Available online at www.sciencedirect.com

ScienceDirect

Electronic Notes in Theoretical Computer Science

Electronic Notes in Theoretical Computer Science 340 (2018) 123–135

www.elsevier.com/locate/entcs

# Impact of Scalability on the Performance of Secured Cognitive Radio Networks

Ejike E Chuku[1] Demetres D Kouvatsos[2]

*School of Electrical Engineering and Computer Science*
*University of Bradford*
*Bradford, United Kingdom*

**Abstract**

A Cognitive Radio Network (CRN) allows Secondary Users (SUs) to sense licensed spectrum in order to transmit if an idle band is detected. Therefore it is imperative that SUs swiftly utilize the spectrum band as soon as it becomes available. This paper proposes a new Generalized Stochastic Petri Net (GSPN) model with intrusion detection to study the impact of scalability on a single node of the CRN towards an effective optimization of an idle band by SUs in cloud computing platforms. In this context, the instant the band becomes idle and there are SU requests waiting for encryption and transmission, additional resources are dynamically released in order to largely utilize the spectrum space before the reappearance of Primary Users (PUs). These extra resources make the same service provision, such as encryption and intrusion detection, as the initial resources. Typical numerical simulation experiments are carried out with and without scalability, based on the application of Mobius Petri Net package, in order to determine the impact of scalability towards the enhancement of nodal CRN sensing, security and performance trade-offs. These results indicate the sustained performance of SUs at the CRN node due to scalability of resources during heavy traffic periods.

*Keywords:* Cognitive Radio (CR); Encryption; Sensing; Secondary User (SU); Primary User(PU).

## 1 Introduction

The use of CRN has become necessary due to underutilization of licensed spectrum bands. Study shows that about 80% of allocated spectrum are not being utilized in a number of locations [1] [2]. Regulatory bodies have approved the use of CR to allow SUs to access the idle spectrum band without interfering with the PU signal. The main bands of interest for the CR are VHF and UHF due to their excellent propagation [3]. The licenced owners of these bands are television, mobile and satellite operators. Signal from these operators can be very low and require high detection rate. Sensing is therefore required to identify an idle spectrum band. Sensing in this context is probing through spectrum band to detect when it is idle [4]. It is

[1] Email: E.E.Chuku@bradford.ac.uk

[2] Email: D.Kouvatsos@braford.ac.uk

https://doi.org/10.1016/j.entcs.2018.09.009

1571-0661/

carried out periodically and only when there are requests to transmit. If an idle band is detected, SU will utilize the space for the transmission of its requests based on the Service Level Agreement (SLA). CRN sensors are powered by battery [5]. A combination of sleeping and censoring is assumed as in [6] in order to conserve energy. Sleeping in this context implies that the radio device switches off its power when not sensing to save power. Censoring in contrast denotes sensing and deciding the status of the band.

It was stated in [7] that PUs may not allow SUs to access their band without benefit. Though idle band may be identified, however, SUs may continue to experience denied access to the spectrum due to PU activities and attacks on CRN, leading to drop in SU throughput. To enhance the throughput and maintain optimal security, [8] [9] proposed sensing, security and throughput trade-off. The aim was to determine the sensing time that maximizes the combined metric for sensing, security and performance. Unfortunately, the above studies only considered static resources. In this case, though the idle band may be identified, the available static SU resources may be inadequate to fully utilize the idle spectrum band before the reappearance of PU.

This work proposes scalability as an approach to fully utilize the idle spectrum band. Scalability in this context is the ability of the CRN to dynamically add or remove resources according to the service requests [8] [10] . Very often, PU activities on spectrum band may lead to delay in transmission of SU requests. Security incidents also denies SU the opportunity to utilize the idle spectrum band. These situations result to build-up of SU requests. To boost transmission, if an idle band is detected, considering that there is a build-up of SU requests, additional resources are automatically released in order to largely utilize the idle band and transmit the waiting SU requests before the reappearance of PU. This way, much of the waiting SU requests are served within the given idle time of the spectrum. The main contributions of this paper are:

1) To produce an architectural design of CRN that is dynamic and can guarantee optimal performance upon sudden surge in SU service requests.

2) To maintain high spectrum utilization while guaranteeing optimum security.

The rest of the paper is organised as follows. In section 2, the related works was introduced. Section 3 briefly discussed cloud and its advantages as a platform for CRN. Section 4 considered the threshold for addition or withdrawal of spectrum resources. The next section also presented sensing and different sensing techniques. Section 6 gave a brief details of CRN and PU activity model. Section 7 discussed the bottlenecks to SU spectrum access. A security implementation in the proposed GSPN was introduced in section 8. Section 9 gave details of the simulation package for the implementation of the proposed model. Section 10 gave detailed explanation of the proposed model. Section 11 presents the results and analysis. Section 12 concludes and future work was proposed.

