ICIC Express Letters
Volume **15**, Number **2**, February **2021**

 ISSN 1881-803X
pp. **125–134**

ENHANCED COGNITIVE RADIO NETWORK APPROACH WITH AN EFFECTIVE AUTHENTICATION ALGORITHM

Faisal Yousef Alzyoud

Faculty of Information Technology
Isra University
P.O. 11622 Box (22&23), Amman, Jordan
faisal.alzyoud@iu.edu.jo

Received May 2020; accepted August 2020

Abstract. *The request for network using is expanding quickly to address the enormous growth of networks users' human-to-human, human-to-machine, or machine-to-machine communications. Fifth generation technology is a promising innovation that can be utilized as an arrangement to address the increment request of clients, but unfortunately it may not be adequate solution for frequency or spectrum shortages, so different solutions were proposed to utilize the frequency usage. This paper discusses cognitive radio networks and the simulation depends on energy detection techniques to handle the channel availability to be used by unlicensed clients. However, cognitive radio networks suffer from network security as they mainly depend on frequency spectrum, so in this research a one-way hash user ID is proposed to authenticate cognitive radio networks' clients using BCrypt. The proposed solutions were tested using MATLAB software and C# language that is used to implement BCrypt, the obtained results are promising solutions, and it can be implemented on a wide range of cognitive radio applications including security networks and so on.*

Keywords: Cognitive Radio Networks (CRNs), Denial of Service (DoS), Primary Users (PUs), Secondary Users (SUs), 5th Generation (5G)

1. **Introduction.** The transformation towards the 5 Generation (5G) and the proliferation of smart devices among the network users raise the tendency for bandwidth consumption, and several researches started to provide the insight and the roadmap for future to overcome the whelming use of available secure frequencies. One of these solutions is the use of dynamic spectrum access technique which is known as Cognitive Radio Networks (CRNs). Using CRNs will enable users to share and utilize available idle bandwidth between themselves without the need to compromise security; this approach will help service providers to accommodate more users efficiently with available bandwidth which will reduce cost on both service providers as well as bandwidth users taking account of maintaining high level of QoS.

The main feature for CRNs is using frequency spectrum in an effective way by taking advantage of channel conditions, code books, and message transformation to share the spectrum between different users. The number of users can be classified into two kinds of users: Primary Users (PUs) and Secondary Users (SUs), and the secondary users can be classified also by giving those weights according to their types of application through enabling the type of service field in network layer as depicted in [10]. Cognitive radio can be defined as smart software which can fulfill and settle users demand according to free spectrum status. Free spectrum is dynamically sensed and the free spectrum is assigned for unlicensed user when the licensed users are not present, so cognitive radio has four main functions: firstly, spectrum sensing followed by spectrum decision [11],

DOI: 10.24507/icicel.15.02.125

then spectrum sharing and finally spectrum mobility. There are several techniques used to sense spectrum availability and to prevent interference between users as listed below:

- Energy detection: in this technique the signal strength is measured and compared with the output energy level, and compared with a threshold level, this technique suffers from the inability to differentiate between primary users signals and noise [12].
- Filters matching: demodulation in this technique is used for PUs signal in order to perform coherent detection within a less time; however, this technique needs a special receiver for every PU [13].
- Cyclostationary: this technique is based on feature detector to exploit the inherent in the received signal to detect primary signals periodically, as most of the signals are varying with time, so it can differentiate noise from PUs signals as well. This issue suffers from longer processing time and higher computational complexity [12].
- Cooperative detection: in this technique, the number of different radio signals is sensed using different sensing techniques suitable to cognitive radio systems [13].
- Waveform based detection: this technique is usually used to synchronize wireless network systems, and it needs short measurement time [14].

CRNs are classified into two types: Cognitive Radio Ad Hoc networks and Cognitive Radio infrastructure networks as Figure 1. As CRNs are kind of Ad Hoc network, they are vulnerable to the same threats Ad hoc networks are. These attacks are classified as per targeted layer into: Physical, Link, Network, and Transport. Any solution proposed to counter CRN attacks should abide by the Federal Communication Commission (FCC) requirement which states that "no modification to the incumbent system should be required to accommodate opportunistic use of the spectrum by secondary users" [15]. In order to maintain this requirement, security solution against attacks on CRN ought to be introduced to the secondary user system [27].

