The Nucleus ***57****, No. 4 (2020) 141-149*

https://doi.org/10.71330/thenucleus.2020.1180

www.thenucleuspak.org.pk

The Nucleus

ISSN 0029-5698 (Print)

ISSN 2306-6539 (Online)

Performance Modeling and Analysis of Secure Registration Process of CPEs in IEEE 802.22 WRAN Cognitive Radio Network

H. Afzal[1], M.R. Mufti[2*], K.T. Ahmed[1], M. Rehman[3], M. Yousaf[4] and D.M. Qaseem[2]

[1]*Department of Computer Science, Bahauddin Zakariya University, Multan, Pakistan.*

[2]*Department of Computer Science, COMSATS University Islamabad, Vehari Campus Vehari, Pakistan.*

[3]*Department of Information Technology, Government College University Faisalabad. Pakistan.*

[4]*Riphah Institute of Systems Engineering, Riphah International University, Islamabad, Pakistan*.

ABSTRACT

The proliferation of wireless technologies has affected the radio frequency spectrum which is a limited natural resource. Increase in the development of diverse wireless technologies is creating a spectrum shortage problem. The usage of radio frequency spectrum is not uniform because, some of the licensed spectrums remain vacant most of the time. A cognitive radio (CR) is one of the solutions to address this problem. Meanwhile, the popularity of cloud computing has attracted the researchers to get its benefits for the efficient utilization of cognitive radio networks (CRNs). Both of these technologies can be integrated to form a new type of network called cognitive radio cloud network in which security is one of the major issues in CRNs. This paper presents the analytical framework to perform analysis of the registration process of Customer Premises Equipment (CPE) with the base station in Wireless Regional Area Network (WRAN) in addition of the cloud platform for applying the security. The performance is investigated by comparing the scenarios of keeping the security features on and off in the system. The numerical results confirm that the proposed system works well, when security is kept on.

Keywords**:** *Admission Control, Cloud Computing, Cognitive Radio Network, Customer Premises Equipment, IEEE 802.22 WRAN, Security*

1. Introduction

The Federal Communication Commission (FCC) of United States has decided in 1999 to efficiently use the frequencies of spectrum for wireless broadcasting, e.g., television broadcasting, radio broadcasting, etc. This has caused the danger of overloading the spectrum and its scarcity beside the risk of bad utilization [1]. The FCC then defined the solution of these problems in the form of the Cognitive Radio Network (CRN). According to it, a Cognitive Radio (CR) is a radio that can adjust its transmission parameters based on the interaction with its operating environment [2]. It is the enhanced form of the Software Defined Radio (SDR) that enables the dynamic use of the spectrum [3] to improve the utilization of radio frequencies [4]. Due to the growing interest in CRN, a CR has been seen as a possible driver for the next-generation wireless networks [5]. To efficiently use the frequencies, FCC divides the users into two categories: (i) Primary Users (PUs) or licensed users that have the right to operate in a band, (ii) Secondary users (SUs) or CR users that can use the spectrum of PUs opportunistically when the spectrum is in idle state [6].

Meanwhile, in the last few years, the demand to shift the onsite computing into the cloud computing has been increased. Cloud computing allows to access the resources from a pool to serve the objectives of availability, scalability, and hardware abstraction from the clients and is designed to work on the principle of "pay-per-use". The resources are provided with service, storage space, some computing platforms as virtual machines [7] and networking infrastructures that can be attained upon requests [8-9]. When CRNs are combined with cloud computing, the resulting paradigm behaves more intelligently than the previous ones [10]. The behavior of attacks and hacking in CRNs is almost the same as in traditional wireless networks. Some SUs in CRN may behave as malicious users by presenting themselves as PUs. In order to access the CR channel falsely, these malicious SUs preempt those SUs that are already using CR channels. This is because the malicious SUs present themselves as PUs with higher priority to access the radio channel. This paper investigates the performance of a secure registration process of customer premises equipment (CPE), i.e., SUs in CRN (WRAN) with the support of the cloud platform. In the present study, the security server, admission control server and buffer are saved on the cloud in order to check the authenticity of both the CPEs and incumbents, i.e., PUs along with the channel status whether free or occupied. The primary advantage of integrating WRAN with Cloud platform is that, any other network communicating with current WRAN can access the same information. All users within the WRAN cell can get the respective information either from base station (BS) or from the cloud. No extra overhead is borne by the WRAN BS. In Table 1 the key notations used in this work are summarized.

The proposed framework may be applied to other wireless emerging technologies, such as 5G and 6G, whether centralized or ad-hoc based on or integrated with CRN concept. If the future technologies are centralized, then the same framework can be utilized. On the other hand, if they are ad-hoc, then the steps for registration with the BS after last phase will be ignored. Almost all the future wireless technologies will have to include CR technology and cloud framework in order to survive. Due to this reason, they need more spectrum and more space to work efficiently with less delay and more throughput.

*Corresponding author: rafiq_mufti@ciitvehari.edu.pk

Table 1: Key notations.

Notation	Definition
N	Total number of CPEs
N_Q	Mean queue length
K	Number of available channels for communication
λ	Poisson arrival rate
μ	Exponential service rate
w_t	Mean waiting time
σ	Additional waiting time for security of users
β	Security server waiting time
γ	Admission control waiting time

The proposed framework may be applied to other wireless emerging technologies, such as 5G and 6G, whether centralized or ad-hoc based on or integrated with CRN concept. If the future technologies are centralized, then the same framework can be utilized. On the other hand, if they are ad-hoc, then the steps for registration with the BS after last phase will be ignored. Almost all the future wireless technologies will have to include CR technology and cloud framework in order to survive. Due to this reason, they need more spectrum and more space to work efficiently with less delay and more throughput.