## 2 Related Works

Many researches have been proposed to improve the efficiency of CRN with respect to sensing, security and performance. An experiment was carried out in [11] [12] to improve the performance of service channel by applying scalability approach. The result of the simulation shows an increase in the throughput as a result of this approach. An investigation was carried out in [10] to study scalability and performance of web application on cloud platform. The paper presents novel dynamic scaling architecture with load balancer for routing user requests to web application deployed on a virtual machine. The work demonstrated an increase sustenance of performance upon sudden surge in service demand. A study was undertaken in [9] relating to sensing-throughput trade-off in cognitive radio networks. The focus was to determine the sensing duration to maximize the achievable throughput with sufficient protection of PUs. The analysis of the simulation results shows that there exist an optimal sensing time which yields the highest throughput. An experiment was carried out in [13] to determine the number of sensing nodes required in cooperation in order to improve the accuracy of spectrum detection. The optimal number of cooperating radios needed to minimize detection error probability and maximize throughput in CRN for Wi-Fi networks were derived. One of the studies above considered dynamic infrastructure but with no reference to its use in CRN.The study also did not reflect on security and its performance implications. The rest of studies did not take note of the unpredictable nature of service demand so as to apply scalability as appropriate in order to improve the performance of CRN.

## 3 CRN and CLOUD

Cloud computing is used to define an application delivered as a service through the internet and system software that provide the service [14]. It has been found to provide some advantages to CRN. In [7], cloud computing infrastructure was used to store spectrum opportunities. This way, it was easy for SUs to access and securely use idle spectrum band. Sensors of each of the multiple spectrum reports the idle spectrum space to a geolocation database located in cloud. In this work, scalability feature of cloud computing has been adopted to improve the utilization of idle spectrum and to largely transmit waiting requests. In this case, load balancer is used to add resource when needed or withdraw it when it is no longer required.

### *3.1 Scalability*

This is a feature of cloud computing that allows its resources to be scaled according to service demand [15]. It is difficult to achieve due to unpredictable nature of service demand and unknown nature of service invocations. In order to achieve scalability, [11] introduced two effective scalability approaches: service replication and migration. Service replication is a method of making a replica of service already running on a main server without affecting the operation of the service in progress. This is a way of securing additional resources to bear up against large amount of service requests. Service migration is an approach that places a service to another node when a node cannot provide High Quality of Service (QoS) as a result of problems. In the proposed model, it is a means of transfering service to a new server when there is service degradation resulting from unpredictable service demand. This transfer occur when the average number of requests in waiting is of a certain threshold predetermined based on service level agreement.The flowchart for the scalability of CR resources is as shown in Fig.1. Scalability is highly needed in a long term ON and short term OFF PU activities as stated in section VI. In a