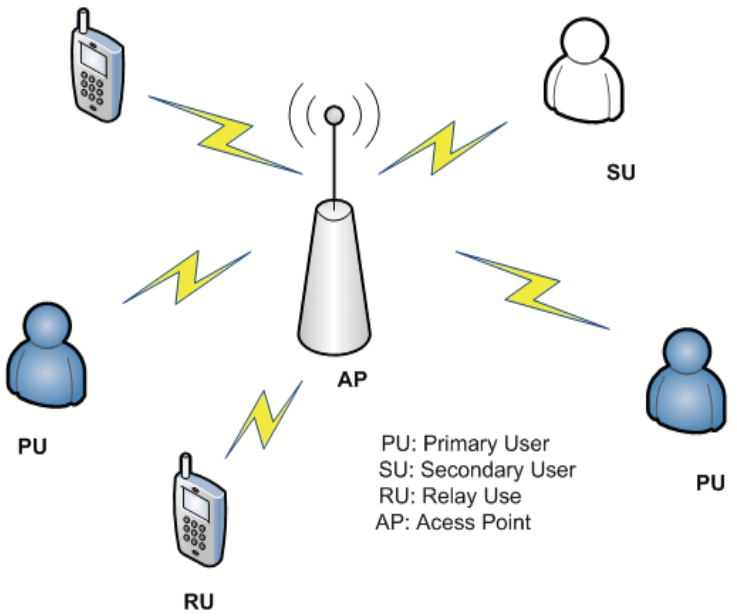

FIGURE 1. Cognitive radio simple central network model

2. **CRNs Security Requirements.** Security in network system is considered as a dominant factor for network system development and users' satisfactions, cognitive radio networks suffer from network security as it exposes to two types of users: one is authorized while the other is not authorized as explained before. The unauthorized users or secondary users have extreme degree for adversaries, and their mobility management cannot

be controlled which lead to difficulties in implementing security countermeasures [2]. Most of the cognitive network threads and attaches are: Denial of Service (DoS), Jamming, and Butter Overflow [1]. Since CRNs are types of wireless network, they need the following security requirement [3,4]:

- Data Availability
- Data Confidentiality
- Data Integrity
- User Authentication
- User Identification
- Non-repudiation

2.1. **CRNs security threats and attacks.** An attack can be defined as any undesired effect on CRNs users which causes service disruption. An attack may occur on any of the five layers in CNRs protocol stack as shown in Figure 2, or between cross-layer [5]. In physical layer, the security is related to the process of spectrum sensing. Transmitter location and the strength of the received signal are used to identify the attackers. MAC address is tested in data link layer and each channel is controlled by a time schedule for transmission and average data packet rate, so unusual activity will not obey this schedule and data rate, which indicates that there is an attack [6]. In network layer the packet will pass from sender node to destination node through different intermediate nodes according to the used routing algorithm and intermediate node routing table, so when there is attack in this layer, the malicious node will either change the captured packet content or discard it after capturing it, so to prevent abnormal activity the received packet should be compared with a buffered one, and if a difference exists then there is abnormal activity or attack. Round trip time is used to detect transport layer attack by monitoring the number of frequent retransmissions with a definite threshold or average value, so when the round trip time is longer than the average value, then there is an attack. The intrusion detection schemes used in this layer are based on RSS and RTT detection [7]. In application layer, attacks can be sensed through monitoring the many connections without real operations such as abnormal activity.

A smart attacker can attack several layer in CRNs at the same time to reduce the possibility of its detection, and this attack is known as the cross-layer attack [8].

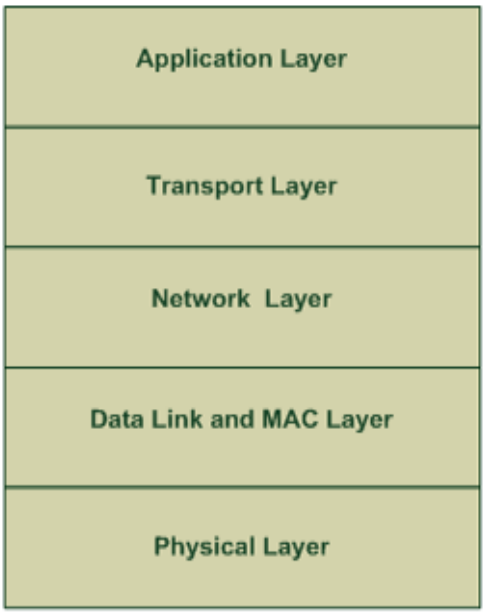

FIGURE 2. CRNs protocol stack

2.2. **CRNs layer attacks and countermeasures.** CRNs have many security threads on each layer as explained before, and there are different countermeasures to handle these thread as depicted in Table 1.