A CR has the ability to automatically detect its surrounding radio frequency (RF), analyze it, and then dynamically adapts its operating parameters according to the needs of the network to fulfill user requirements [11]. If a channel occupied by CR user is needed to be utilized by a licensed user, the CR user leaves that channel and finds another available spectrum band to continue its remaining transmission. A CR can also remain in the same band by changing its modulation scheme or transmission power level that can prevent interference [12]. A CR has two main characteristics [6, 13]: (i) cognitive capability, (ii) reconfigurability. The former means that a CR has the capability to be aware of any changes made in its surrounding radio environment to detect the available free channels for use. The latter means that a CR has the ability to transform itself according to the new free radio spectrum by programming itself dynamically. In terms of functionality, a cognitive radio performs the four basic functions, i.e., (i) spectrum sensing, (ii) spectrum decision, (iii) spectrum sharing and (iv) spectrum mobility [14]. As part of the spectrum sensing, a CR user detects the unoccupied licensed channels as well as the presence of any licensed user. The CR user then selects the most appropriate channel among the available channels. This step is termed as spectrum decision. A CR user can also share the chosen spectrum with other CR users, i.e., spectrum sharing. Lastly, the CR user leaves the licensed channel whenever the licensed user reappears on it and continues its communication on another available vacant channel, i.e., the spectrum mobility.

IEEE standardizes the usage and implementation of CR in the form of IEEE 802.22 WRAN (Wireless Regional Area Network). IEEE 802.22 WRAN defines a master/slave architecture in which a base station (BS) acts as the master node and a number of CPEs act as the slave nodes. One WRAN cell consists of one BS and up to 512 fixed or portable CPEs of varying QoS (Quality of Service) requirements. There are two types of CPEs in the cell, i.e., (i) PUs which are licensed users and have more priority as compared to the other users and (ii) SUs (CPEs) that are unlicensed and agree to communicate opportunistically and thus have less priority as compared to the PUs. As a master node, the BS performs the authorization process for the CPEs. The BS periodically keeps on sensing the spectrum and broadcasts the spectrum usage on an operating channel. The usage of frequency spectrum by the PU is straight forward. However, an opportunistic algorithm is required for the communication of the CPE. Whenever a CPE is powered on, it scans the frequency spectrum and looks for the free channel that can be used for the communication. If a CPE finds a free channel, then it requests the BS for the allocation of such band. After performing the authorization and availability checks, the BS allocates that band to the requesting CPE and transmits the necessary information about the allocated channel and operating parameters to the SU. The CPE sends back the spectrum usage report to the BS as the acknowledgement [15].

The initial idea of cloud computing was perceived as “intergalactic computer network” by Licklider in 1963 [16]. He described the idea of a global network that allowed people to access data and execute their code anywhere. The dream came true after a long time when salesforce delivered services to an enterprise via a website in 1999 [17]. Licklider’s dream was actually realized when large companies like Microsoft and Amazon started to propose personal computing and enterprise services. Cloud computing now offers many benefits to the companies and individuals [18]. Its basic use is to store and compute data and information remotely. Currently, such storages are provided by most of the main online cloud service providers such as Dropbox, Amazon Cloud Drive, etc. The users of Apple may connect themselves to iCloud for gaining access to the local storage capacity. Some of the similar services are offered by Google Drive and Microsoft OneDrive.

Cloud computing consists of three forms: (i) public, (ii) private and (iii) hybrid cloud. In the public cloud, the general public can access the cloud in the pay-as-you-go way and in private cloud, the infrastructure is offered to some specific organization or business. The combination of both public and private clouds is referred to as a hybrid cloud. Some of the rapidly growing data centers to provide cloud computing services in various locations of the world are: Microsoft, Yahoo, IBM, Google, etc. A variety of applications are hosted by these data centers on a hardware platform and these applications are either time sensitive or require guaranteed security. The applications may include distributed databases, internet banking and web-based applications. Considering the flexibility and the scalability of

the could platform, this work presents a model that places the security and admission control servers in the private cloud platform for secure registration process of the CPEs.

2. Methodology

This section reviews the threats posed to the CRN. A security threat is a potential danger that can be caused by any subject, internal or external, to the system. An attacker can translate the threat into an attack by exploiting some of the vulnerabilities of the system. These vulnerabilities can be mitigated by applying some security controls in the system. For the reliable functioning of the system, it becomes very critical to identify the potential attacks and vulnerabilities and then apply the appropriate security controls in the system [19]. The attacks faced by CRN can be classified into various categories. In this paper, we discuss the attacks that are launched by exploiting the communication protocol layers, i.e., physical layer, link layer, network layer and transport layer. The solutions to alleviate attacks should follow the FCC requirement, which states that "no modification to the incumbent system should be required to accommodate the opportunistic use of spectrum by SUs" [20, 21]. So with this condition, the solutions to counter the attacks can only be suggested to the SU system, not to the PU system. Some of the attacks related to the four layers are discussed in the following subsections.

2.1 Physical Layer Attacks

2.1.1 Jamming

In this attack, the attacker continuously sends the illegitimate signals on the spectrum and thus depriving the legitimate SUs to sense the available idle channel on the network, and thus leading to a sort of denial of service attack [22]. Moreover, the channel dedicated for exchanging sensing information among CRs can also be jammed by the jamming attacks.

