency among M frequency with a probability of α_T then the spectral efficiency will be:

$$S_{effjam} = \sum_{\substack{f=1, \\ \alpha_{f\in\{\rho1,\rho2,\rho3..\rho l\}}}}^{M} \alpha_f log_2(1+\frac{P_{crf}}{P_{nf}+P_{fjam}}) \qquad (7)$$

By making the parallel play of the game by using multicore or distributive processors, we can fully utilize the free spectrum with a nominal frequency switching time Ts.

3. RESULTS AND DISCUSSION

The two-player game is simulated, and the Nash equilibrium is achieved. The anti jamming is modeled as a zero-sum game where the CRIoT node and the jammer are considered players. Here the cognitive user tries to occupy a free frequency without jamming and the jammer attempts to jam the frequency used by the cognitive radio. A different set of frequency ranges is used in the game theory mechanism, from the range of 50MHz to 3GHz. The played frequency ranges are, 500MHz, 700MHz, 800MHz, 900 MHz ,1.25GHz, 2.5GHz and 3.5GHz respectively.

Cognitive radio will be the winner if it can use the free frequency without jamming. The jammer will be the winner if he jams the frequency used by the cognitive radio.

In Eq. (2) and Eq. (3) are used in proposed method, under the jamming attack detection, the utility matrix is calculated from the utility function. The utility function consists of the effect of jamming and the performance of both the cognitive user and the primary user. The spectrum efficiency is used as utility function which is given in Eq. (7).

Table 1 shows the various game played and their corresponding performance measure. The first game deals with only one frequency used by the CRIoT node, which will be attacked by the jammer. Game two deals with the usage of two different frequencies where the CRIoT node tries to use the frequency which is not being attacked by the jammer while the jammer is trying to attack the frequency being used by the CRIoT node. Game three deals with the usage of 3 different frequencies of F1, F2 and F3, in which the CRIoT node is applying a strategy of selecting the frequency which is not being jammed by the jammer at the given time. Game four deals with the usage of four different frequencies by the CRIoT node. Game five deals with the usage of 5 different six different frequencies being used cognitive radio. In all games, the CRIoT node follows a strategy that will use any frequency not being jammed by the jammer from the available set frequency. The core strategy is that it has to randomly select one of the frequencies and compute the utility value. The frequency for which the utility values are highest is selected for the transmission.

Table 1. Various cases of the game and their performance

Game	Strategy	Peak performance at 25 dB SNR	Nash equilibrium
Zero-sum game 1	Only one frequency F1, which is used by CR and attacked by Jammer	1.2 bits/sec/Hz	Usage F1 with 50% ideal
Zero-sum game 2	2 frequencies F1, F2 used by CR and attacked by Jammer	6.67bits/sec/Hz	Using F1 and F2 with a probability of 0.5
Zero-sum game 3	3 frequencies F1, F2, F3 used by CR and attacked by Jammer	11 bits/sec/Hz	Using F1, F2 and F3 with probability of 1/3
Zero-sum game 4	4 frequencies F1, F2, F3, F4 used by CR and attacked by Jammer	14 bits/sec/Hz	Using F1, F2, F3 and F4 with probability of 1/4
Zero-sum game 5	6 frequencies F1, F2, F3 used by CR and attacked by Jammer	21.8bits/sec/Hz	Using F1, F2, F3, F4, F5 and F6 with probability of 1/6

Figure 3 shows the utility value of the CRIoT node while taking different strategies when jammer also taking different strategies. From the Figure 3, that represents the utility value of the jammer and CR radio. For jam is jammer and the 1-jammer are CR radio. The x-axis value represents the probability of the frequency being occupied by the jammer. The Y-axis value represents the utility value of both the jammer and the CR.

(*Uc*, *σc*T)1 is represent utility of jammer. (*Uc*, *σc*T)2 utility of CR. When the probability of occupying the frequency for jammers is zero, then the utility of the CR radio value is 1. When the probability of occupying the frequency for jammers is 1, then the utility of the CR radio value is -1.

The utility values are discrete one, because the entire utility function is discrete, and the jamming attack occurs at random in the discreate interval.

Here, the utility values are taken between -1 to +1. From the figure, it is evident that when the CR radio occupying one frequency and if the jammer is not occupying the same frequency, then the utility value is “1”. suppose the jammer also inhabiting the same frequency. The utility value becomes “-1”. Similarly, the utility value of the jammer also followed. That utility is plotted by assuming a zero-sum game between the CRIoT node and the jammer.

