International Innovative Research Journal of Engineering and Technology
ISSN: 2456-1983 Vol: 6 Issue: 2 December 2020

An Energy-Efficient Jamming Attacks Detection based on Cognitive Radio Networks

Bob Subhan Riza
Universitas Potensi Utama
bob.potensi@gmail.com

Abstract: 5G wireless networks, primarily because of the device - to - device connections can enable huge networking. Dynamic bandwidth connectivity is a feature that enables device-to-device connections. Applications configured with cognitive radios must be authorized to reprocess the bandwidth consumed by cellular connections. The complex efficiency of the bandwidth allows cognitive consumers to switch between networks. In specific, switching contributes to energy efficiency, delay, and bandwidth connectivity. When the system is under the jamming attack, the computational cost much more. It is a major problem to fix jamming while ensuring an optimal level of operation. Thus, existing anti-jamming methods consider static users, this suggests preventive measures for wireless cognitive radio users in this paper and test them. The multivariate cumulative total was used in this study to classify suspicious activity like jamming attacks in Cognitive Radio Networks (CRN). Preventive-measures are being taken to resolve security risks to cognitive radio networks. The Intrusion Detection System (IDS) has been presented, including a way of preventing attacks on the cognitive radio network infrastructure.

Keywords: Cognitive Radio Networks; Energy_Efficiency; Jamming Attacks; Intrusion Detection System

I. INTRODUCTION

Shortly, 5G is predicted to replace prior iterations of wireless networks, offering faster bandwidth and reduced latency, allowing technologies including 'self-driving' vehicles, the Internet of Things, e-health systems, virtual reality, and intelligent cities [1]. 5G internet services will enable performance increases that are a thousand times greater. Interfaces with a maximum hundred billion users would also be enabled by 5G networks [2]. The implementation of networks with this kind of huge capability and availability raises several problems, the most important of which is the control of radio energy. When security risks are analyzed, the issue becomes even more significant. Thus, this turn increases the usage of bandwidth needed for high-density networks to be accomplished. Cognitive users should be self-managed, as they can perceive, understand, and respond to internal and external changes [3]. When it refers to implementing networks of huge numbers of computers, self-management is a calculated value. The difference of preference for the entry, nevertheless, sufficient standard among cognitive users more prone to security threats. It is difficult to build frameworks that interact with security risks and recognize the impact of resource uncertainty.

The author Mitola [4] initially described the term cognitive radio network (CRN) as cognitive radio networks. In 1999, the word cognitive radio [5] was first formally proposed by Mitola and Maguire. Cognitive radio (CR) is a device that could adjust its transmitting specifications based on contact with the operating environment, according to the Federal Communications Commission (FCC). There are two features of Cognitive broadcasting. Cognitive capacity does the same and improved reliability is something. Cognitive capacity makes it easier for the system to detect the world and select the best propagation range available. The method of spectrum control achieves this goal. By changing its metrics like frequency, modulation, etc., specification helps the system to conform to its condition. Cognitive radio has the flexibility to contribute and suggest improvements to the globe, as a result of its emotional intelligence for safe communication [6]. In the case of cellular networks, privacy is insecure and there is a risk of eavesdropping or jamming. CRNs are smart networks that require wireless devices to use radio applications to ensure most of the accessible/available frequency.

1.1. Cognitive Radio Networks (CRNs)

Cognitive radio is an adaptive wireless networking device that is cognizant of its external environment, as per

Simon Haykin's [7], which follows the technique of awareness to know about the environment and respond to its cognitive processes to statistical variations, considering two main goals. Spectrum sensing, spectrum exchange, spectrum control, and spectrum versatility are the features of cognitive broadcasting. Figure 1 illustrates the cognitive radio technology's key concepts. CR system helps users to decide which portion of the continuum is open. It also includes the participation of certified/approved users to be identified while a user works in a licensed spectrum. Spectrum sensing is considered this method. Spectrum control is nothing but a choice on the spectrum. The spectrum decision feature is to choose the best path provided. The synchronization of communication links between several service providers is known as spectrum access. Spectrum versatility, when a permitted person is detected, is to exit the network. Authorized and unlicensed users are classified as users and external on cognitive radio networks [6].