2.1.2 Objective Function Attack

A CR is a smart radio that can learn from the history and the external environment, and can dynamically adjust its operating parameters like frequency, modulation, coding rate, encryption type, etc. [21]. These parameters are computed by the objective function that resides in the component known as the cognitive engine. This cognitive engine has been the target of many attackers. At the time when the cognitive engine is performing its function, the attacker can trick the victim SU to pick the weak parameters that may be easy to eavesdrop or hack the channel [22].

2.1.3 Primary User Emulation (PUE) Attack

While using the licensed spectrum band, the SU has to leave the channel when the owner of the channel, i.e., PU returns back. On the other hand, if an SU detects another SU then the spectrum is shared between these two users using some spectrum sharing techniques. In PUE attack, a malicious SU pretends to be an emulating PU to get the access of the channel without allowing to share it among the other legitimate SUs [22]. In this way, the malicious user can get full access to the whole spectrum. This attack is further subdivided into two categories: (i) malicious PUE and (ii) selfish PUE. In malicious PUE attack, the objective of the attacker is to raise its share to use the spectrum and it can also make a dedicated link with another attacker for communication, hence the channel is shared by two attackers; whereas in selfish PUE attack, the goal of the attacker is to prevent the legitimate SUs for the positively use the spectrum.

A selfish PUE attack on the other hand occupies the target attacked channel selfishly for data transmission and stops interference from the PU, thus degrading the performance of CRN.

2.2 Link Layer Attacks

2.2.1 Asynchronous Sensing Attack

SUs in the CR can use synchronous and asynchronous sensing. A selfish SU can use asynchronous sensing when other SUs are using the synchronous sensing, thus forcing other SUs to postpone their transmission. If this attack is combined with the PUE attack, then legitimate SUs can falsely assume that a PU is present there, and thus stop using that channel [23].

2.2.2 Control Channel Saturation DoS Attack

If a number of CR users want to share the channel, they communicate at the same time creating collisions due to the bottleneck at the channel. In this situation, the common control channel (CCC) becomes saturated [24]. The attacker can make unfair use of such situation by sending forged messages on CCC to saturate it, hence deteriorating the system performance.

2.2.3 Spectrum Sensing Data Falsification Attack

This attack is based on the fact that incorrect spectrum sensing reports are sent by the attacker to its neighbors. As a result, the receiver makes wrong decisions about the status of channels [25, 26]. This attack can affect both the centralized and the distributed CRNs. There is a variety of attacks in which a SU can maliciously or accidentally send false data to the other users, i.e., fabrication attack, on-off attack, resource hungry attack, false alarm attack, and Sybil based attacks [23].

2.3 Network Layer Attacks

2.3.1 Sinkhole Attack

A malicious user can use this attack to divert all the network traffic towards him. The attacker introduces itself as the finest route to send packets to the destination, so misguiding the neighboring nodes to forward the packets. Sometimes the attacker captures the packets to modify or discard them [27].

Table 2: Summary of the CRN attacks and their countermeasures.

Type	Attack	Countermeasure
Physical Layer Attacks	Jamming Attack	Using statistical or machine learning based model to differentiate between normal and abnormal noise levels on the channel
		Comparing Packet Delivery Ratio with the received signal strength to identify the abnormal level of noise caused by the jamming attacks
	Objective Function Attack	Restricting the changes in all updatable radio parameters either by defining threshold values or using some statistical or machine learning based approaches
	Primary User Emulation (PUE) Attack	Distance difference based approaches
		Localization of the primary user based approaches
Link Layer Attacks	Asynchronous Sensing Attack	Selfish behavior mitigation techniques may be used
	Spectrum Sensing Data Falsification Attack	Threshold based decision fusion test, weighted sequential ratio test or statistical or machine learning based approaches
	Control Channel Saturation DoS Attack	Trust based detection mechanisms may be used
Network Layer Attacks	Sinkhole Attack	Rule, anomaly or statistical based tests, using encryption based authentication of the routing packets, geographic routing protocols
	HELLO Flood Attack	Rate limiting based approaches, stateless protocol design
Transport Layer Attacks	Lion Attack	Rate limiting based approaches, using other available suitable transport protocols

2.3.2 HELLO Flood Attack

The malicious messages are broadcasted by the attacker to all users in the system with high power, so misleading them to consider this node as their neighbour. If any node uses this neighbour to send its packets to the destination node, then these packets may be lost because the forwarding node is the attacker [27].

2.4 Transport Layer Attacks

2.4.1 Lion Attack

In this attack, PUE attack is employed to disrupt the transmission control protocol (TCP). Due to this, the SUs have to perform frequent spectrum handoffs, for which the TCP may not be aware of. The logical connections will be created frequently without receiving acknowledgments, producing timeouts and doubling retransmission timers, resulting in the delays and packet loss. More detailed countermeasures against these attacks can be found elsewhere [28, 29]. Summary of the CRN attacks and their countermeasures is given in Table 2.

3. Proposed Model

The proposed work is basically the extension of our previous work, which is based on the performance analysis of registration process [30, 31] for WRAN with the addition of supporting cloud platform that provides security benefits. Our earlier work was based upon continuous-time Markov chain [30] and discrete-time Markov chain [31]. In this study, it is assumed that before actual registration, the CPEs will have to pass through the process given on cloud.

