An investigation of performance versus security issues in Cognitive Radio Networks

Aliyu Abubakar

Abstract: Cognitive Radio (CR) is introduced in order to alleviate the problem of Spectrum shortage whereby unlicensed users are allowed to coexist with licensed users to utilize the spectrum band. Studies have shown that more than 75% of spectrum remains unutilised by the licensed users; this motivated the Federal Communication Commission (FCC) in 2010 to approve a new law that allows unlicensed users equipped with CRs to co-exist with licensed users and have access to spectrum band opportunistically without disrupting the licensed users operation. This allows the efficient utilization of spectrum band.
However, this research work is primarily aim to look at how security mechanisms affect the performance of the Cognitive Radio Network users.

Keywords: Cognitive Radio Network, Primary User, Secondary User, Spectrum.

1. INTRODUCTION

Cognitive Radio is an intelligent communication device in wireless technology that has the ability to sense the environment in which it operates, and adjust its parameters in order to utilize the available spectrum band which is legally or authoritatively assigned to licenced users (called primary users) [16],[18]. Cognitive User, or sometimes referred to as Secondary User, is a user that has no legal right to access the spectrum band or use the transmission channel [10]. The static allocation of spectrum band to Primary Users only has introduces a tremendous problem today as the wireless devices in the world keep increasing every day, and there is a requirement for these devices to have access to this scarce natural resource. Studies have shown that more than 75% of allocated spectrum band remains idle (unutilized), so this inefficient usage of the spectrum necessitates the emergence of the Cognitive Radio to provide a high reliable communication and to utilize the spectrum efficiently [19]. This efficient usage of the spectrum is achieved by allowing the unlicensed users (Secondary Users) to opportunistically access the spectrum band in the absence of the licensed users, and also the secondary users must vacate the channel immediately to another idle channel when primary users reappear [4]. When a Primary User is using the spectrum band, Secondary User must not transmit in that channel, and even if the Secondary User is transmitting when the Primary User reappears to start transmitting in that channel, the Secondary User must stop and allow the Primary User because it has the exclusive right to access the channel at any time.

Cognitive radio is as well faced with security threats and attacks. Some of which are common in wireless communication networks while some are peculiar to cognitive radio networks only. Therefore numerous researches have been conducted by many scholars trying to address the security challenges in CRNs and the solutions to those attacks.

- *Aliyu Abubakar is currently working as Assistant Lecturer at Gombe State University, Nigeria (Academic researcher) in the department of Mathematics. He obtained a BSc degree in Computer Science at Gombe State University in 2012, and MSc degree in Cyber Security at University of Bradford, United Kingdom in 2015*
  E-mail: aleeuzin@gmail.com

1.1 motivation

The vast growing of wireless communication today has posed a great problem due to lack of enough spectrum band to accommodate all the wireless devices or users. Today, due to increasing wireless devices around the world, which led to the introduction and adoption of IPv6, also necessitates the emergence of Cognitive Radio Networks. It is a network that allows unused spectrum band to be utilised by other users that are not registered. It provides solution to the problem faced by underutilization of spectrum band by allowing the unlicensed users to opportunistically access and utilised the idle spectrum resources as long as the licensed users cannot be interrupted.

Despite this promising solution provided by Cognitive Radio Network to wireless users, it suffers security attacks and performance drawbacks due to security controls that need to be put in place to thwart the security challenges. The security issue in Cognitive Radio Networks is the main focus of this research and to comprehensively understand the effect of security on the performance of the network

2. OVERVIEW OF COGNITIVE RADIO AND SECURITY ISSUES

2.1Characteristics of Cognitive Radio

Cognitive Radio has two major characteristics as discussed below.

2.1.1 Cognitive Capability

This characteristic of cognitive radio refers to the ability to detect or receives information from the radio environment [20]. The monitoring of the radio environment is not only restricted to the power frequency band, but also ability to detect the idle white spaces in the channel and the availability of license users in order to avoid interference by secondary users (unlicensed users).