The radio connection functionality is expanded by cognitive radio networks to different network functionality and beyond. It determines the best spectrum configurations by studying the communication network and network evolution through cognitive radio interaction. Based on the sensing experimental verification by the CRN participants, each channel is chosen for CRN activity. This is categorized into two parts, either centralized or cooperative [8]. CRNs are structured as infrastructure-based systems in three main frameworks are architectures for networks, ad-hoc network frameworks, and configurations of mesh networks [6].

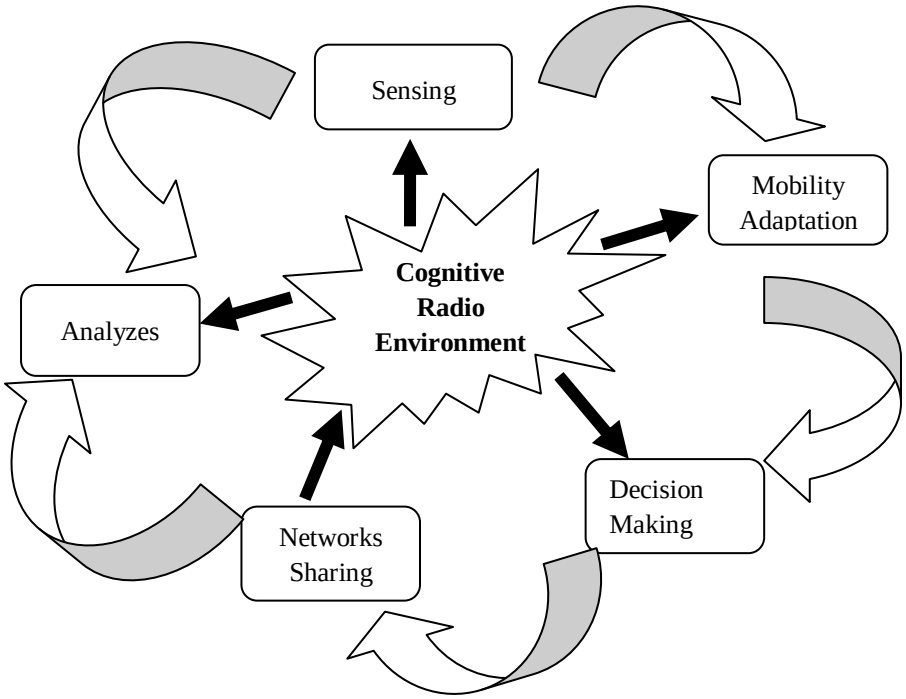

Figure 1. Cognitive Radio Networks

There are base stations or control points at an infrastructure CRN. A system with CR capability communicates between several devices via the base station themselves, within the scope of a single base station. The base stations path interactions between systems in separate cells. Modules that do not need base stations to build ad-hoc CRNs. With different security mechanisms, these systems set up connections towards each other. They might also use applications that are used, like licensed spectrum or ethernet. It is a hybrid of ad-hoc networks and infrastructure. Nodes are attached via neighboring nodes to the base stations, and the transmissions are processed and distributed via the access points.

II. RELATED WORKS

There are also several other recent articles focused on security risks in neural networks [9]. User interface optimization attacks are being thoroughly investigated; see similar research, for example [10, 11]. A lot of work was also applied to the protection of spectrum access;

consider prior studies [12] [13] & [14], for instance. Jamming attacks also had generated active interest and they're more disruptive and bandwidth efficiency is substantially degraded. Many modern jamming security measures presume that several channels are open and thus regard surfing between them as a means of withdrawing from jammers. The findings state in [15] that cognitive users hop between multiple channels and integrates the capacity to challenge against jammers spontaneously. As a prototype for Colonel Blotto, the design relationships between jammers and user equipment. Hopping structures were extracted based on the method of Markov's decisions or other effective teachings. Similarly, the authors in [16] suggested preventive measures based on frequency hopping and modeled the anti-jamming method as a simulation. In [16], hopping structures are generated, including [15], depending on the decision theory.