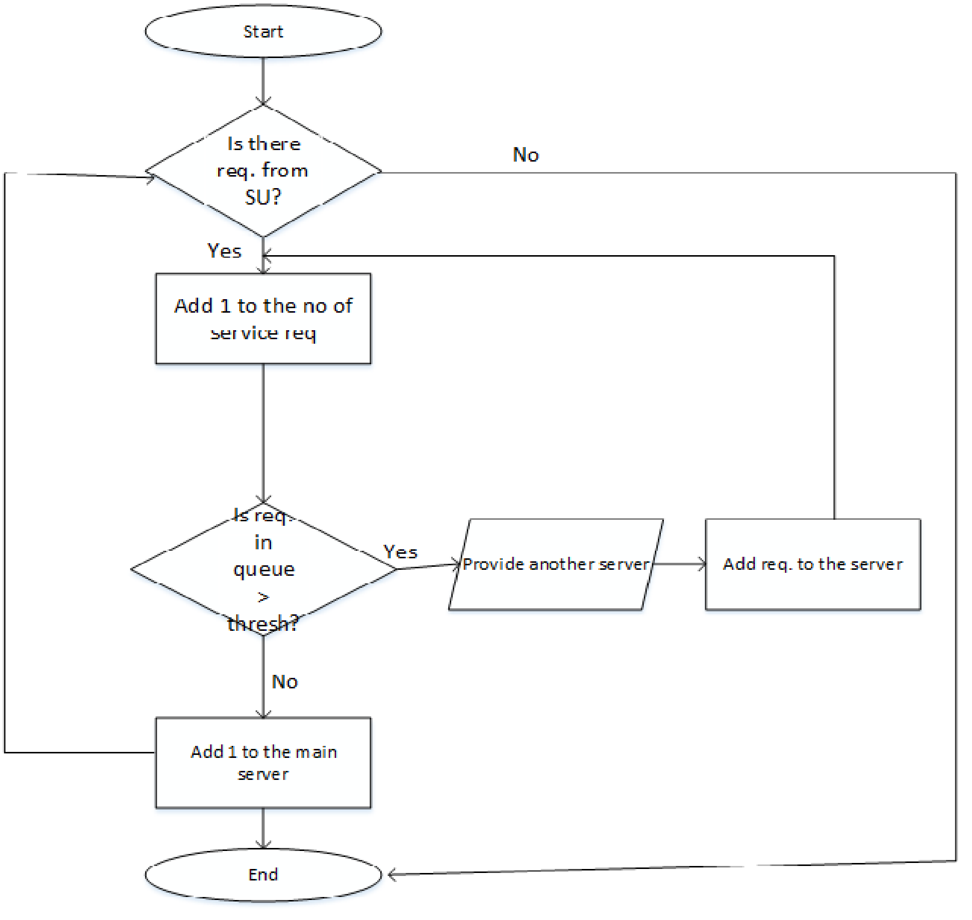


Fig. 1. Flowchart for the scalability of CR resources

long term ON, PUs utilize the band for a long time while SUs are in queue waiting for PUs to vacate. When the band becomes idle, SU will swiftly transmit all its waiting request within the time space by releasing additional resources since the waiting requests may have already exceeded the threshold. However, the utilization of the idle spectrum band depends on the sensing time of CRN sensor. If it takes time to sense, then SUs will be denied the opportunity to transmit all its requests. In this case, the average number of requests required to flag the release of additional resources will remain below the threshold and no extra resources is released.

## 4 Predetermine threshold for performance measurement

In queue network model, length of queue is an important performance metrics to determine the quality of service of a wireless network. It is the average number of requests waiting to be served in queue. This can be expressed as [16].

$$Lq = \rho^2/1 - \rho \tag{1}$$

where $\rho$ is the server utilization given by

$$\rho = \lambda/\mu \tag{2}$$

$\lambda$ is the service request rate and $\mu$ is the service rate. It is assumed that to have a stable system, $\lambda < \mu$. This in words implies that to have stable network without much number of requests in the queue, the arrival rate must be less than the service rate [7] [16]. Queue discipline such as FIFO commonly obtainable in queue network model is complex to represent in GSPN model. In the proposed GSPN model, the average number of requests is represented as the average number of tokens in the place 'Enc queue' as shown in Fig. 3. It is used as a flag to determine when an additional resources is required. If the average number of requests in the place is greater than a predetermined threshold, then additional resources is released, but withdrawn otherwise.

## 5 Sensing

Sensing is carried out in CRN to identify an idle spectrum band. The three most commonly used sensing techniques are energy detection, cyclostationary feature detection and matched filter detection. Each of the detection techniques has its features. For example, in [17], it was stated that cyclostationary feature detection and matched filter detection require a prior information of the PUs in order to operate efficiently. However, in energy detection, no prior knowledge of PU signal is required. Energy detection is the most commonly used due to its low complexity. In energy detection, CRN senses the spectrum and the signal received is divided into N segments. Binary hypothesis testing is applied to determine the energy of the received signal in each of the segments. It is given by [9]

$$T(X) = \frac{1}{N}\sum_{t=1}^{n} |X_n|^2 \tag{3}$$

Where T(x) is the energy of the signal available to SU which can be used to decide the status of the band at time t. To decide the status of the band, this energy is compared with a predetermine threshold. This threshold vary according to noise value and it is given by the following equations [9,18]

$$\varrho = \sigma_w^2 + \frac{Q^-1(P_f a).\sigma_w^2}{\sqrt{N}} \tag{4}$$

Where Q is the complementary cumulative distribution function of standard Gaussian variable, N is the number of samples, $P_f a$ is the probability of false alarm and $\sigma_w^2$ is the noise variance.