2.1.2 Re-Configurability

This feature allows the network to dynamically adjust its configuration in order to improve the Quality of Service based

on the sensed parameters of the radio environment [8], [3]. In Cognitive Radio Network, the Secondary User must always keep track of the presence of the Primary User in the network. Secondary User can make use of the channel if the Primary User is absent, and vacate the channel whenever the Primary User re-appears. The main idea behind Cognitive Radio is to have efficient spectrum usage through cognitive capability and re-configurability. This is because most of the spectrum is assigned to licensed users and there is a proliferation in wireless devices which also needs to have access to these resources. The best way to confront the problem is to share these resources with other users in need without causing any interruption to the authorised users (Primary Users) [2].

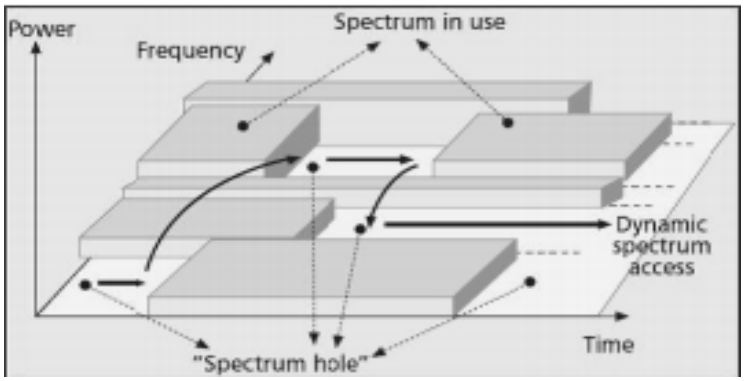

Figure 1: Spectrum white space [7]

2.3 Main Functions of Cognitive Radio

Basically, Cognitive Radio has four major functions, namely;

1. Spectrum sensing
2. Spectrum sharing
3. Spectrum management and
4. Spectrum mobility

2.3.1 Spectrum sensing

Cognitive Radio has the ability to determine available spectrum and also sense the presence of Primary User (license user) in a channel. The sensing technique is very important in Cognitive Radio because it avoids collision between the unlicensed users and licensed users.

2.3.2 Spectrum Management

The based available spectrum band is allocated by CR to the users in order to achieve best quality of service requirement. In spectrum management, two techniques exist; spectrum analysis and spectrum decision. In spectrum analysis, white spaces are not only determined by time varying radio environment but also the activities of the primary user. When all such analysis is done, appropriate spectrum band will be selected to meet up the QoS requirement, this is done under spectrum decision.

2.3.3 Spectrum Sharing

Spectrum sharing is to share some of the idle spectrum band to secondary users in such a way that the operation of primary users will not be affected in any way. If primary users reappear to use the shared spectrum band, secondary users must halt their operation and vacate the channel [9].

2.3.4 Spectrum Mobility

CR can change its operating frequency in order to use spectrum in a dynamic manner and make use of the best available frequency band. When PU appears to use a channel, SU must dynamically determine a best idle white hole and vacate the current channel it's operating in.

2.4 Security Issues in Cognitive Radio Networks

Cognitive radio provides a promising technique in solving the problem of spectrum scarcity by dynamically giving the opportunity to unlicensed users to access the unutilised spectrum band. As in wireless networks, security challenges exist in cognitive radio networks which are mostly ignored by most of the researchers. Therefore, this research work provides an insight of some existing security attacks on Cognitive Radio Networks.

2.4.1 Primary User Emulation

The principle adopted by Cognitive Radio is that a secondary user is only allowed to access and use a spectrum band when Primary User is not using it (i.e. the channel is idle). It also part of the principle that whenever Secondary User is using the spectrum band in the absence of Primary User, if the Primary User re-appears to use the spectrum band, Secondary User must vacate that channel because Primary User is the legitimate user to utilise the channel without interference.

Primary User Emulation attack is launched by malicious Secondary User impersonating a primary user in order to have full access and utilise the whole resources of a given channel without sharing such resources with other secondary users [1], [5],[21],[23].

In [1], [14] and [15], the authors stated that Primary User Emulation Attack is classified into two;

- Selfish Primary User Emulation attack
- Malicious Primary User Emulation attack

Selfish Primary User Emulation attack

In selfish Primary User Emulation attack, the motivation behind the attack is to deny other secondary users utilising the resources, in order to increase the attacker's share.