In the paper [17], the work is identical to [15]. Even so, though energy consumption is dynamically distributed in [15], the authors in [17] have implemented their suggested techniques to effectively distribute power. The test samples in [18] that jammers and legal consumers are competing concurrently. Using the Stackelberg method, they modeled their relationship as a simulation. Secondary consumers of their framework distribute power depending on expected jamming efficiency. As a moderately experienced Markov mechanism, Su et al.[19] modeled spectrum coverage and accessibility. The authors in [19] thought that, according to other articles, users learn to disappear from jammers by contextual networking. Depending on the multiple-armed hacker issue, they extracted their retreat technique on the framework in which multiple users have the same intelligence of spectral efficiency and jammers. The developers have treated spectral networking in [20] as a jamming preventive measure on the premise that secondary consumers use the key - based hidden keys to choose channels.

Mistra et al. [21] propose a centralized solution, a fuzzy inference-based method, that uses three parameters obtained from every sensor node to identify jamming attacks at wireless devices. These parameters are the maximum packets provided over a given time, the number of packets lowered during this same time frame and the signal intensity provided. To detect the variance in significance between the existing RSS and the standard RSS, the base station modifies the power obtained during the jamming attack. The base station uses such factors to measure the attacks per node and the signal-to-noise ratio, which is often used as inputs to achieve the jamming parameter for the fuzzy control method. The jamming score differs from 0 to 100 and is required to calculate the jamming attack rate, which may vary from 'no jamming' to 'full jamming' condition.

Strasser et al.[22] established the source of false negatives for packet headers in their analysis by studying the RSS to identify responsive jamming attacks in sensor networks during the processing of these bits. This strategy of detection was founded on defined information, minimal connectivity of nodes, and codes for error correction. Experimental findings on generating strong radios indicate its performance without adding unnecessary workload in detecting susceptibility tests jamming attacks. Spuhler et al.[23] suggested a methodology that calculates the rate of packet distribution during the synchronization phase of packet forwarding to detect dynamic reactive jamming attacks. This strategy requires that by measuring the packet distribution frequency using the chip error margin in the obtained sequence number signals, jammers that affect the network topology of the WSN are found. The author Guan and Ge [24] have suggested a distributed technique to identify multimedia network attacks in the WSN. By utilizing several measurement networks to prevent random attacks, a partial differential equation homogenous linear function comprising of a dynamic two-level data transmission multichannel jamming proposed technique was built in their method. The potential jamming attack styles refer to every dynamical system of the covariance matrix. The differences in the frequency of the distribution process could be divided into differences at a higher stage, such as stochastic switching and average deterministic frequency hopping.

In the paper [25], Cordero and Lisser studied a heterogeneous WSN under jamming attack to use a selective issue of a different-player non - cooperative potential. The functional form utilized here is dependent on both transmission errors and noise proportion at the detector and the issue of the system has also been solved by a simple linear cone system. Numerical findings indicate also that the interface difference between the different networks should be considered during the development of a jamming attack detection approach. To protect towards jamming attacks in WSNs, Mpitziopoulos, and Gavalas [26] suggest a design network, Ares, which would be a combination of frequency - hopping continuum and frequency - hopping spread spectrum. The FHSS is being used in the 5GHz

band with 51 different frequencies in the proposed approach to producing a network series to use a code also specified in the sensor network and the data channel. Each one of these channels uses 16-bit pseudo-noise code enhancement with DSSS synchronization generated from a certain security code used in the development of FHSS channels. Simulation findings show that within a jammed Wsns, as described in the following sensor network systems, Ares nodes will maintain an adequate average packet performance with decreased energy consumption.

The author, Alnifie, and Simons [27] suggested a dynamic network system, MULti-channel encrypted communications framework, which is intended to extract data from jamming fields to respond to a WSN radio jamming malicious attacks. It operates by identifying relevant nodes in the jammed region to various networks to destroy the intruder. The vulnerability to effective jamming attacks of WSN network architectures like AODV, DSR, and the new MPH has also been studied [28]. An updated variant of the networks, AODV-M, DSR-M, and MPH-M, was subsequently evaluated and the results indicate that the nodes are protected if the nodes operating the detection techniques identify an attack and the scheduling algorithms modify their routes to prevent independent entities. In the paper [29], a query-based jamming detector technique was introduced. It is a methodology focused on an anomaly and its implementation is spread. It operates by distinguishing, using parameters like negative packet ratio, packet distribution ratio, and amount of effort used, between instances of attack state and normal network topology. This again guarantees the sensor nodes connect to their neighbors to obtain a better degree of detection.