# 6 CRN and PU activity model

It has been stated in [7] [19] that PU use the spectrum in on-and-off manner. It occupies the band for a period of time and then vacate. CRN employs spectrum sensing to detect the off period and allow SU to use it. The Fig.2 demonstrates the idle and busy time of the spectrum band. If the PU occupies the spectrum more

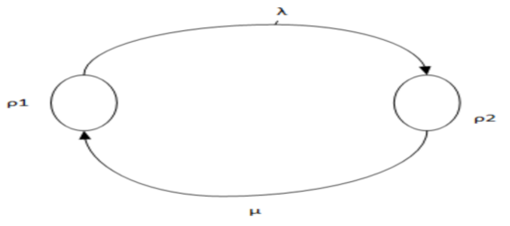


Fig. 2. Transition diagram for the spectrum going from idle to busy state.

frequently, then it will be available for CR users only for a short period of time [19]. Therefore, the throughput of SU is expected to decrease. To increase the SU throughput within this time, the processing capacity of the SU transmitter is increased by releasing additional resources that will carry out parallel encryption and transmission when the number of request in queue is at a certain threshold defined by the network. If the PU occupies the spectrum band more frequently, it will only allow short interleave spectrum band for cognitive use [19]. This will negatively affect the throughput of SU. The SU throughput can be marginally increased within each interleaved spectrum space by automatically releasing additional resources if the number of SU requests is greater than some predetermine threshold. For illustration, the probability of spectrum band being in idle state (interleave space) for cognitive use can be estimated using Kolmogorov equations [20] as shown in (5)-(11)

$$\frac{dp_0}{dt} = -p_0\lambda(t) + p_1\mu(t) \tag{5}$$

$$\frac{dp_1}{dt} = p_1\mu(t) - p_0\lambda \tag{6}$$

where $\frac{dp_i(t)}{dt}$ is the rate of flow of probability to i. Solving the equation using Maxima, the following symbolic equations can be obtained

$$P_0(t) = \frac{\mu}{\lambda+\mu} + \frac{\lambda e^-(\lambda+\mu)t}{\lambda+\mu} \tag{7}$$

$$P_1(t) = \frac{\lambda}{\lambda+\mu} - \frac{\lambda e^-(\lambda+\mu)t}{\lambda+\mu} \tag{8}$$

Where $\mu$ is the rate at which PU reoccupy the band and $\lambda$ is the rate at which the spectrum band becomes idle. The equation (7) shows that the long term availability of the spectrum for cognitive use is defined as

$$\lim_{t\to\infty} P_0(\infty) = \frac{\mu}{\lambda+\mu} \tag{9}$$

and the long term unavailability of the band is

$$\lim_{t\to\infty} P_1(\infty) = \frac{\lambda}{\lambda+\mu} \tag{10}$$

Equation (9) can be further represented as

$$P_0(\infty) = (1 + \frac{\lambda}{\mu})^-1 \tag{11}$$

It simply means that if the rate at which PU accesses the spectrum band decreases, then the probability for the availability of spectrum for cognitive use increases leading to increase SU throughput. This is further illustrated in the numerical experiment in figure 4.

## 7 Bottlenecks to SU spectrum Access

There are some identified factors that impede the use of idle spectrum by CR users:
***PU Activities:*** One of the conditions given by regulatory bodies before SUs are allowed to opportunistically utilize idle spectrum band is to ensure no harmful interference to PU transmission [7]. Therefore, CRN is required to sense the spectrum band and only transmit if an idle band is detected. As stated section IV, longer stay of PU on the band denies SU the opportunities to utilize it. This is mostly common in urban areas where they are concentration of PUs. In rural areas, there is infrequent use of spectrum band by PUs. In this case, the band is mostly available for cognitive use. However, CRN may still need to sense the spectrum to ensure no interference whenever SU wants to access it.
***Errors in Spectrum Detection:*** Errors in spectrum detection such as false alarm can deny SU the chances of using the licenced spectrum. False alarm is detecting the band to be occupied when actually it is idle [4]. It may be caused by attack [21] or multipath fading. In this paper, it is assumed that as the probability of false alarm increases, SUs are denied the opportunity to utilize the spectrum leading to decreased throughput of SU. Using energy detection technique, the probability of false alarm can be expressed as [9]

$$prob(T(x) > \varrho | H_0 true) = \int_{\varrho}^{\infty} fH_0(L(x))dL \tag{12}$$

where T(x) is the energy of the received signal which is compared to a predetermined threshold given in equation (4). $H_0$ denotes noise sample. L(x) is the Likelihood ratio of the data under observation. Based on the above equation, false alarm can be expressed as the probability that the received signal T(x) is greater than the threshold given that PU is not active on the band. If this probability increases, then SUs are denied opportunities to use the spectrum band.
***Malicious Attack and Detection:*** One of the factors affecting SU from sharing spectrum band is malicious attack. Attackers may try to eavesdrop on the content

of requests being transmitted. In [22], a model is proposed that encrypt request and also detect an attack. This model is not tailored to a specific system. The operation of the system is ceased on detection of attack. This causes delay and increase in the number of requests waiting to be transmitted and invariably lead to decrease in throughput of SU transmitter.