Malicious Primary User Emulation attack

While in Malicious Primary User Emulation attack, the aim of the attack is to deny other Secondary Users from using the idle spectrum holes.

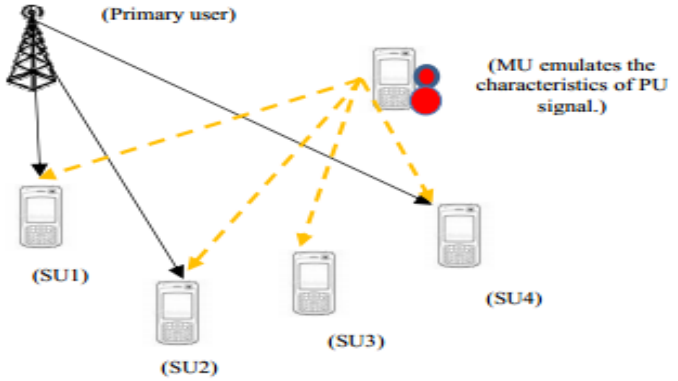

Figure 2: Illustration of PUEA launching scenario [12]

2.4.2 Objective Function Attack

It can be recalled from the definition of cognitive radio that " *Cognitive radio is a smart radio that has the ability to sense the external environment, learn from the history, and make intelligent decisions to adjust its transmission parameters according to the current state of the environment*" (c.f.,[1]). In other literature, Cognitive Radio is defined as "*software defined radio in wireless communication that sense the environment and detect the free space amongst the crowded channel and utilise the vacant space sufficiently*" (c.f., [6]). The cognitive engine has the sole responsibility to adjust the parameters of the radio in order to conform to certain specific requirements such as low energy consumption, high data rate, and high security. The radio parameters include centre frequency, bandwidth, power, modulation type, coding rate, channel access protocol, encryption type, and frame size. When cognitive engine is trying to find the appropriate radio parameters to the current environment, the attacker manipulates the parameters he has control on (such as transmission rate) in order to make the result biased and tailored to his interest. In this type of attack, cognitive engine is prevented from using high security level by that attacker. Whenever the cognitive engine tries using it, the attacker initiates the jamming attack on the radio there by degrading the overall objective function. Then the cognitive engine is forced to halt its attempt of increasing the security level in order not to degrade the objective function.

2.4.3 Jamming Attack

This is a physical layer attack in which the attacker sends continuous series of packets in order to stop the legitimate users from sending their packets into the channel. It is a form of Denial of Service attack. The attacker (jammer) may send continuous packets of data making it impossible for legitimate users to sense a channel that is idle [6], [17]. In some cases, the attacker can disrupt communication by blasting a radio transmission resulting in the corruption of packets received by legitimate users.

2.4.4 Spectrum Sensing Data Falsification

In this type of attack, the attacker send false spectrum sensing output to other users or fusion centre, to make receivers to make wrong sensing decision [11]. Fusion centre is responsible for collecting all sensed information and making decision on which frequency bands are occupied and which are free.

2.4.5 Control Channel Saturation DoS Attack

It happens when many Cognitive Radios tries to communicate at the same time. The common control Channel becomes a problem because the channel can only support a certain number of concurrent data channels. Attacker uses this feature to generate and forged MAC control frames in order to make control channel saturated and thus decreasing the network performance due to the collision in the link layer [5].

2.4.6 Sinkhole Attacks

The attacker fools the neighbours by broadcasting itself as the best route to a certain specific destination [1]. When a neighbour send packet to the attacker thinking it's the best route reach a specific destination, the attacker may launch a new attack called "*selective forwarding*", whereby packets from other nodes in the network can modified or discarded.

2.4.7 Hello Flood Attack

This is also accomplished when attacker broadcast message to all the nodes in the network to convince them that it's their neighbour in the network [13]. Other nodes in the network will be convinced to forward their packets to the attacker as their neighbour, this leads to packet loss. And also if the attack is later discovered, the victim will be left with no neighbour to communicate with as all the nodes are now transmitting towards the attacker.