The cloud shown in Fig. 1 has three servers with some CRs, which are used for sensing the idle channels and their reports will be stored in the buffer server. The security server has the repository of techniques to mitigate PUE attacks [32, 33]. Its main task is to guarantee the reliability of PUs to prevent the PUE attack. As both users, i.e., incumbents and CPEs have to pass through the security server; it checks the authenticity of SUs behaving themselves as PUs by not applying any single algorithm for their authentication but applying multiple PUE attacks mitigating techniques until SUs are identified as trustworthy SUs. If a SU is malicious then the security server will reject it as shown in Fig. 2.

The admission control is also incorporated to check the reliability of CPEs. If data rate, geo-location and payment offered are not according to the system demand, then the particular CPE may be rejected by the admission control server. In this work, a queuing system shown in Fig. 2 is also employed to provide security at two levels, i.e., at SU (CPE) level and at PU (incumbent) level.

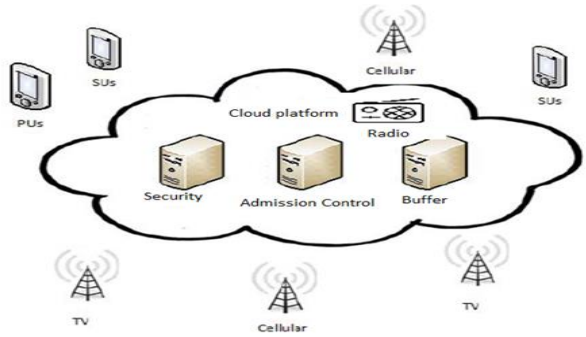

Fig. 1: Cloud platform with security and admission control servers for CRN.

The admission control is also incorporated to check the reliability of CPEs. If data rate, geo-location and payment offered are not according to the system demand, then the particular CPE may be rejected by the admission control server. In this work, a queuing system shown in Fig. 2 is also employed to provide security at two levels, i.e., at SU (CPE) level and at PU (incumbent) level.

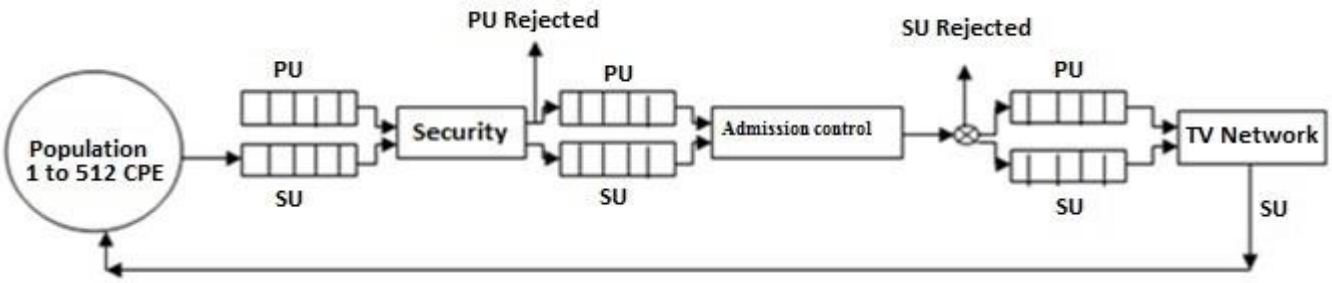

Fig. 2: Queuing model.

As shown in Fig. 1, two networks called Cellular and TV are taken into account. The base stations in both networks report the status of idle channels to the cloud platform. Here, we are concerned with the TV network because it is the primary network in the WRAN. Whenever a CPE is looking for an idle channel, it will consult TV BS and the cloud. Now the registration process with the BS of WRAN starts. However, during the registration process, the CPE validates its configuration according to the BS requirements. If validation is successful, then the particular CPE will be permitted to enter into the WRAN. After entering the network, the BS acquires the list of available channels, based on the current location of the CPE by contacting database service. If the database service is available, then a free channel is given to CPE for continuing its communication. However, if database service is not available due to the presence of incumbent either on N or N±1 channel, then BS will decline to register that particular CPE.

After accessing the channel, it will continue its communication, with the condition, that PU is not using the channel. In case, if PU appears, then CPE will have to perform spectrum handoff to continue its remaining transmission.

A queue is formed when more than one user attempt to use the same channel. The queuing model used in this work is shown in Fig. 2.

The system contains maximum of 512 CPEs. To get access to the channels, the CPEs and incumbents have to pass through the cloud; where first of all, the security server checks the activities of the incumbents and CPEs. In case of a malicious user, its request is rejected. On the other hand, if an incumbent is trustworthy, then it is allowed to enter into the system and its request is forwarded to the next server. The next phase is the admission control, where the CPEs and incumbents are admitted in the system to get access to the free channels. Here, the CPEs can be rejected if they fail to fulfill the desired limits of parameters requirements as discussed earlier. Since, the status and the list of available channels is stored in buffer server; therefore, the last phase is related to the allocation of available channels as long as the incumbents are not actively transmitting. If channels are successfully allocated to CPEs then they will get register with the BS by following the native registration process [30]. In short, after synchronizing with the free channel, the CPE will first get the upstream and downstream parameters from superframe. Then initial ranging process will be performed [11]. After the successful initial ranging, CPE transmits its basic capabilities to the BS. Most of the basic capabilities are already confirmed by admission control server except EIRP. If all the basic capabilities are according to the preferred requirements, then CPE will get registered with the BS. In case, incumbents return to their native channels, the CPEs must leave the channels and return to the front of the queue. They will continue their transmission on another idle channel, if it is available.