In the paper [30], a game-theoretic strategy was implemented to attain a proper network existence and packet distribution efficiency during several or individual jammer attacks in WSN using Stackelberg game mechanics of single-leader maximum-followers. This method, TC-JAM, follows a method of topological power, where the sink node functions as a representative in monitoring nodes influenced by the jamming attack. The mobile nodes, that function as associates, maintain that an optimal degree of transmission capacity is reached while maintaining the coverage of a significant percentage of neighboring nodes. To predict the existence of a jamming attack, all of these proposed approaches have been used parameters from various layers, but there are certain system impacts like interactions and packet errors due to intrusion and poor connections that display general similar behavior to a jamming attack. Any of these parameters that have been used to detect jamming attacks in the literature would also yield high false alarm rates. This paper proposes the Cognitive Ratio Networks (CRNs) techniques in this article and uses the IDS Detector as the key measure to differentiate between processes and changes of traffic and jamming attacks.

III. PROPOSED WORK

The attacker malicious code starts sending or receive signals in a jamming attack to block legitimate users in a group. In general, this scenario produces a state of denial of services. The jammer could also send encrypted data actively so that the network might not even be sensed as inactive by a real person. Legitimate members, on either side, could be required to collect junk data constantly transmitted by the jammer and thus attack a radio signal and destroy the network packets received by an authorized user. The attacker could jam the support vectors used to communicating sensor data between CRs as a bad attack. This attack is considered a typical attack on healthcare services. If the intruder makes threats on the access info, they would also come to recognize that new paradigm the CRN would move to and he will be able to jam it. In MAC and physical layers [8][9][10], this form of jamming attacks could be performed.

3.1. Framework for Jamming Attacks

Jamming attacks threaten the wireless systems' actual and cross-layer layers [31]. The required contact between a receiver at position A and a receiver at position B is disrupted in these activities by jamming sensors that hold the network occupied. When the jamming sensors represent the channel for a long period, a denial of service may be generated [31]. If the output frequency at position A is defined by a (m) and the transfer function at position B is defined by b (m), then, in the isolation of the jammer signals, the signal power at position B is provided by,

$$b(m) = a(m) + I(m) \quad (1)$$

Where a (m) is the required signal, the signal strength is b (m), and i (m), is a gaussian distribution found in the transmitter-receiver direction. The jammers will spoof the desired signals to overflow the channel by producing a signal defined as $a_z(m)$. In the involvement of the jammer transmitter at position B, the receiving signals are then provided as:

$$b(m) = a(m) + a_z(m) + i(m) + i_1(m) \quad (2)$$

Where $a_z(m)$ is the jammer signal and $i_1(m)$, is the interference between the transmitter and the direction of the jammer along the direction. The issue of jamming analysis can therefore be described as a hypothesis, one where the recipient must select between the different sides, F_1, and F_p. F_1, is the condition where there is no jamming of the transmitted power, thus F_p. The place in which the transmitted power is jammed in the system. This issue could therefore be represented as a classification task for which the adding functionalities must be assigned to several of the 2 categories by the Cognitive Ratio techniques: the frequency response is the intended signal, class F, or the signal strength is a jamming response, class G.

To track and monitor jamming attacks, an intrusion detection system is used. IDS is a standard protocol and a program capable of detecting system intrusions. IDS is usually known as IDS based on signatures and IDS based on anomalies. IDS dependent on signatures is often referred to as IDS given the information or IDS dependent on misuse. It aims at network traffic and scans for patterns that complement the system's established signatures. Anomaly-based IDS is often referred to as IDS based on behavior. By monitoring network traffic over the current pattern of measurement, it gathers time recording and this provides an output benchmark. Data collection is an information collection that contains factors like the kinds of network packets, use of server storage or CPU, and numbers of packets. The IDS framework evaluates the network operation with this benchmark until the benchmark is defined. If it reaches the average, the "wrapping point" defines it as standard. Then the IDS node transmits a notification to the developer [32] directly. An anomaly-based IDS is being used in an analysis to recognize jamming attacks. It requires two stages, such as the process of learning and the stage of identification. It extracts all the knowledge about cognitive radio network criteria during the learning process, like packet distribution ratio, regular protocol service activity, signal power, primary access control time, and traffic congestion, to efficiently detect CRN irregularities due to attacks. Anomalous variations in the sensor nodes named as an anomaly are verified in the detection process.