3. SYSTEM MODELLING USING QUEUING MODEL

When we talk of modelling, we are just referring to a process of creating a model. A model is a representation of a real system in an abstract from [22]. It actually looks similar to the real system but in a simplified format. It has almost all the approximation features of the actual system but it must not be so complex also, it should be so simple to understand and experiment with it. This is because models are normally used to enable us predict the changes on the system.

3.1 Queuing Model

A queuing system comprises of one or more servers that provide services to arriving customers or users. It is normal for people waiting to receive service to wait in a queue for each to be served by a server or servers. Some of the normal queues that exist in today's human activities include joining a queue to be served from an ATM, buy stamp, purchase a movie ticket, boarding an aeroplane, etc. This happens when the server is handling too much service requests than it can cope with. In the aforementioned scenarios, the server could be bank cashier, ATM machine, etc. Queues are also common in Computer systems, service request to be processed by an interactive system, I/O requests queues, queues formed by users to have an access to a certain channel, this is common in various areas like military operations, airline reservation systems, telephone systems, etc. So a queue is collection of service centre, which

stands for system resources that can be accessed, and users that request for such resources.

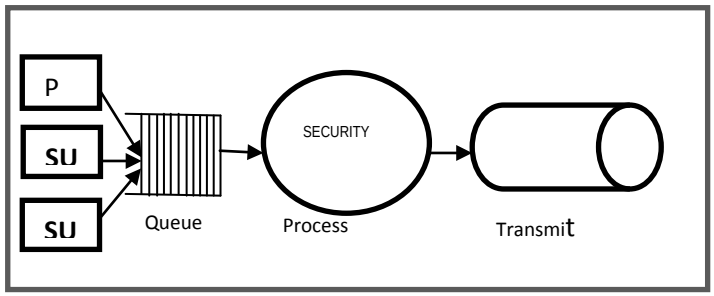

Figure 3 Queuing Model

For the purpose of experimenting, the above queuing model was used in predicting the behaviour and the arrival rate of the users in the network. The arriving packets have to wait in a queue depending on the availability of the idle channel. Secondary Users experience much waiting time because while in waiting, the arriving Primary User will join the head of the queue leaving Secondary Users behind. Then, get served by the server (this is where all the processes are applied including the security controls like encryption) before sent for transmission at last.

4. SIMULATION

To reconfigure and experiment with a real system is difficult and very expensive, so model is used instead. Simulation is the operation of the model of the system it represents. Performance of a system under different configurations can be predicted using simulations.

Simulation is use to predict the behaviour of a system before it is built, helps to avoid the probability of system failure in order to meet certain specifications, to determine and avoid unforeseen hold-up and to evaluate and optimize the performance of a system. In most cases simulation answers the following question as stated in [22] like "What is the best design for a new telecommunication network? What are the associated resource requirements? How will a telecommunication network perform when the traffic load increases? How will a new routing algorithm affect its performance? What will be impact of a link failure? What will be the impact of security on performance of the network?"

4.1 Benefit of using Simulation

- Simulation can be used to explore operating methods, how information flows in a system without disrupting the normal or on-going process of the real system.
- Simulation can save the cost of acquisition of resources by testing new hardware designs, transport and communication systems.
- It helps to understands how the real system operates.

4.2 Objective of the Simulation

The main objective here is to investigate the service performance of the system under two conditions:

1. the performance behaviour of the system when security is disabled
2. the performance of the system when security is enabled.

Then the result analysis aims to suggest the best working condition (performance) of the system despite the security presence.

4.3 Results and Analysis

Queue Time: This is the average time spent by each arriving packet in a queue waiting to be served by the server.

The figure 4 below depicts the best performance of the network when the security is turned off (disabled). This can be seen clearly that the total delay experienced by each user in the queue is insignificant. The Primary Users experienced a very low delay in the queue because they have much more priority to get their requests processed than Secondary Users. Therefore whenever they are in a queue with Secondary Users which have low or no priority, secondary users are kept waiting in the queue until Primary Users are exhausted. Despite the fact that both Primary Users and Secondary Users have the same arrival rate, Secondary Users experienced more delay in the queue compared to Primary Users.