TABLE 1. Stack of CRNs layers' attacks and countermeasures [9]

Layer attack	Example	Countermeasures
Physical layer	• Selfish and Malicious Primary Emulation Attacks, Intentional Jamming and Primary receiver jamming Attacks, and Eavesdropping	• Implement one-way hash function to authenticate tags and embed the physical tag with controlled constellation perturbation [20]. • Use either single hop or multi hops directional antenna, and increase number of relays to reduce the probability of eavesdropping [18,19].
Data link layer	• Malicious attacks that include spectrum data sensing, and channel saturation attack	• Use center fusion to keep tracks for the presence of PU's by implementing decision fusion techniques, and use cluster with assigning each cluster with a limit to control the channel [21], and implement predistribution algorithm to distribute the layers to nodes [22].
Network layer	• Routing Disruption Attacks (e.g., Hello attacks)	• Use bidirectional verification and authentication such as fusion center entity verification [23].
Transport layer	• Key Depletion Attack	• Use new ciphering algorithms to perform session key sharing, and implement game theory to prevent attacking through monitoring the behaviors of network users [24].
Application layer	• CR Software	• Use an effective virus detection technique, and use tamper resistance and implement authentication mechanisms and digital signature scheme using keyless hash function and a constant fixed output [25,26].

3. **Cognitive Radio Model Using MATLAB.** In this paper power spectral density estimation is used to discover free spectrum as Power Spectral Density (PSD) is considered an effective technique to determine the instance power being transmitted at a specific channel frequency. PSD can be defined as a positive real or frequency variable functions of that are related to stationary stochastic process, or a deterministic function of time, PSD measured by power per hertz (dB/Hz) units, or energy per hertz units. Figure 3 represents a proposed model for applying cognitive radio network using MATLAB software; it starts with initializing five frequencies that are modulated using Amplitude Modulation (AM) to handle carrier signals. PSD is used to estimate the spectrum density for the five input frequencies and in this stage the results can be represented without the effect of noise as shown in Figure 3. The final two steps are related to the noise using Additive White Gaussian Noise (AWGN) model to mimic the real situation, after considering the noise effect modulation is considered and the results can be presented.

MATLAB is recommended to be used for cognitive radio networks as it is the most suitable and ease computing techniques for most engineering applications; since MATLAB can be implemented in data visualization, data analysis, interactive environment for