Figure 4 shows the utility value of the CRIoT node, which is measured in the form of spectral efficiency. From Figure 4, we can see that utility value is nothing but spectral efficiency for every game. The utility values in Table 1 are given in the table itself under peak performance at 25db SNR.The spectral efficiency is measured and plotted without jamming, which achieves a maximum of 4.8 bits per second for SNR of 25 dB and achieves a minimum of 2.7 bits per second when 5 dB SNR. When the jammer is introduced with jamming of 90% of cognitive radio transmit power, the spectral efficiency is measured and plotted. At Jammin, spectral efficiency measurement shows that a maximum of 1. 2 bits per second can be achievable at 5 dB SNR and a minimum of 1.1 bits per second at 25 dB SNR. The game is played such that randomly the jammer will occupy any one of the frequencies with equal probability. An attempt to measure the spectral efficiency value is also made and plotted in the graph. From the graph, we can observe that when such random jamming is introduced, the spectral efficiency gets reduced to the jamming level. Once the jammer leaves the frequency or the cognitive radio selects the frequency not occupied by the jammer, the spectral efficiency value reaches the maximum. This behavior is floated as a green color graph in Figure 4.

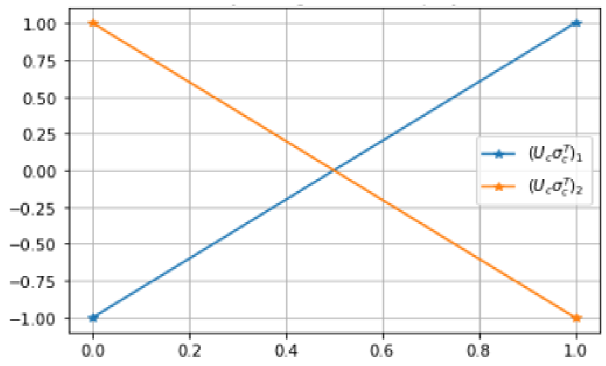


Figure 3. Utility value of CRIoT node with a different strategy

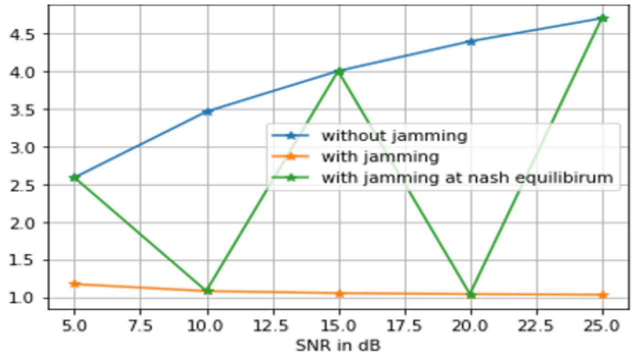


Figure 4. Utility (Spectral efficiency) of CRIoT node fro various SNR

The jammer occupies the frequency randomly at a random time. To analyze the jamming effect, the system model has taken the 6 different frequencies used by the CRIoT node. The game is formulated such that the CRIoT node will make a strategy of occupying the frequency which is not jammed by the jammer from the six frequencies. Similarly, the jammer will create a strategy of occupying the frequency which is being used by the CRIoT node. Under this game, the CRIoT node tries to maximize the achievable rate by selecting unoccupied frequency by the jammer, whereas the jammer playing the game to minimizes CRIoT node spectral efficiency by occupying the same frequency, which is being used by the CRIoT node. By keeping the SNR value as constant and the transmitted power of the CRIoT node and jammer power also as a constant, the game is played between the jammer and CRIoT node and the performance measurements are obtained for different frequencies. The performance is plotted between the spectral efficiency of the CRIoT node and the different probability of being occupied by the same frequency by the jammer. The Figure 5 shows the performance measure measurement of such game when CRIoT node uses two different frequencies, three different frequencies, four different frequencies and six different frequencies. From the plot, it is evident that if the number of frequency used by the CRIoT node is more, then the probability of getting higher spectral efficiency is higher. This is happening because if the number of frequencies is more, then the CRIoT node has more choice of selecting the frequency that is not being jammed by the jammer with the highest probability. On the other hand, the jammer has the lowest priority to select the occupied frequency of the CRIoT node when the number of frequencies used by the cognitive radios is more. From the Figure 5, we can observe that we can achieve a maximum of 20bits/sec/Hz spectral efficiency when the CRIoT node is using six different frequencies at the probability of an attack of the jammer is 0.2. It can be observed that the achievable spectral efficiency decreases with respect to the possibility of occupancy of the jammer at the same frequency. For example, the capacity reduces from 20bits/sec/Hz to 10bits/sec/Hz when the probability of jamming increases from 0.2 to 0.9. The lowest performance is observed when the CRIoT node uses only two different frequencies with 6.9 bits/sec/Hz when the probability of an attack is 0.2, which is getting reduced by 0.19 bits/sec/Hz when the probability of an attack is 0.9. Other levels of moderate performance can be observed when the frequency by CRIoT node is 3 and 4. We can also observe from the Figure 5 that whenever the number of frequencies used by the CRIoT node increases, the spectral efficiency is growing by the factor of 2.5 bits/sec/Hz approximately for every single frequency usage increment. When the number of frequencies is higher, then there is a greater probability of available free spectrum to use, so most of the time the cognitive radio will have the choice to use free spectrum. Since the probability of using the free spectrum is higher, which results in higher spectral efficiency.