There are various ways for attackers to identify the network anywhere and anytime. Thus, it is simple for all organizations to identify security risks. Both descriptive and inferential users of the network can be targeted by attackers. The attackers are often influenced by secondary consumers. In the identification and prevention of attacks on cognitive radio networks, different detection methods are used. The detection strategy requires two stages. The cellular network attack is analyzed in this section, such as the jamming attack. The evaluation of signal frequency and the packet delay ratio detects jamming attacks. To accurately detect malicious activity in CRNs, the processing of the Switch and Routing protocol system requires the identification stage of the IDS. The normal activity or output of the network is recognized during the learning process. The anomalous changes were found using the discriminant analysis, linear regression algorithm in the detection stage.

IDS' identification process easily detects the level of difference in the activity of CRN. Samples calculated by the source node are tested in the instance of a malicious network jammed a key user. If the Sample is huge, its performance of the system will be reduced. An application's Detection rate is the ratio of the number of requests that the user receives and the number of nodes received. The optimal threshold detection method is proposed based on the multivariate algorithm is used in this function to identify the significant change in the proposed method activity of sensor nodes attacked by jamming intruder. In standard circumstances, it is known that if some difference is observed, the average scores of the probability distribution are poor, it becomes positive. F_x, series is obtained as

$$F_x = \partial * H_x, \quad (3)$$

Where, ∂ is the average of H_x, standard results during the testing span. During each jamming attack, the rapid increase in the average F_x, a function could be less constrained by, i = (2∂).

After that, as in equation (3), the non-parametric series S_m, is represented where x^+ = x if x > 1; otherwise x^+ = 1. An exception suggests a significant amount of S_m. The maximum of identification π is calculated as follows [33].

$$S_m = S\_(m+1) * F\_x^+; F_1 = 1 \quad (4)$$

$$\pi = (x - \partial)\, m_e \quad (5)$$

Where the relevant high spectral efficiency is denoted by m_e. A specific rate is calculated for easier identification of an exception in the CRN. The IDS modifies S_m, over a certain time in the detection process. When the CRN is in a normal state, the quality of Yn keeps insignificant. On

International Innovative Research Journal of Engineering and Technology
ISSN: 2456-1983 Vol: 6 Issue: 2 December 2020

such a jamming attack, this S_m, begins to develop. If S_m, reaches the predefined amount of ∂ and the SS is strong at the sensor node, a warning is created to the possibilities of jamming attack.

IV. PERFORMANCE RESULTS

The monitoring framework for intrusion is introduced in the Matlab software. Using the time-frequency representation in a specific bandwidth, the existence of the privilege holder or default user is known. Suppose that IDS works at similar times-rounds. The energy efficiency spectrum in each major source of energy accessible in the position is given in figure 2. The additional usage positions are open, indicating the bandwidth is accessible to alternative providers / cognitive radio users. The frequency range of the CRN structure is given. There are 3 main applications required in the section below. Some other device positions are open, which indicates the sufficient to improve / cognitive user range is active.