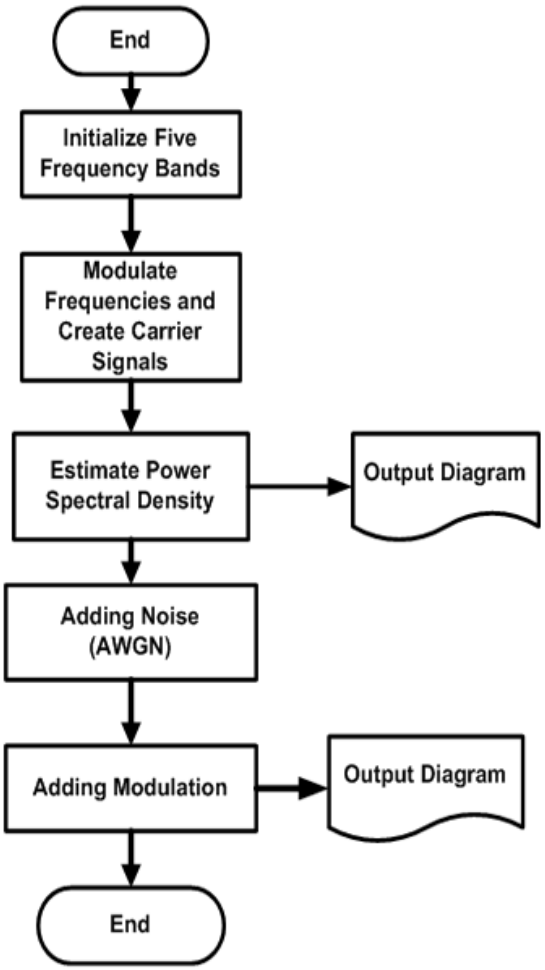

FIGURE 3. A proposed model for cognitive radio network using MATLAB

algorithm development, and numerical computation [16]. In this research the following parameters are used in the proposed model for CRNs: five carrier frequencies Fc1 = 1000 KHz, Fc2 = 2000 KHz, Fc3 = 3000 KHz, Fc4 = 4000 KHz & Fc5 = 5000 KHz and every user's base band data signal is modulated over the spectrum density. Power spectrum density is estimated and the output is presented as shown in Figure 4. The results represent the allocated free space which can be allocated to SUs. Noise is added using Additive White Gaussian Noise (AWGN) model to mimic real situations since AWGN is considered as a basic noise model that occurs in nature with constant spectral distribution, as it is a good model for many wireless deep space communication links [10,16]. It is noted from Figure 4 that the power spread speed spectrum represents two primary users and three free frequency slots, since the power/frequency ratio is above zero level just for frequency one and two respectively which means that these two frequencies are occupied by PUs, while power/frequency ratios for three, four and five frequencies are less than zero which means that they are not occupied and can be assigned to other users.

In Figure 5, the frequencies' spectrum for three, four and five are assigned to secondary users to utilize the available frequency, so it is noted that all the power/frequency ratios are above zero level, which means that the spectrum is fully optimized.

4. **Cognitive Radio Authentication Proposed Algorithm.** The main use for CRNs technology is to share the available spectrum opportunistically without causing any harmful interference to primary user. However, unfortunately the attacker may mimic primary user signals to get unfair share of radio channels. Therefore, it is important to distinguish primary user's signals from an attacker signals or unauthorized users signals.