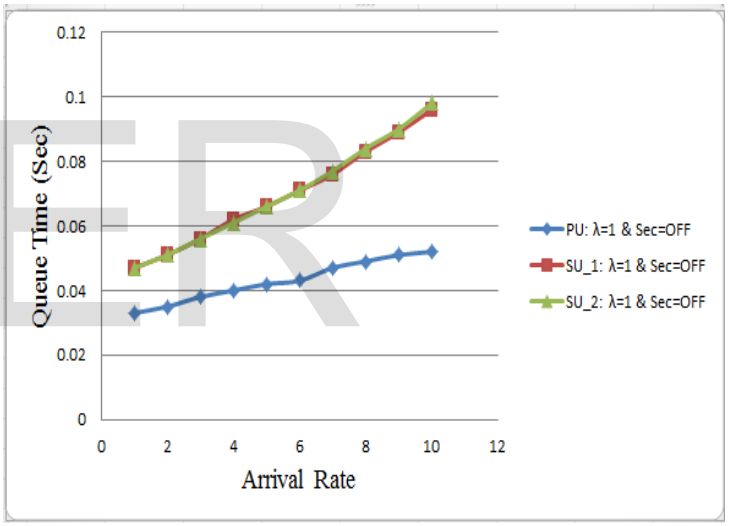

Figure 4 Queue Time without Security

It is shown in figure 5, both primary users and secondary experienced a longer period of time (delay) in the queue because of the security is enabled. This definitely affected the performances of all the users in the system. The delay experienced is higher than when there is no security at all. This is because a user receiving service spent much time because of the undergoing security processes, which affects the users in the queue.

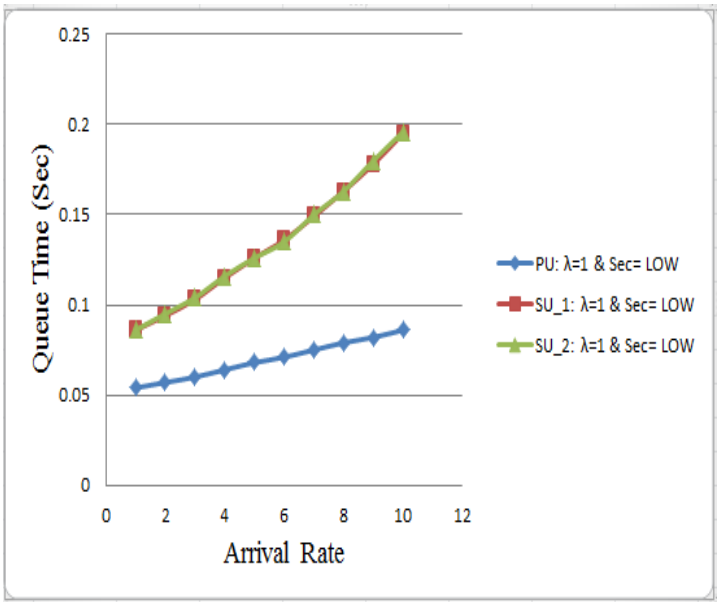

Figure 5 Queue Time with minimum security

But trying to enable much more security can result in having worst performance of the system. Figure 6 shows all the users experienced worst performance delay in the queue when the enabled security is very high.

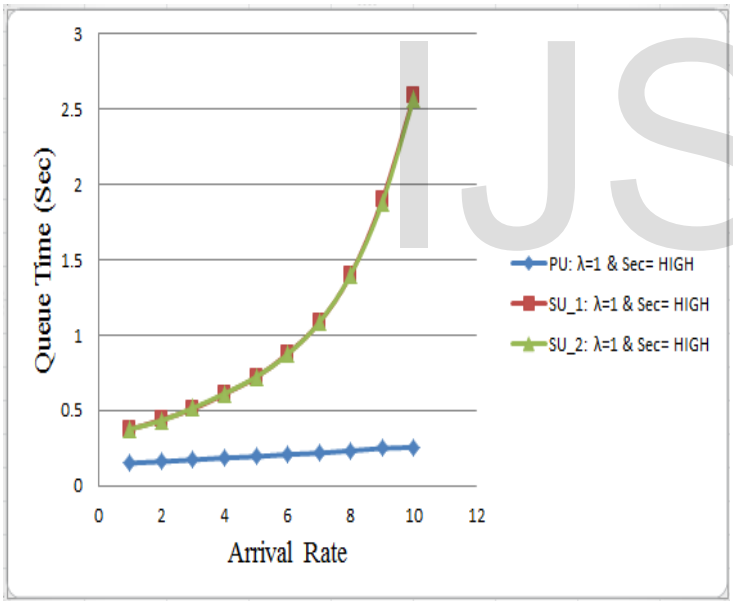

Figure 6 Queue Time with high security showing worstperformance

Response Time:

Response time is sum amount of time a system takes to respond to a service request [24]. In another word, response time is the time between sending a request and receiving a response or feedback or the time it take a system to complete executing a task [25],[26].

Figure 7 depicts that the response time of all SUs and Pus request is very minimum when security is OFF compared to what we get when security is ON in figure 8. This depends on the amount of security set

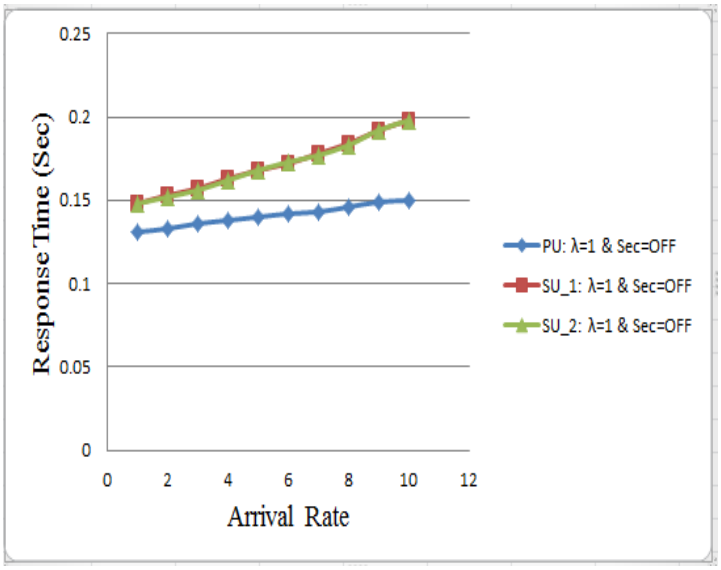

Figure 7 Response Time without security

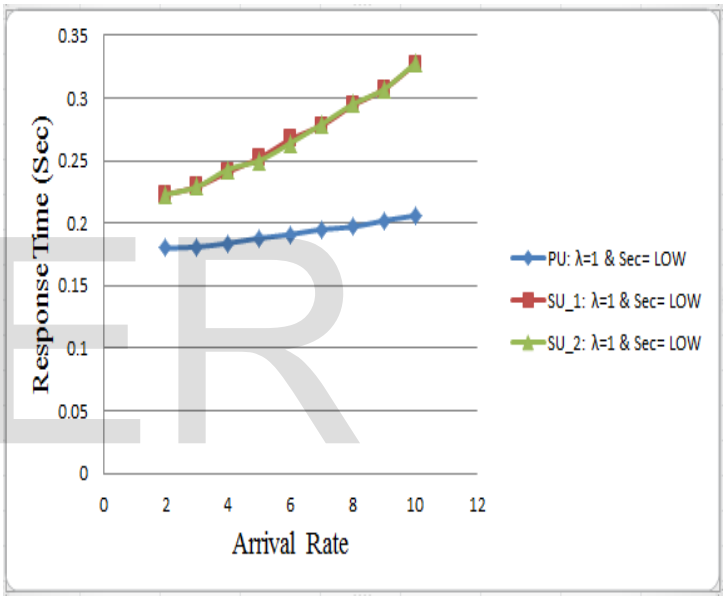

Figure 8 Response Time with minimum security

Figure 9 shows the worst average response time experienced if the security is very high.