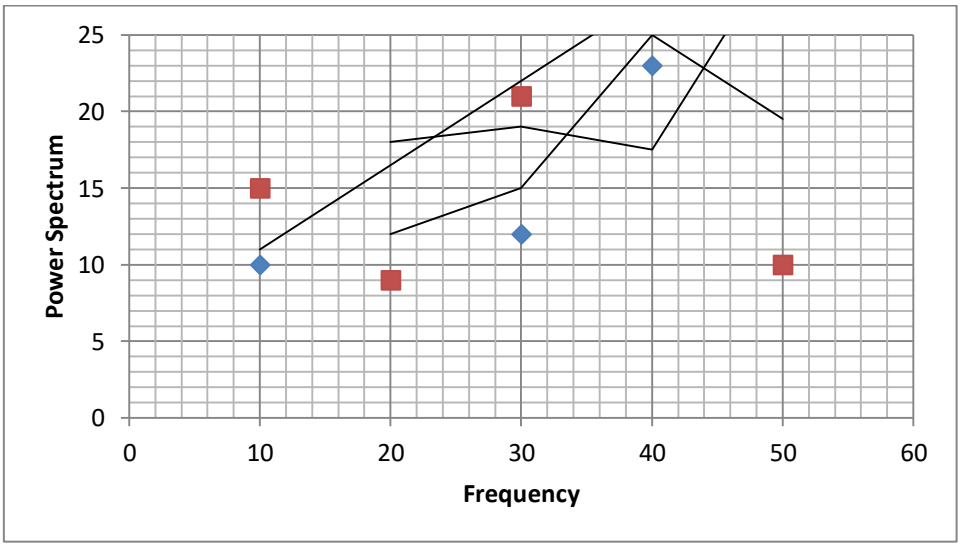

Figure 2. CRN platform's sampling rate

The F_x, series detected by the IDS during most of the training and identification process at the sensor node is shown in figure 3. Figure 4 shows H_x, series, or the predicted values that have been acquired by $F_x = \partial * H_x$. This note that the identification of irregularities is about the steadily expanded time. Also, this algorithm has much less difficulty and it is easy to achieve.