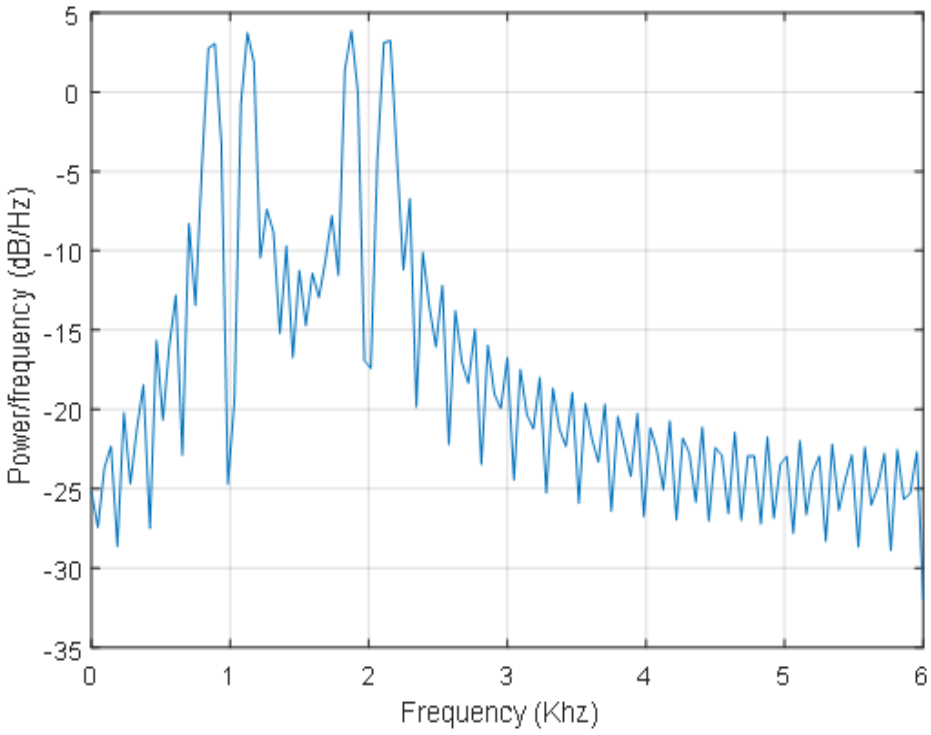

FIGURE 4. Power spectrum density with two occupied frequencies' spectrum

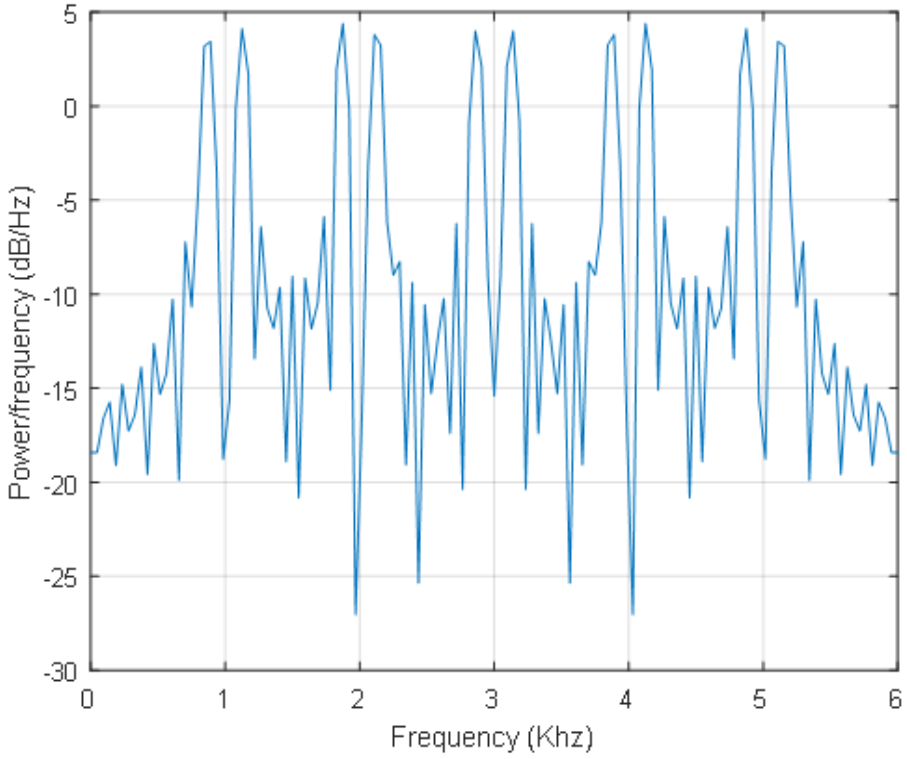

FIGURE 5. Fully utilized spectrum

Cognitive radio networks suffer from network security as they mainly depend on frequency spectrum, so the main idea in this research is improving security in application layer by a one-way hash user ID through proposing authentication procedures in cognitive radio networks' users by using BCrypt as it is based on the Blowfish block cipher in the

form of an adaptive hash function. Net port of BCrypt is implemented in C#. It uses a variant of the Blowfish encryption algorithms keying schedule, and introduces a work factor, which allows in determining how expensive the hash function will be. To prove why BCrypt is important to be used as authentication algorithm, its strength comes from the security of password storing process. In general, it uses a hashing algorithm which is adjusted over time, so it requires more CPU power to generate the hashes leading more protection against Moore's Law. The more CPU power that is required to hash a given password, the more time a hacker must perform for each password. For example, if someone needs to know how long the interval to crack a password of 8 random lower case letters, it has an entropy of $n = \log_2(26^8) = 38$ bits, so to track it you would need $2^{38-1}/1000$ seconds = 4 years [17].

In this research infrastructure CRNs is used as it has a control base station. CRNs' users are categorized into: Primary Users (PUs), and Secondary Users (SUs). When any user wants to use the channel, it has to register its information in the control base station by implementing an effective BCrypt algorithm which will hash its ID as depicted in Figure 6. The PUs can use the channel after they are registered by the control station, while SUs have to wait until the channel has free spectrum frequency and this procedure is guided by the control base station. Every user is assigned with a user name and a password after the registration process, so if any intruder tries to capture the password more than three times it is halted by the control base station.