The disadvantage of this higher number of frequencies to be used in the CR is that it must search many frequencies and decision making is complex.

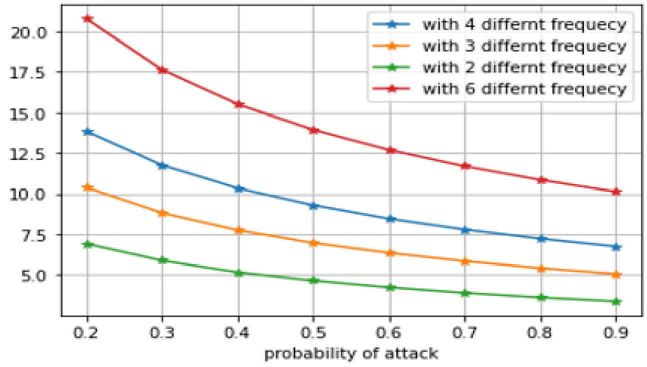


Figure 5. Utility (Spectral efficiency) of CRIoT node for the various probability of attack

4. CONCLUSIONS

An anti-jamming attack mitigation mechanism is developed using game theory for cognitive Internet of Things applications. The detection of jamming attack is performed using an autoencoder and those results are used to compute the probability of occupancy of the jammer at a particular frequency. A zero-sum game is formulated between the attacker and CRIoT node and jammer; then, the anti-jamming solution is formulated through Nash equilibrium. The results of the simulation show that the proposed zero-sum game model of anti-jamming mechanism is able to mitigate the jamming effect by means of selecting different frequency which is not being jammed. The future direction of the work will be implementing the proposed mechanism on a practical hardware platform and analyzing its performance.

ACKNOWLEDGMENT

The authors with a deep sense of gratitude would thank the supervisor for his guidance and constant support rendered during this research.

REFERENCES

[1] Alsulami, B.S., Bajracharya, C., Rawat, D.B. (2021). Game theory-based attack and defense analysis in virtual wireless networks with jammers and eavesdroppers. Digital Communications and Networks, 7(3): 327-334. https://doi.org/10.1016/j.dcan.2021.04.002

[2] Nallarasan, V., Kottursamy, K. (2021). Cognitive radio jamming attack detection using an autoencoder for CRIoT network. Wireless Personal Communications, 1-17. https://doi.org/10.1007/s11277-021-08786-5

[3] Nallarasan, V., Kottilingam, K. (2021). Spectrum

management analysis for cognitive radio IoT. In 2021 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, pp. 1-5. https://doi.org/10.1109/ICCCI50826.2021.9402690

[4] He, J., Chen, C., Zhu, S., Yang, B., Guan, X. (2018). Antijamming game framework for secure state estimation in power systems. IEEE Transactions on Industrial Informatics, 15(5): 2628-2637. https://doi.org/10.1109/TII.2018.2871933

[5] Signori, A., Chiariotti, F., Campagnaro, F., Zorzi, M. (2020). A game-theoretic and experimental analysis of energy-depleting underwater jamming attacks. IEEE Internet of Things Journal, 7(10): 9793-9804. https://doi.org/10.1109/JIOT.2020.2982613

[6] Arul, R., Raja, G., Kottursamy, K., Sathiyanarayanan, P., Venkatraman, S. (2017). User path prediction based key caching and authentication mechanism for broadband wireless networks. Wireless Personal Communications, 94(4): 2645-2664. https://doi.org/10.1007/s11277-016-3877-5