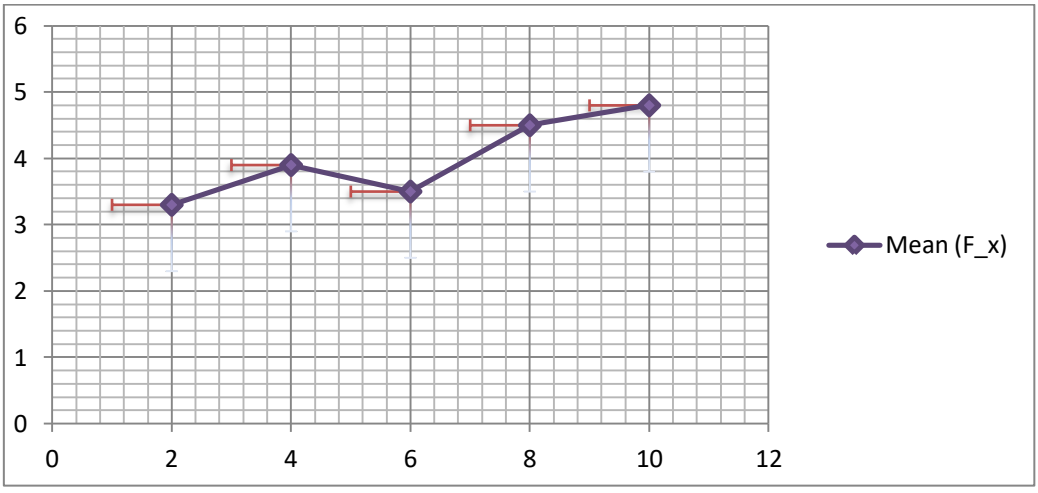

Figure 3. F_x Mean Value

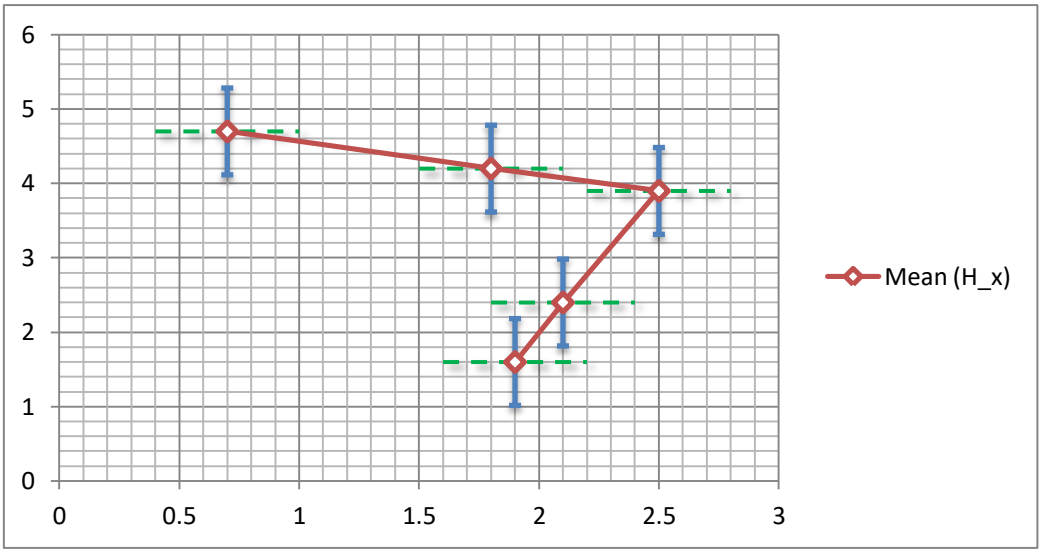

Figure 4. H_x Mean Value

V. CONCLUSION

The important security intrusion on cognitive radio networks is a jamming attack. It impacts the effectiveness of the overall CRN. The great choice is thus used to detect the network's irregular shifts. For intermediate customers, it is most beneficial to reach the bandwidth without interruption. And it also ensures greater efficiency in the instance of any network intrusion. The experimental data for jamming, swapping, and error frequencies were estimated by multiplying to consider jamming attacks, user mobility, and spectrum accessibility variables. Given transferring frequency and error frequency, analysts have shown that the jamming strategies perform better than the frequency hopping jamming system. Proposing a technical solution to the game in which it makes user versatility to minimize jamming is underway.

REFERENCES

[1] Arjoune, Y., Salahdine, F., Islam, M. S., Ghribi, E., & Kaabouch, N. (2020, January). A Novel Jamming Attacks Detection Approach Based on Machine Learning for Wireless Communication. In *2020 International Conference on Information Networking (ICOIN)* (pp. 459-464). IEEE.

[2] Adem, N., Hamdaoui, B., & Yavuz, A. (2016). Mitigating jamming attacks in mobile cognitive networks through time hopping. *Wireless Communications and Mobile Computing*, *16*(17), 3004-3014.

[3] Hossain, E., Rasti, M., Tabassum, H., & Abdelnasser, A. (2014). Evolution toward 5G multi-tier cellular wireless networks: An interference management perspective. *IEEE Wireless Communications*, *21*(3), 118-127.

[4] Mitola, J., & Maguire, G. Q. (1999). Cognitive radio: making software radios more personal. *IEEE personal communications*, *6*(4), 13-18.

[5] Mitola, J. I. (2002). Cognitive radio. An integrated agent architecture for software defined radio.

[6] Chen, K. C., Peng, Y. J., Prasad, N., Liang, Y. C., & Sun, S. (2008, January). Cognitive radio network architecture: part I--general structure. In *Proceedings of the 2nd international conference on Ubiquitous information management and communication* (pp. 114-119).

[7] Haykin, S. (2005). Cognitive radio: brain-empowered wireless communications. *IEEE journal on selected areas in communications*, *23*(2), 201-220.

[8] El-Hajj, W., Safa, H., & Guizani, M. (2011). Survey of security issues in cognitive radio networks. *Journal of Internet Technology*, *12*(2), 181-198.

[9] Shan, D., Zeng, K., Richardson, P., & Xiang, W. (2013, July). Detecting multi-channel wireless microphone user emulation attacks in white space with

noise. In *8th International Conference on Cognitive Radio Oriented Wireless Networks* (pp. 154-159). IEEE.

[10] Borle, K. M., Chen, B., & Du, W. (2013, May). A physical layer authentication scheme for countering primary user emulation attack. In *2013 IEEE International Conference on Acoustics, Speech and Signal Processing* (pp. 2935-2939). IEEE.

[11] Chin, W. L., Tseng, C. L., Tsai, C. S., Kao, W. C., & Kao, C. W. (2012, May). Channel-based detection of primary user emulation attacks in cognitive radios. In *2012 IEEE 75th Vehicular Technology Conference (VTC Spring)* (pp. 1-5). IEEE.

[12] Li, H., & Han, Z. (2010). Catch me if you can: An abnormality detection approach for collaborative spectrum sensing in cognitive radio networks. *IEEE Transactions on Wireless Communications*, *9*(11), 3554-3565.

[13] Gao, Z., Zhu, H., Li, S., Du, S., & Li, X. (2012). Security and privacy of collaborative spectrum sensing in cognitive radio networks. *IEEE Wireless Communications*, *19*(6), 106-112.

[14] Grissa, M., Yavuz, A., & Hamdaoui, B. (2015, December). Lpos: Location privacy for optimal sensing in cognitive radio networks. In 2015 IEEE Global Communications Conference (GLOBECOM) (pp. 1-6). IEEE.