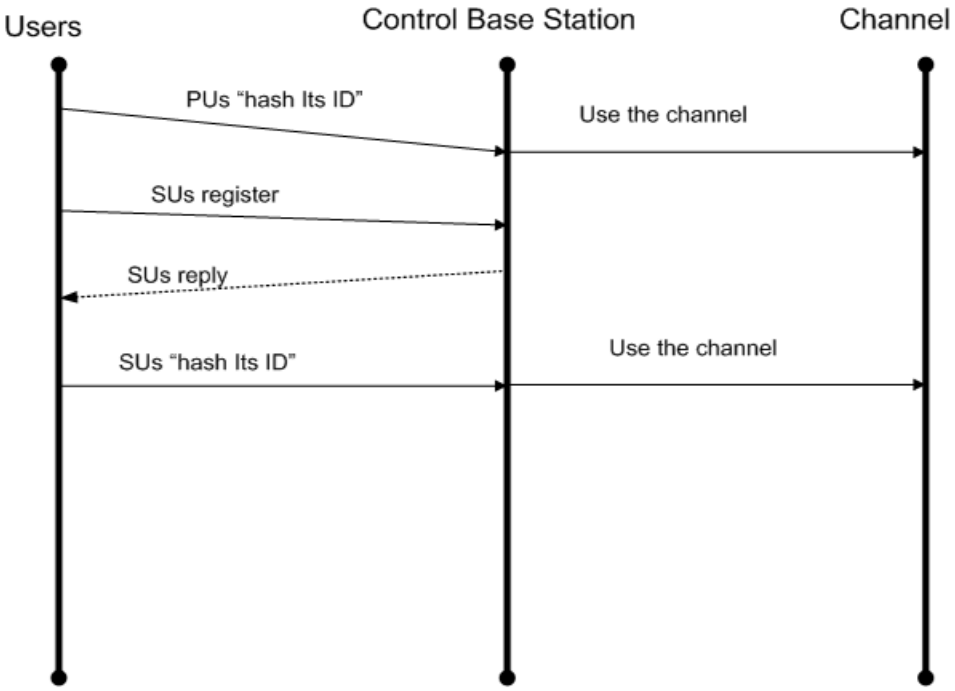

FIGURE 6. A proposed CRNs state diagram

The details of the proposed authentication algorithm are illustrated in Figure 7 starting from the registration process which is done by the control station using the user ID, and then the users are classified as two kinds of users (PUs and SUs) that give the highest priority to PUs to use the channel. In addition, the proposed method is improving average waiting time for SUs by enabling SUs to register and wait in queue depending on his registration time and process time.

5. **Conclusion and Future Work.** CRNs are considered a promising network technology that can be implemented in the future to overcome the leakage in frequency spectrum as