The derivation of mean queue length is taken from our previous study [30] and the closed-form expression is as follows:

$$N_Q = \Phi\, \zeta^{-1} \tag{1}$$

where

$$\Phi = \sum_{n=0}^{K} n\binom{N}{n}\left(\frac{\lambda}{\mu}\right)^n + \sum_{n=K+1}^{N} n\binom{N-K}{n-K}\binom{N}{K}\frac{(n-K)!}{K^{(n-K)}}\left(\frac{\lambda}{\mu}\right)^n + \sum_{n=K}^{N-1} n\binom{N-K}{n-K+1}\binom{N}{K}\frac{(n-K)!\ \lambda}{\alpha K^{(n-K)}}\left(\frac{\lambda}{\mu}\right)^n$$

$$\zeta^{-1} = \frac{1}{\Omega_1(N,K,n,\lambda,\mu) + \Omega_2(N,K,n,\lambda,\mu) + \Omega_3(N,K,n,\lambda,\mu,\alpha)}$$

where

$$\Omega_1(N,K,n,\lambda,\mu) = \sum_{n=0}^{K}\binom{N}{n}\left(\frac{\lambda}{\mu}\right)^n$$

$$\Omega_2(N,K,n,\lambda,\mu) = \sum_{n=K+1}^{N}\binom{N-K}{n-K}\binom{N}{K}\frac{(n-K)!}{K^{(n-K)}}\left(\frac{\lambda}{\mu}\right)^n$$

$$\Omega_3(N,K,n,\lambda,\mu,\alpha) = \sum_{n=K}^{N-1}\binom{N-K}{n-K+1}\binom{N}{K}\frac{(n-K)!\ \lambda}{\alpha K^{(n-K)}}\left(\frac{\lambda}{\mu}\right)^n$$

Mean waiting time is given as:

$$w_t = \frac{N_Q}{\lambda} \tag{2}$$

where λ is the mean arrival rate with poisson arrival process.

4. Experimentation

In this section, we used two new terms: (i) security on and (ii) security off. Security on means the security server checks for the validity of CPEs and incumbents, whereas the security off means functionality of the security server is ignored.

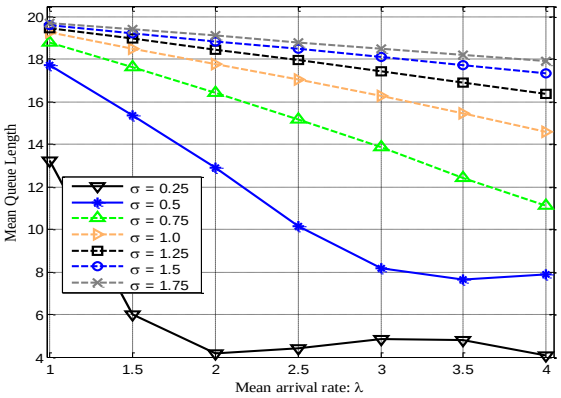

Fig. 3: Mean queue length versus mean arrival rate with the security on for different values of σ.

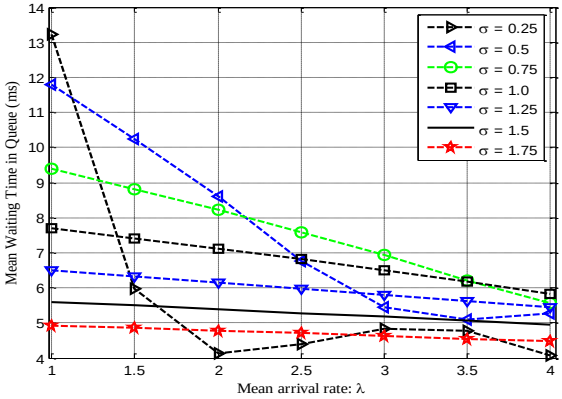

Fig. 5: Mean waiting time in queue versus arrival rate with the security on for different values of σ.

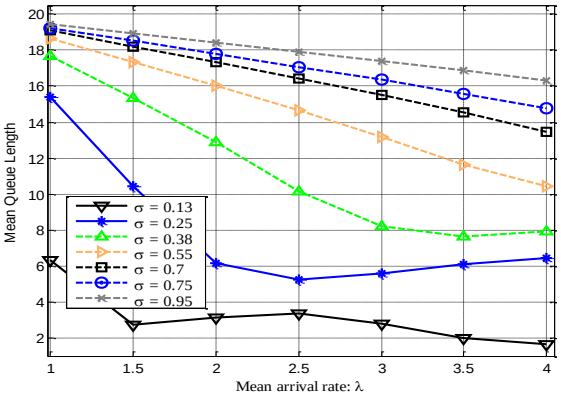

Fig. 4: Mean queue length versus mean arrival rate with the security off for different values of σ.

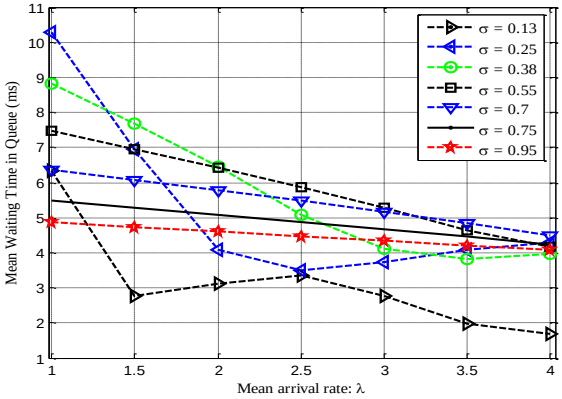

Fig. 6: Mean waiting time in queue versus arrival rate with the security off for different values of σ.