[15] Wu, Y., Wang, B., Liu, K. R., & Clancy, T. C. (2011). Anti-jamming games in multi-channel cognitive radio networks. IEEE Journal on Selected Areas in Communications, 30(1), 4-15.

[16] Xiao, L., Liu, J., Li, Y., Mandayam, N. B., & Poor, H. V. (2014, December). Prospect theoretic analysis of anti-jamming communications in cognitive radio networks. In *2014 IEEE Global Communications Conference* (pp. 746-751). IEEE.

[17] Dabcevic, K., Betancourt, A., Marcenaro, L., & Regazzoni, C. S. (2014, May). A fictitious play-based game-theoretical approach to alleviating jamming attacks for cognitive radios. In *2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)* (pp. 8158-8162). IEEE.

[18] Xiao, L., Chen, T., Liu, J., & Dai, H. (2015). Anti-jamming transmission Stackelberg game with observation errors. *IEEE Communications Letters*, *19*(6), 949-952.

[19] Su, H., Wang, Q., Ren, K., & Xing, K. (2011, June). Jamming-resilient dynamic spectrum access for cognitive radio networks. In *2011 IEEE International Conference on Communications (ICC)* (pp. 1-5). IEEE.

[20] Li, X., & Cadeau, W. (2011, March). Anti-jamming performance of cognitive radio networks. In *2011 45th Annual Conference on Information Sciences and Systems* (pp. 1-6). IEEE.

[21] Misra, S., Singh, R., & Mohan, S. V. (2010). Information warfare-worthy jamming attack detection mechanism for wireless sensor networks using a fuzzy inference system. *Sensors*, *10*(4), 3444-3479.

[22] Strasser, M., Danev, B., & Čapkun, S. (2010). Detection of reactive jamming in sensor networks. *ACM Transactions on Sensor Networks (TOSN)*, *7*(2), 1-29.

[23] Spuhler, M., Giustiniano, D., Lenders, V., Wilhelm, M., & Schmitt, J. B. (2014). Detection of reactive jamming in DSSS-based wireless communications. *IEEE Transactions on Wireless Communications*, *13*(3), 1593-1603.

[24] Guan, Y., & Ge, X. (2017). Distributed secure estimation over wireless sensor networks against random multichannel jamming attacks. *IEEE Access*, *5*, 10858-10870.

[25] Cordero, C. V., & Lisser, A. (2015). Jamming Attacks Reliable Prevention in a Clustered Wireless Sensor Network. *Wireless Personal Communications*, *85*(3), 925-936.

[26] Mpitziopoulos, A., & Gavalas, D. (2009). An effective defensive node against jamming attacks in sensor networks. *Security and Communication Networks*, *2*(2), 145-163.

[27] Alnifie, G., & Simon, R. (2007, October). A multi-channel defense against jamming attacks in wireless sensor networks. In *Proceedings of the 3rd ACM workshop on QoS and security for wireless and mobile networks* (pp. 95-104).

[28] Del-Valle-Soto, C., Mex-Perera, C., Monroy, R., & Nolazco-Flores, J. A. (2017). MPH-M, AODV-M and DSR-M performance evaluation under jamming attacks. *Sensors*, *17*(7), 1573.

[29] ÇAKIROĞLU, M., & ÖZCERİT, A. T. (2011). Design and evaluation of a query-based jamming detection algorithm for wireless sensor networks. *Turkish Journal of Electrical Engineering & Computer Sciences*, *19*(1), 1-19.

[30] Bhavathankar, P., Mondal, A., & Misra, S. (2017). Topology control in the presence of jammers for wireless sensor networks. *International Journal of Communication Systems*, *30*(13), e3289.

[31] Sufyan, N., Saqib, N. A., & Zia, M. (2013). Detection of jamming attacks in 802.11 b wireless networks. *EURASIP Journal on Wireless Communications and Networking*, *2013*(1), 208.

[32] Axelsson, S. (2000). *Intrusion detection systems: A survey and taxonomy* (Vol. 99). Technical report.

[33] Wang, H., Zhang, D., & Shin, K. G. (2004). Change-point monitoring for the detection of DoS attacks. *IEEE Transactions on dependable and secure computing*, *1*(4), 193-208.