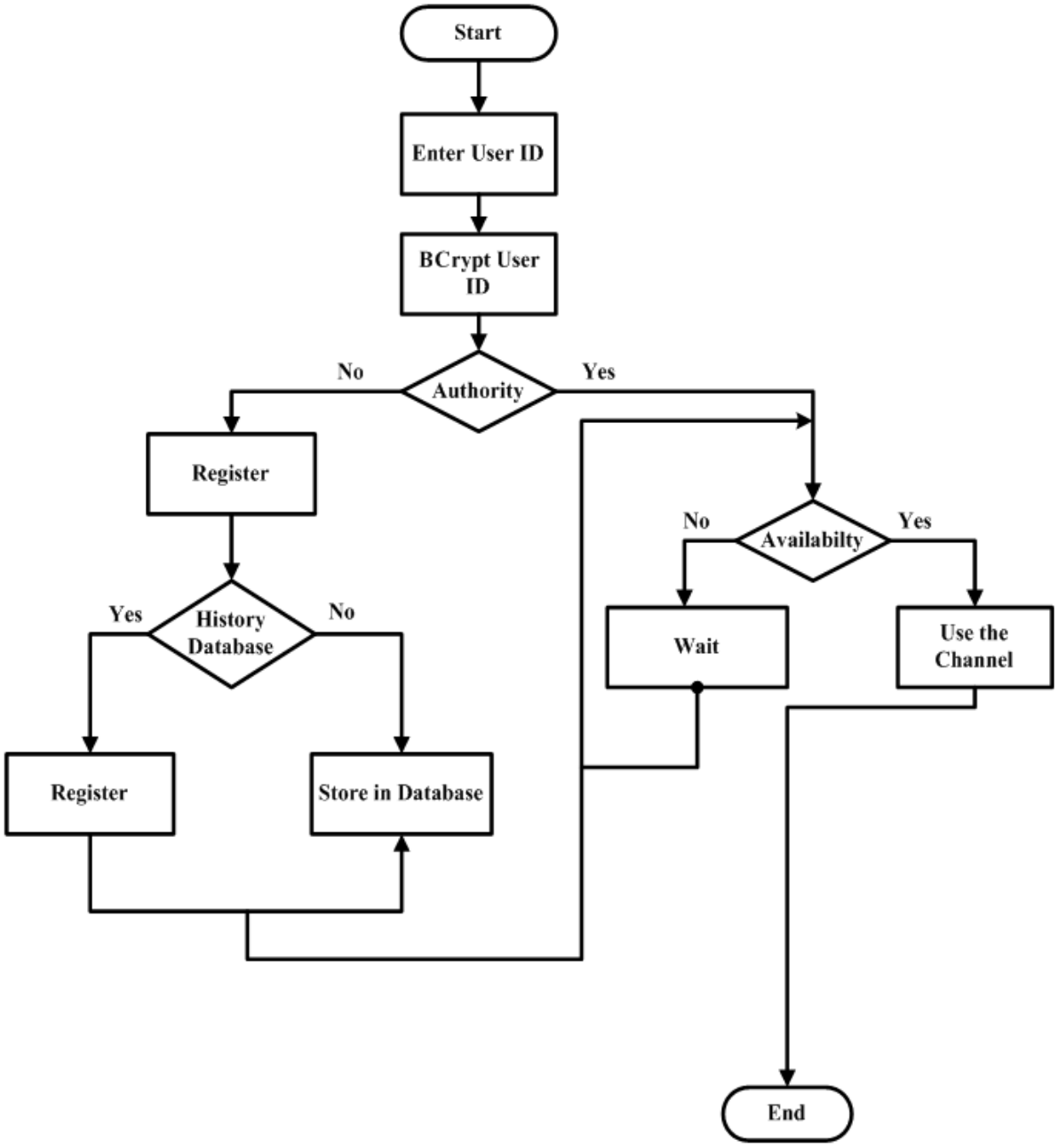

FIGURE 7. Proposed user authentication and channel usage algorithm

the number of networks' users is whelming and growing up. As CRNs use unguided media, they suffer from security threads, so in this research MATLAB software is developed to implement enhanced CRNs relying on energy sensing to detect the empty frequency slots or holes, and then the empty slots of free frequencies are assigned to unlicensed users to utilize the channel usage. CRNs architecture is studied in detail to locate the expected threats and countermeasure for each threat. A one way hashing function BCrypt algorithm is used to authenticate the channel users either primary users or secondary user; since this algorithm is invulnerable to brute force and dictionary attacks as it consumes a lot of power and resources to crack. C# language is used to implement the users' authentication. The obtained results are applicable. In the future we are going to do further implementation on spectrum sensing techniques and try to apply them using the available hardware and do further researches on the expected threats and develop countermeasures for them. We plan to extend this paper to include a framework for ad hoc CRNs authentication; since most of CRNs researches are concentrated on infrastructure CRNs.

REFERENCES

[1] Sohu, I. Ahmed et al., Analogous study of security threats in cognitive radio, *The 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*, 2019.

[2] N. Mishra, S. Srivastava and S. N. Sharan, Countermeasures for primary user emulation attack: A comprehensive review, *Wireless Personal Communications*, pp.1-32, 2020.

[3] E. H. Salman, N. K. Noordin, S. J. Hashim, F. Hashim and C. K. Ng, An overview of spectrum sensing techniques for cognitive LTE and LTE-A radio systems, *Telecommunication Systems*, vol.65, no.2, pp.215-228, 2016.

[4] M. Z. Alom et al., Enhanced spectrum sensing based on energy detection in cognitive radio network using adaptive threshold, *2017 International Conference on Networking, Systems and Security (NSysS)*, pp.138-143, 2017.

[5] F. Salahdine and N. Kaabouch, Security threats, detection, and countermeasures for physical layer in cognitive radio networks: A survey, *Physical Communication*, vol.39, 2020.

[6] X. Zhang and L. Cheng, Constructing secured cognitive wireless networks: Experiences and challenges, *Wireless Communications and Mobile Computing*, vol.10, no.1, pp.50-69, 2010.

[7] M. W. Akram et al., A review: Security challenges in cognitive radio networks, *The 23rd International Conference on Automation and Computing (ICAC)*, 2017.

[8] M. K. Murmu and A. K. Singh, Security issues in cognitive radio ad hoc networks, *Handbook of Computer Networks and Cyber Security*, pp.247-264, 2020.