Fig. 3 shows the mean arrival rate vs. mean queue length for different values of σ with security on, where $\sigma = \beta + \gamma$ is additional waiting time spent on the security of primary and secondary users, β and γ represent the waiting times used in the security server and admission control, respectively. The same information is also represented by Fig. 4 with security being turned off, i.e., $\beta = 0 \Rightarrow \sigma = \gamma$. From these results, it is clear that as the mean queue length decreases, the mean arrival rate increases at different values of σ. However, the decrement in mean queue length is less with respect to the security off as compared to the security on. It can also be noted that σ increases with an increase in the mean queue length. Here the mean queue length represents the number of active CPEs, which are high when the security is on (Fig. 3) as compared to the security off (Fig. 4). This implies that the system performs well when security is turned on.

In Fig. 5 and Fig. 6, the mean arrival rate is plotted against mean waiting time for different values of σ. The security is kept on in Fig. 5, whereas in Fig. 6, the security is turned off, i.e., only γ is included and β is kept off. Using Fig. 5, for $\sigma = 0.25$ and $\lambda = 1$, the mean waiting time is more than13 *ms*. When $\lambda = 1.5$, the mean waiting time abruptly drops to 6 *ms*. It further reduces to 4 *ms* when λ approaches to 2. Again, when λ changes from 2 to 4, the mean waiting time lies between 4 to 5 *ms*. For $\sigma = 0.75$ and $\lambda = 1$, the mean waiting time is 9.2 *ms*. When λ moves from 1 to 1.5, the mean waiting time reduces from 9.2 *ms* to 8.9 *ms*. Similarly, when λ either moves from 2 to 2.5 or from 3 to 3.5, the mean waiting time reduces from 8.3 *ms* to 7.7 *ms* or from 7 *ms* to 6.2 *ms* respectively. Now using Fig. 6, for $\sigma = 0.25$ and $\lambda = 1$, the mean waiting time is 10.3 *ms*. When λ increases by 100%, i.e., $\lambda = 2$, the mean waiting time reduces by 61%, i.e., 4 *ms*. It further reduces with increasing λ. Similar is the case for other values of σ. It can be noted that in both cases, the mean waiting time decreases with increasing the arrival rate and its value is larger at any particular arrival rate when the security is on. It means more CPEs become active for association with IEEE 802.22 network.

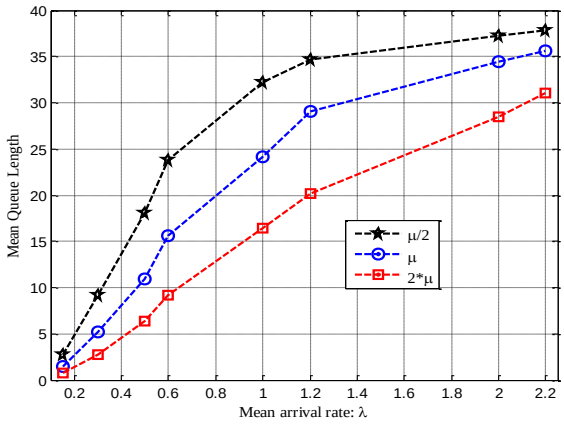

Fig. 7: Mean queue length versus mean arrival rate with the security on at different values of μ.

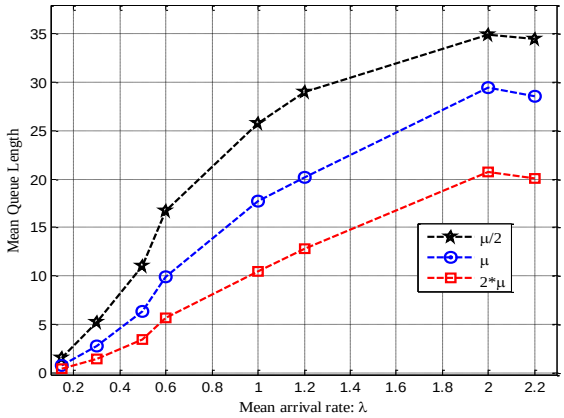

Fig. 8: Mean queue length versus mean arrival rate with the security off at different values of μ.

Fig. 7 and Fig. 8 show the mean queue length against the mean arrival rate at different service rates with security on and off, respectively. From Fig. 7, we can observe that at some particular service rate μ = 1.0, and λ = 0.5, the mean queue length is 11. When λ increases from 0.5 to 1, the mean queue length increases from 11 to 24. Moreover, when λ moves from 1 to 2, the mean queue length moves from 24 to 34. Similar situation can be seen at other values of λ. This shows that at any particular service rate, the mean queue length increases with increasing λ. Again at λ = 1, when service rate is decreased by 100%, i.e., μ/2, the mean queue length is increased by 37%. Similarly, when the service rate is increased by 100%, i.e., 2μ, the mean queue length is decreased by 29%. This shows that at any particular arrival rate, the mean queue length increases by decreasing the service rate and vice versa. Similar results are observed from Fig. 8, when security is off. From these results, it can be observed that at any service rate and at any arrival rate, the mean queue length is more significant when security is on as compared to security off. This implies that more CPEs have to wait for the registration process with the BS, which confirms the good performance of the system when security is kept on.