Any of the above scenarios could lead to a build-up of the number of requests waiting to be transmitted. When the queue is long, taking into account that the idle time of the spectrum band decreases as soon as PU vacate the channel, our system propose the release of additional resources to complement the existing one. This is to largely transmit the requests before the reappearance of PU on the band.

# 8 Security implementation in the proposed GSPN model

This paper adopts the combined sensing, security and performance tradeoff in CRN [8]. In the model, arriving SU on finding an idle encryption node gets encrypted and then transmitted. The model included security control that ceases the operation of the CRN on intrusion detection. The effects of encryption and security control was quantified and sensing time at which the combined tradeoff was maximized was predicted. In the proposed model, sensing time is used as the reference point to determine the improvement in the performance as a result of scalability.

# 9 GSPN and Mobius Petri Net Package

Queue network model and GSPN are two modelling approaches that can be used to generate the required traffic into the proposed model. Queue network representation of the model behaviour are only possible where only few details are required in the specification of the model [23]. On this note, GSPN is a preferred in the representation of proposed model. Moreover, GSPN is introduced to capture system behaviour involving synchronization, concurrency and conflict phenomena. Mobius petri net package is a simulation tool that support GSPN model. The package has some features to demonstrate the behaviour of the proposed GSPN model. A set of transitions, graphically as rectangular bars are used to generate actions that changes the state of the system [24]. The transition is enabled when an input place connected to transition contain at least one token. Enabling indicate execution of process while firing of a transition corresponds to completion of execution process [25]. Enabling and firing of a transition is associated to some random delay which is exponential [24]. Circular component is used represent the buffer for storing incoming requests. Transitions connected to the buffer are enabled immediately there is arrival of token to the place (buffer) indicating start of execution process. Tokens are requests or packets being transmitted through the network. There is arc for connecting input place to transition and from transition to output place. Inhibitor arc stops the execution of enabled transition. Inhibitor arc inhibits the firing of enabled transition.

# 10 Proposed Model

The proposed model is presented as a single node of CRN with two classes of requests(PU and SU requests) on a single spectrum band. PUs have priority over SU requests. As shown in Fig. 3, transitions SU generates requests to SU queue. The model consists of 3 components: SU activity, PU activity and security control components. The PU arrival is modelled as the firing of the transition 'PU arrival'. A token is deposited in the place 'PU in service'. Firing of transition 'PU departure' implies completion of service by PU and the transfer of token to place 'idle band' implies that the band is now idle. Similarly, SU arrival generate arrival to the SU encryption queue. While in the queue, load balancer monitors the average number token in the place 'Enc queue' and decides when an additional resource is needed. SU components consist of sensing, encryption and transmission nodes. Encryption node and SU transmitter is replicated and made redundant in events of low traffic but comes into operation when there is surge in service demand. It is assumed that SUs pay more for this extra services rendered to them. The sensing, encryption and transmission nodes for the existing resources are connected to a security control. The complementary server which consist of encryption and transmission nodes is also connected to security control. In the security control, the token in the place Secure is used to indicate a secured system. However, firing of transition Sec Inc shows security bleach which is demonstrated by transfer of token to place Insecure but not detected. The detection of the security incident is indicated by the firing of the transition Detect, transferring the token to the place Restore. Token at the place Restore block the operation of CRN until a new key is generated. The rate at which the security fails depends on the length of the encryption key. It was stated in [8] [22] that the longer the encryption key, the stronger the security of the network. In the proposed system, extensive sensing has adverse effects on the security and by extension the throughput of the SU. More information about the combined sensing, performance and security tradeoff in CRN can be found in [8]. As shown in Fig.3, the performance part of the model has a redundant resources that only come to operation when flagged by the average numbrer of request in the place 'Enc queue' greater than threshold.
The experiment was started with sensing time of 0.1 to 3.4 while the encryption time varies from 3.4 to 0.1 for both the main server and virtual server. It is assumed that the encryption time is proportional to the encryption key length. The rate of service request for both PU and SU is 0.5. The transition rate for SU transmission node is 10. Time to security incident starts from 15100s and decreases in steps of 1000s until it gets 1100s, then decreases in steps of 100s until 100s and further decreases by (time-time/2)s in each progression until it gets to 12.5s. In this work, we assumed the frame structure of [26] in which each CR user is assigned a frame size. The frame is divided into 3: the first part is for sensing, the second part is for request encryption and the last part is for transmission. As shown in the Fig.3 the request generated by SU joins the SU queue. This activates the sensing node. The sensor senses the band through the place 'PU in service' to detect the presence or otherwise of the PU signal. If there is token in the place 'PU in service' then