[9] D. Ganesh and T. P. Kumar, A survey on advances in security threats and its counter measures in cognitive radio networks, *International Journal of Engineering & Technology (IJET)*, vol.7, pp.372-378, 2018.

[10] F. Y. Alzyoud, W. J. Al_Zyadat, F. Hamed and F. Shrouf, A proposed hybrid approach combined QoS with CR system in smart city, *Eurasian Journal of Analytical Chemistry*, vol.13, no.6, pp.178-185, 2018.

[11] A. Alahmadi et al., Defense against primary user emulation attacks in cognitive radio networks using advanced encryption standard, *IEEE Trans. Information Forensics and Security*, vol.9, no.5, pp.772-781, 2014.

[12] Mohan, P. T. V. Bhuvaneswari and B. J. Stephen, Advanced spectrum sensing techniques, *Sensing Techniques for Next Generation Cognitive Radio Networks*, IGI Global, pp.133-141, 2019.

[13] F. Salahdine et al., Matched filter detection with dynamic threshold for cognitive radio networks, *International Conference on Wireless Networks and Mobile Communications (WINCOM)*, 2015.

[14] M. M. Rathore, A. Ahmad, A. Paul and S. Rho, Urban planning and building smart cities based on the Internet of Things using big data analytics, *Computer Networks*, vol.101, pp.63-80, 2016.

[15] M. S. Gupta and K. Kumar, Progression on spectrum sensing for cognitive radio networks: A survey, classification, challenges and future research issues, *Journal of Network and Computer Applications*, vol.143, pp.47-76, 2019.

[16] E. Bayaki, D. S. Michalopoulos and R. Schober, EDFA-based all-optical relaying in free-space optical systems, *IEEE Trans. Communications*, vol.60, pp.3797-3807, 2012.

[17] J. Blocki, B. Harsha and S. Zhou, On the economics of offline password cracking, *IEEE Symposium on Security and Privacy (SP)*, 2018.

[18] H.-N. Dai, Q. Wang, D. Li and R. C.-W. Wong, On eavesdropping attacks in wireless sensor networks with directional antennas, *International Journal of Distributed Sensor Networks*, 2013.

[19] Y. Zou, J. Zhu, L. Yang, Y. Liang and Y. Yao, Securing physical-layer communications for cognitive radio networks, *IEEE Communications Magazine*, vol.53, no.9, pp.48-54, 2015.

[20] K. M. Borle, B. Chen and W. K. Du, Physical layer spectrum usage authentication in cognitive radio: Analysis and implementation, *IEEE Trans. Information Forensics and Security*, vol.10, no.10, pp.2225-2235, 2015.

[21] F. Nasnin, M. N. Islam and A. Chakrabarty, Security analysis on cognitive radio network, *Smart Innovations in Communication and Computational Sciences*, pp.305-313, 2019.

[22] D. Nagireddygari and J. P. Thomas, MAC-TCP cross-layer attack and its defense in cognitive radio networks, *Proc. of the 10th ACM Symposium on QoS and Security for Wireless and Mobile Networks (Q2SWinet'14)*, pp.71-78, 2014.

[23] G. Rahman and C. C. Wen, Man in the middle attack prevention for edge-fog, mutual authentication scheme, *International Journal of Recent Technology and Engineering (IJRTE)*, 2019.

[24] M. S. Abdalzaher and O. Muta, Employing game theory and TDMA protocol to enhance security and manage power consumption in WSNs-based cognitive radio, *IEEE Access*, vol.7, pp.132923-132936, 2019.

[25] R. K. Sharma and D. B. Rawat, Advances on security threats and countermeasures for cognitive radio networks: A survey, *IEEE Communications Surveys & Tutorials*, vol.17, no.2, pp.1023-1043, 2015.

[26] J. N. Soliman, T. A. Mageed and H. M. El-Hennawy, Countermeasures for layered security attacks on cognitive radio networks based on modified digital signature scheme, *The 8th International Conference on Intelligent Computing and Information Systems (ICICIS)*, Cairo, pp.2-8, 2017.

[27] X. Liu et al., Multi-modal cooperative spectrum sensing based on dempster-shafer fusion in 5G-based cognitive radio, *IEEE Access*, vol.6, pp.199-208, 2017.