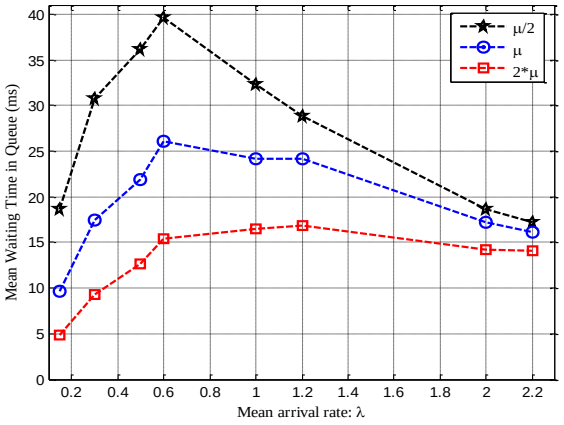

Fig. 9: Mean waiting time in queue versus arrival rate with the security on at different values of μ.

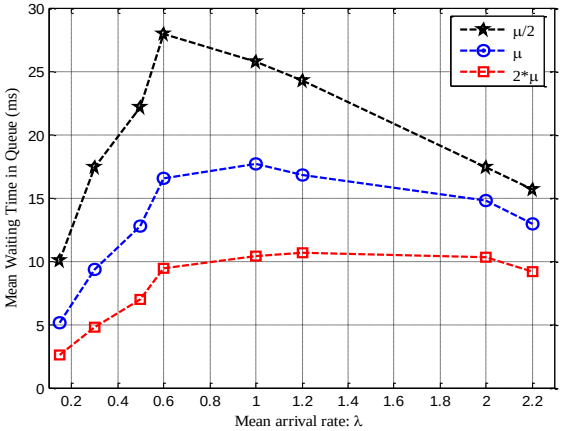

Fig. 10: Mean waiting time in queue versus arrival rate with the security off at different values of μ.

Fig. 9 and Fig. 10 depict the behavior of the mean waiting time in the queue over the mean arrival rate with respect to different service rates. Using Fig. 9, for λ = 0.5 and μ = 1.0, the mean waiting time is 22 ms. It further increases up to λ = μ and then it starts reducing with increasing λ. When μ is increased by 100%, i.e., μ=2.0 and λ = 1.0, the mean waiting time reduces from 24.5 ms to 16.5 ms. Similarly, when μ is decreased by 100%, i.e., μ = 0.5, the mean waiting time increases from 24.5 ms to 32.5 ms at the same value of λ. In Fig. 10, when λ = 1.0 and μ = 1, the mean waiting time is nearly 10.4 ms, which is about 36% less, when the security in kept on. Again, when μ decreases from 1.0 to 0.5, the mean waiting time increases from 10.4 ms to 18 ms. It means that in both cases, the mean waiting time in queue decreases with increasing the service rate and vice versa at a particular value of arrival rate. However, mean waiting time in queue is more in case of security on because of the primary user using the channel and the CPE has to wait until the channel becomes free. On the other hand, when security is off, the mean waiting time is small because the CPE may mistakenly access the channel through the malicious user, but actually the particular channel is not free. As a result, the CPE comes again in the queue.

5. Conclusions

This paper addressed the issue of secure registration process in wireless cognitive radio networks by presenting an analytical model and then analyzing the performance of the registration process with and without the security and admission control servers in the cloud platform. The parameters of mean queue length and the mean waiting time are investigated to evaluate the performance of the system by keeping the security on and off. We have shown that the performance parameters of mean queue length and the mean waiting time are largely affected by the service rate and arrival rate parameters. The mean queue length is larger at any service rate or at any arrival rate when security is on as compared to when security is off. This confirms that more CPEs have to wait for the association process with the BS. Moreover, the mean waiting time decreases with increasing the arrival rate and is more at any particular arrival rate when security is on. This proves that the performance of the system is best when security is kept on. However, if security is off, the mean waiting time becomes shorter; but in this case, the system is open for security threats which will eventually degrade the system performance.

This is the generic model that evaluated the overhead and efficiency of the security and admission control servers in the CRN. In future, performance of more specific security controls for CRN may be evaluated by using the proposed model.

References

[1] J. Mitola, "Cognitive Radio: An Integrated Agent Architecture for Software Defined Radio", PhD Thesis, Royal Institute of Technology, Sweden, 2000.

[2] X. Liu, K. Zheng, L. Fu, X.Y. Liu, X. Wang and G. Dai, "Energy efficiency of secure cognitive radio networks with cooperative spectrum sharing", IEEE Trans. Mob. Comput., vol. 18, no. 2, pp.305-318, 2019.

[3] F.Z. El Bahi, H. Ghennioui and M. Zouak, "Spectrum sensing technique of OFDM signal under noise uncertainty based on Mean Ambiguity Function for Cognitive Radio", Phys. Commun., vol. 33, pp.142-150, 2019.

[4] D. Capriglione, G. Cerro, L. Ferrigno and G. Miele, "Performance analysis of a two-stage spectrum sensing scheme for dynamic spectrum access in TV bands", Meas., vol. 135, pp.661-671, 2019.

[5] B.S. Awoyemi, B.T. Maharaj and A.S. Alfa, "Resource allocation in heterogeneous buffered cognitive radio networks", Wirel. Commun. Mob. Comput., vol. 1, pp. 1-12, 2017.

[6] Federal Communications Commission, Notice of proposed rule making and order. ET Docket no. 03-222, 2003.

[7] D.A. Fernandes, L.F. Soares, J.V. Gomes, M.M. Freire and P.R. Inácio, "Security issues in cloud environments: a survey", Int. J. Inf. Secur., vol.13, no. 2, pp.113-170, 2014.

[8] P. Mell and T. Grance, "The NIST definition of cloud computing", Special Publication 800-145, National Institute of Standards and Technology, U.S. Department Commerce, 2011.

[9] J. Köhler, K. Jünemann and H. Hartenstein, "Confidential database-as-a-service approaches: taxonomy and survey", J. Cloud Comput., vol. 4, no. 1, p.1, 2015.