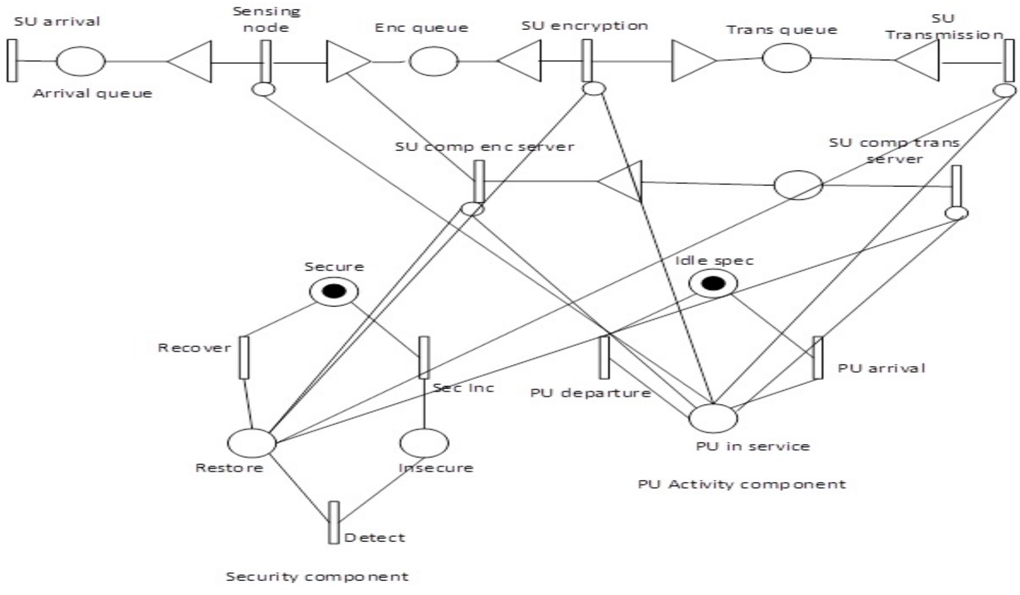


Fig. 3. Proposed GSPN model for CRN

no encryption is allowed to take place and vice versa. Similarly, if the same place contain a token, no transmission takes place. However, if the token moves from 'PU in service' to 'idle spec' then SU requests can be encrypted and transmitted.

# 11 Results and Analysis

This experiment is carried out to determine the highest throughput that would be achieved in a scalable and unscalable CRN with consideration to encryption and security control. The Fig.4 shows the result of the experiment carried out. The total throughput attained by SU depends on the access activities of PU as illustrated in equations (5) - (11)

At the beginning, the average sensing time is 0.1. This implies that the network senses for an average of 10 times in a unit of time. Since sensing occurs more frequently, the chances of detecting an idle spectrum band is higher resulting to large portions of SU requests being transmitted when an idle band is detected. If there is a frequent occupancy of the band by PU as illustrated in equation (5)-(11),or false alarm detection as highlighted in equation (12), resulting to build-up of SU requests, immediateley an idle band is detected, an additional resources is released in order to largely transmit the waiting request before the reappearance PU signal. This as shown in Fig. 4. leads to high throughput of SU than a system that is static in handling the surge in service demand. The study was carried out with different sensing time. The result shown in Fig.4. shows that without scalability the highest throughput of the SU is 0.428 while with scalability the throughput rose to 0.460. The result also indicates that it takes less sensing time for SU to attain its maximum throughput in scalable system than unscalable system. This implies that energy is more energy is conserved in a scalable system.