[7] Ponnusamy, V., Kottursamy, K., Karthick, T., Mukeshkrishnan, M.B., Malathi, D., Ahanger, T.A. (2020). Primary user emulation attack mitigation using neural network. Computers & Electrical Engineering, 88: 106849. https://doi.org/10.1016/j.compeleceng.2020.106849

[8] Thien, H.T., Vu, V.H., Koo, I. (2021). A transfer games actor–critic learning framework for anti-jamming in multi-channel cognitive radio networks. IEEE Access, 9: 47887-47900. https://doi.org/10.1109/ACCESS.2021.3068129

[9] Taggu, A., Nath, M., Banik, P., Marchang, N. (2017). A jammer-resilient cognitive radio network using evolutionary game theory. In 2017 20th International Symposium on Wireless Personal Multimedia Communications (WPMC), pp. 638-641. https://doi.org/10.1109/WPMC.2017.8301890

[10] Deepak, B.R., Bharathi, P.S., Kumar, D. (2017). Radio frequency anti-jamming capability improvement for cognitive radio networks: An evolutionary game theoretical approach. In 2017 Fourth International Conference on Signal Processing, Communication and Networking (ICSCN), pp. 1-6. https://doi.org/10.1109/ICSCN.2017.8085719

[11] Chaczko, Z., Slehar, S., Shnoudi, T. (2018). Game-theory based cognitive radio policies for jamming and anti-jamming in the IoT. In 2018 12th International Symposium on Medical Information and Communication Technology (ISMICT), pp. 1-6. https://doi.org/10.1109/ISMICT.2018.8573725

[12] Wang, Q., Nguyen, T., Pham, K., Kwon, H. (2018). Mitigating jamming attack: A game-theoretic perspective. IEEE Transactions on Vehicular Technology, 67(7): 6063-6074. https://doi.org/10.1109/TVT.2018.2810865

[13] Kakalou, I., Psannis, K.E. (2018). Coordination without collaboration in imperfect games: The primary user emulation attack example. IEEE Access, 6: 5402-5414. https://doi.org/10.1109/ACCESS.2018.2791519

[14] Li, K., Wang, J. (2019). Optimal joining strategies in cognitive radio networks under primary user emulation attacks. IEEE Access, 7: 183812-183822. https://doi.org/10.1109/ACCESS.2019.2957435

[15] Vijayakumar, P., Malarvihi, S. (2017). Green spectrum sharing: Genetic algorithm based SDR implementation. Wireless Personal Communications, 94(4): 2303-2324. https://doi.org/10.1007/s11277-016-3427-1

[16] Nallarasan, V., Kottursamy, K. (2021). Energy efficiency and throughput analysis of cognitive based internet of things. In 2021 Smart Technologies, Communication and Robotics (STCR), pp. 1-6. https://doi.org/10.1109/STCR51658.2021.9588958

[17] Anwar, A.H., Atia, G., Guirguis, M. (2018). Adaptive topologies against jamming attacks in wireless networks: A game-theoretic approach. Journal of Network and Computer Applications, 121: 44-58. https://doi.org/10.1016/j.jnca.2018.06.008

[18] Laszka, A., Abbas, W., Vorobeychik, Y., Koutsoukos, X. (2019). Detection and mitigation of attacks on transportation networks as a multi-stage security game. Computers & Security, 87: 101576. https://doi.org/10.1016/j.cose.2019.101576

[19] Subbulakshmi, P., Prakash, M. (2018). Mitigating eavesdropping by using fuzzy based MDPOP-Q learning approach and multilevel Stackelberg game theoretic approach in wireless CRN. Cognitive Systems Research, 52: 853-861. https://doi.org/10.1016/j.cogsys.2018.09.021

[20] Raja, G., Kottursamy, K., Chaudhary, S.H., Hassan, A., Alqarni, M. (2017). SDN assisted middlebox synchronization mechanism for next generation mobile data management system. In 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), pp. 1-7. https://doi.org/10.1109/UIC-ATC.2017.8397620

[21] Raja, G., Kottursamy, K., Theetharappan, A., Cengiz, K., Ganapathisubramaniyan, A., Kharel, R., Yu, K. (2020). Dynamic polygon generation for flexible pattern formation in large-scale UAV swarm networks. In 2020 IEEE Globecom Workshops (GC Wkshps), pp. 1-6. https://doi.org/10.1109/GCWkshps50303.2020.9367501