[10] H. Patel, D. Patel, J. Chaudhari, S. Patel and K. Prajapati, "Tradeoffs between performance and security of cryptographic primitives used in storage as a service for cloud computing", Proc. CUBE Int. Inf. Tech. Conf., pp. 557-560, ACM. 2012.

[11] H. Afzal, I. Awan, M.R. Mufti and R.E. Sheriff, "Modeling of initial contention window size for successful initial ranging process in IEEE 802.22 WRAN cell", Simul. Model. Pract. Theory, vol. 51, pp.135-148, 2015.

[12] M.R. Mufti, H. Afzal, I. Awan and A. Cullen, "A framework for dynamic selection of backoff stages during initial ranging process in wireless networks", J. Syst. Softw., vol. 133, pp.17-27, 2017.

[13] H. Afzal, M.R. Mufti, K.T. Ahmed, S. Ajmal and M. Yousaf, "Performance Analysis of Hybrid Spectrum Sharing in Cognitive Radio Based Wireless Regional Area Network", The Nucleus, vol. 57, no. 1, pp.27-32, 2020.

[14] F. Awin, E. Abdel-Raheem and K. Tepe, "Blind Spectrum Sensing Approaches for Interweaved Cognitive Radio System: A Tutorial and Short Course", IEEE Commun. Surv. Tutor., vol. 21, no. 1, pp.238-259, 2018.

[15] H. Afzal, I. Awan, M.R. Mufti and R.E. Sheriff, "Performance analysis of contending customer equipment in wireless networks", J. Syst. Softw., vol. 117, pp.357-365, 2016.

[16] J.C.R. Licklider, "Memorandum for Members and Affiliates of the Intergalactic Computer Network", December 11, 2001. https://www.kurzweilai.net/memorandum-for-members-and-affiliates-of-the-intergalactic-computer-network

[17] N.N. Rojas, "CRM Review", http://erpsoftware360.com/salesforce.htm

[18] D. Catteddu, "Cloud Computing: benefits, risks and recommendations for information security", Proc. Web Appl. Secur., p. 17, Springer, Berlin, Heidelberg, 2010.

[19] T. Zeb, M. Yousaf, H. Afzal and M.R. Mufti, "A Quantitative Security Metric Model for Security Controls: Secure Virtual Machine Migration Protocol as Target of Assessment", IEEE China Commun. vol. 15, vol. 8, pp. 126-140, 2018.

[20] R. Chen and J.M. Park, "Ensuring trustworthy spectrum sensing in cognitive radio networks", 1st IEEE Workshop on Networking Tech. Softw. Defined Radio Netw., pp. 110-119, 2006.

[21] Q. Mahmoud, "Cognitive networks: towards self-aware networks", John Wiley & Sons, 2007.

[22] Z.M. Fadlullah, H. Nishiyama, N. Kato and M.M. Fouda, "Intrusion Detection System (IDS) for Combating Attacks Against Cognitive Radio Networks", IEEE Netw. Mag., vol. 27, no. 3, pp. 51-56, 2013.

[23] M.R. Manesh and N. Kaabouch, "Security Threats and Countermeasures of MAC Layer in Cognitive Radio Networks", Ad Hoc Netw., vol. 70, pp. 85-102, 2018.

[24] K. Bian and J.M. Park, "MAC-layer misbehaviors in multi-hop cognitive radio networks", Proc. US-Korea Conf. on Sci. Technol. Entrep., pp. 228-248, 2006.

[25] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures", Ad hoc Netw., vol. 1, no. 2-3, pp.293-315, 2003.

[26] C. N. Mathur and K.P. Subbalakshmi, "Security issues in cognitive radio networks", Cogn. Netw., vol. 25, pp.272-290, 2007.

[27] R. K. Sharma and D.B. Rawat, "Advances on Security Threats and Countermeasures for Cognitive Radio Networks: A Survey", IEEE Commun. Surv. Tutor., vol. 17, no.2, pp. 1023-1043, 2015.

[28] W. El-Hajj, H. Safa and M. Guizani, "Survey of security issues in cognitive radio networks", J. Internet Technol., vol. 12, no. 2, pp.181-198, 2011.

[29] L.I. Jianwu, F. Zebing, F. Zhiyong and Z. Ping, "A survey of security issues in cognitive radio networks", IEEE China Commun., vol. 12, no. 3, pp.132-150, 2015.

[30] H. Afzal, I. Awan, M.R. Mufti and R.E. Sheriff, "Modeling and analysis of customer premise equipments registration process in IEEE 802.22 WRAN cell", J. Syst. Softw.,vol. 98, pp.107-116, 2014.

[31] H. Afzal, M.R. Mufti, I. Awan and M. Yousaf, "Performance Analysis of Radio Spectrum for Cognitive Radio Wireless Networks using Discrete Time Markov Chain", J. Syst. Softw., vol. 151, pp. 1-7, 2019.

[32] N. Nguyen-Thanh, P. Ciblat, A.T. Pham and V.T Nguyen, “Surveillance strategies against primary user emulation attack in cognitive radio networks,” IEEE Trans. Wirel. Commun., vol. 14, no. 9, pp. 4981–4993, 2015.

[33] E.C. Muñoz, E. Rodriguez-Colina, L.F. Pedraza and I.P. Paez, "Detection of dynamic location primary user emulation on mobile cognitive radio networks using USRP", EURASIP J. Wirel. Commun. Netw., vol. 2020, no. 1, pp. 1-19, 2020.