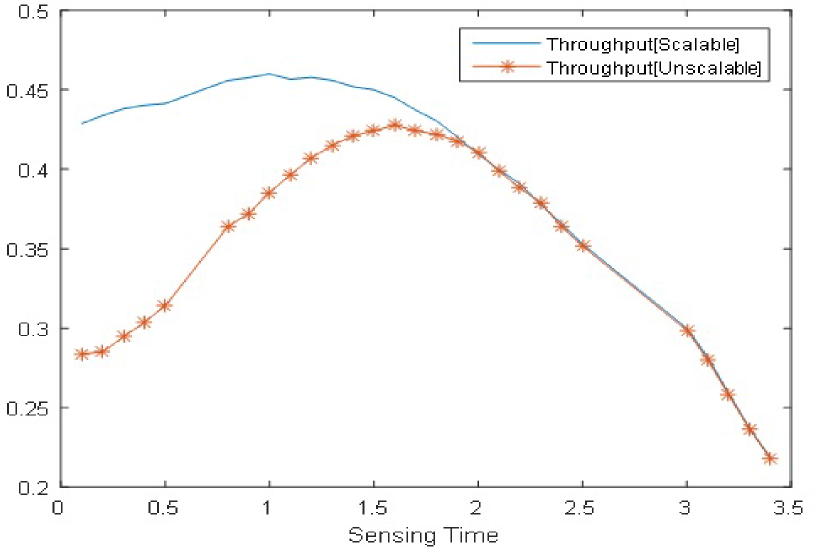


Fig. 4. Throughput for the scalable and unscalable system

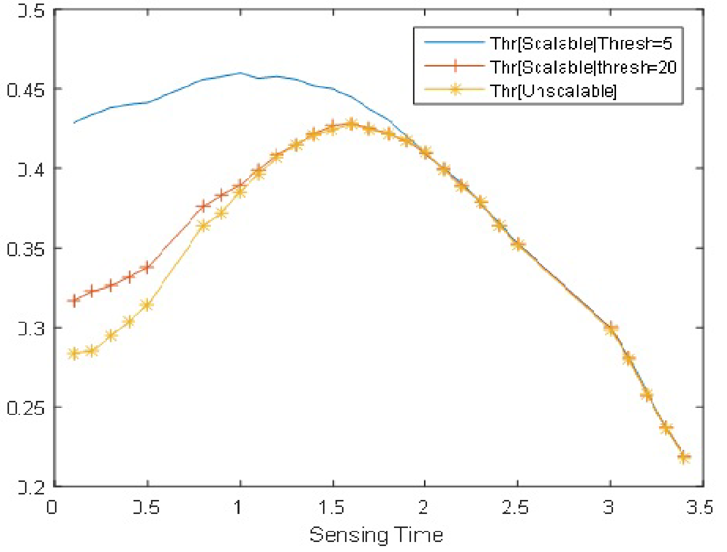


Fig. 5. Throughput for the scalable and unscalable system with different avg. no. of req

Fig.5 shows the result of the experiment with two different average number of requests in queue (5,20) as the threshold. With 5 as the threshold before additional resources is released, it is easily touched, prompting the release of additional resources. This results in two resources of the same capacity operating concurrently, leading to large portions of SU request to be transmitted within the interleaved spectrum band. However, when the threshold is 20, the existing resources operate alone until this this average number of requests is reached before extra resources is release which will take some time.

## 12 Conclusions and Future Work

CRN with scalable feature of cloud computing in conjunction with encryption and security control mechanism has been proposed. An experiment was carried out 'with' and 'without' scalability to determine the impact on the performance of CRN. The result of the investigation shows that the proposed CRN can sustain good performance upon sudden surge in service demand. The experiment also reveals that scalable system attains its maximum throughput at shorter sensing time which is good for battery saving.

Future work will consider extending the model to multiple CRNs with a central database that store spectrum opportunities. In this case, admission control will be applied to admit SUs since the reported idle band may not admit all SUs at same time. The participating CRN shares the idle bands as contained in the central database. For SUs with requests greater than predetermine threshold, additional resources is proposed to be released in order to complement and transmit large portions of its waiting requests before the reappearance of a PU. In this way, the impact of the extended model on the aggregated throughput will be investigated.

## References

[1] Prashob, R. N., Vinod, A. P., and Krishna, A. K. (2010, November). An adaptive threshold based energy detector for spectrum sensing in cognitive radios at low SNR. In Communication Systems (ICCS), 2010 IEEE International Conference on (pp. 574-578). IEEE.

[2] Nekovee, M. (2010, April). Cognitive radio access to TV white spaces: Spectrum opportunities, commercial applications and remaining technology challenges. In New Frontiers in Dynamic Spectrum, 2010 IEEE Symposium on (pp. 1-10). IEEE.

[3] Alamgir, M., Faulkner, M., Gao, J., and Conder, P. (2008, October). Signal detection for cognitive radio using multiple antennas. In 2008 IEEE International Symposium on Wireless Communication Systems (pp. 488-492). IEEE.

[4] Sansoy, M.,and Buttar, A. S. (2015, March). Spectrum sensing algorithms in cognitive radio: A survey. In Electrical, Computer and Communication Technologies (ICECCT), 2015 IEEE International Conference on (pp. 1-5). IEEE.

[5] Naeem, M., Illanko, K., Karmokar, A., Anpalagan, A., and Jaseemuddin, M. (2013). Energy-efficient cognitive radio sensor networks: Parametric and convex transformations. Sensors, 13(8), 11032-11050.

[6] Maleki, S., Pandharipande, A., and Leus, G. (2011). Energy-efficient distributed spectrum sensing for cognitive sensor networks. IEEE sensors journal, 11(3), 565-573.

[7] Rawat, D. B., Shetty, S., and Raza, K. (2012, September). Secure radio resource management in cloud computing based cognitive radio networks. In Parallel Processing Workshops (ICPPW), 2012 41st International Conference on (pp. 288-295). IEEE.

[8] Ejike, C., Demetres, K.(2017). Combined Sensing, Performance and Security Tradeoff in Cognitive Radio Networks. 2017 IEEE International Symposium on Network Computing and Applications (NCA)

[9] Liang, Y. C., Zeng, Y., Peh, E. C., and Hoang, A. T. (2008). Sensing-throughput tradeoff for cognitive radio networks. IEEE transactions on Wireless Communications, 7(4), 1326-1337.

[10] Chieu, T. C., Mohindra, A., and Karve, A. A. (2011, October). Scalability and performance of web applications in a compute cloud. In e-Business Engineering (ICEBE), 2011 IEEE 8th International Conference on (pp. 317-323). IEEE.

[11] Lee, J. Y., and Kim, S. D. (2010, November). Software approaches to assuring high scalability in cloud computing. In e-Business Engineering (ICEBE), 2010 IEEE 7th International Conference on (pp. 300-306). IEEE.

[12] E.E Chuku, A., and D.D Kouvatsos (2016). Performance Evaluation of Service Channel Scalability on Cloud Platforms. In 32nd UK Performance Engineering Workshop, University of Bradford.

[13] You, C., Kwon, H., and Heo, J. (2011). Cooperative TV spectrum sensing in cognitive radio for Wi-Fi networks. IEEE transactions on consumer electronics, 57(1), 62-67.

[14] Vilaplana, J., Solsona, F., Teixid, I., Mateo, J., Abella, F., and Rius, J. (2014). A queuing theory model for cloud computing. The Journal of Supercomputing, 69(1), 492-507.

[15] Lorido-Botran, T., Miguel-Alonso, J., and Lozano, J. A. (2014). A review of auto-scaling techniques for elastic applications in cloud environments. Journal of Grid Computing, 12(4), 559-592.

[16] Allen, A. O. (2014). Probability, statistics, and queueing theory. Academic Press.

[17] Abdulsattar, M. A., and Hussein, Z. A. (2012). Energy detection technique for spectrum sensing in cognitive radio: a survey. International Journal of Computer Networks and Communications, 4(5), 223.

[18] Kim, K., Xin, Y., and Rangarajan, S. (2010, December). Energy detection based spectrum sensing for cognitive radio: An experimental study. In Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE (pp. 1-5). IEEE.

[19] Saleem, Y., and Rehmani, M. H. (2014). Primary radio user activity models for cognitive radio networks: A survey. Journal of Network and Computer Applications, 43, 1-16.

[20] A., Censki (n.d). Reliability Modelling and Analysis with Free and Open Source Software.

[21] Bhattacharjee, S., Rajkumari, R., and Marchang, N. (2014). Cognitive Radio Networks Security Threats and Attacks: A Review. Journal of Computer Applications, ICICT, 16-19.

[22] Wolter, K., and Reinecke, P. (2010, June). Performance and security tradeoff. In International School on Formal Methods for the Design of Computer, Communication and Software Systems (pp. 135-167). Springer Berlin Heidelberg.

[23] Balbo, G., Bruell, S. C., and Ghanta, S. (1988). Combining queueing networks and generalized stochastic Petri nets for the solution of complex models of system behavior. IEEE Transactions on Computers, 37(10), 1251-1268.

[24] Marsan, M. A., Balbo, G., Conte, G., Donatelli, S., and Franceschinis, G. (1994). Modelling with generalized stochastic Petri nets. John Wiley and Sons, Inc..

[25] Mobius Tool: Mobius version 2.4 Rev. 1 (2012). Copyright@2012 William H.Sanders and The Board of Trustees of University of Illinois.

[26] Stotas, S., and Nallanathan, A. (2010, May). Overcoming the Sensing-Throughput Tradeoff in Cognitive Radio Networks. In ICC (pp. 1-5).