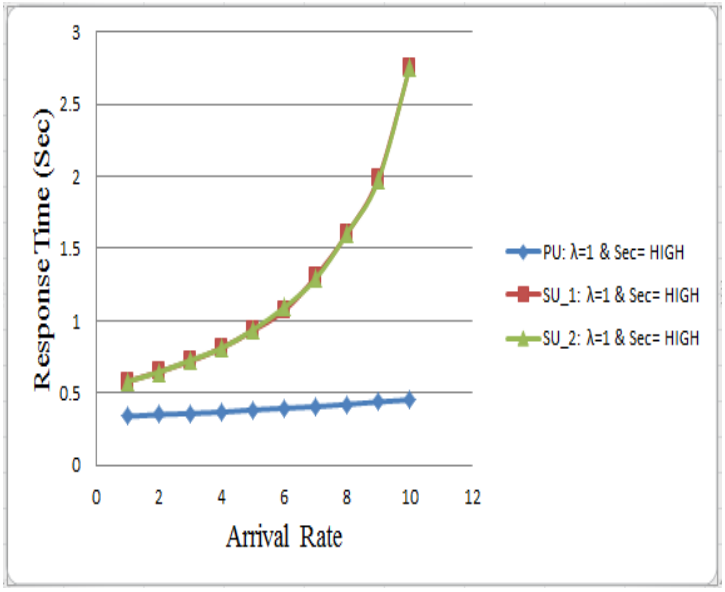

Figure 9 Response Time with high security showing worst performance

5. CONCLUSION AND FUTURE WORK

Based on the investigation carried out, the result shows that the performance of the network is highly effective when security is disabled. However, the system experiences worst performance level when the security tends to be high. But network system today cannot cope with the rate of security attacks targeting the infrastructure; it becomes necessary to implement some security measures in order to thwart the confronting security challenges.

However, it is worth studying, to investigate the optimum performance level (acceptable performance) when security measures are placed.

FERENCE

1. El-Hajj, W., Safa, H. and Guizani, M. (2011). Survey of Security Issues in Cognitive Radio Networks. *Journal of Internet Technology*, 12(2).
2. Akyildiz, I., Lee, W. and R. Chowdhury, K. (2009). CRAHNs: Cognitive radio ad hoc networks. *Elservier*, pp.1-27.
3. Raghuwanshi, S. and Barde, C. (2013). A Survey of Cognitive Radio Network Techniques and Architecture. , *International Journal of Innovative Research in Engineering & Multidisciplinary Physical Sciences (IJIRMPS)*, 1(1).
4. Alhakami, W., Mansour, A. and A. Safdar, G. (2014). Spectrum Sharing Security and Attacks in CRNs: A Review. *(IJACSA) International Journal of Advanced Computer Science and Applications*, 5(1), pp.76-87.
5. Dubey, P. and Choudhury, S. (2014). A Survey-Cognitive Radio Network Attacks & Preventions. *International Journal of Advance Foundation and Research in Computer (IJAFRC)*, 1(2), pp.12-20.
6. Nanthini, S., Hemalatha, M., Manivannan, D. and Devasena, L. (2014). Attacks in Cognitive Radio Networks (CRN) - A Survey. *Indian Journal of Science and Technology*, 7(4), pp.530–536.
7. Irianto, K. and Kouvatsos, D. (2014). An Investigation of performance versus security in Cognitive Radio Networks with supporting Cloud Platforms. *International Journal of Computer, control, quantum and information engineering*, 8(10), pp.1671-1678.
8. Al-Alawi, R. (2011). Quality of Service Cognitive Radio Ad hoc Mobile Network. *Dissertation in Department of Computing, University of Bradford*.
9. Kanth, V., Chandra, K. and Kumar, R. (2013). Spectrum Sharing In Cognitive Radio Networks. *International Journal of Engineering Trends and Technology (IJETT)*, 4(4), pp.1172-1175.
10. Vernekar, D. (2012). *An Investigation of Security Challenges in Cognitive Radio Networks*. MSc. University of Nebraska.
11. C, K. and A.C, S. (2014). A Study on Primary User Emulation Attack in Cognitive Radio Networks. *International Journal of Computer Science Engineering and Technology (IJCSET)*, 4(10), pp.260-262.
12. Das, D. and Das, S. (2013). Primary User Emulation Attack in Cognitive Radio Networks: A Survey. *International Journal of Computer Networks and Wireless Communications (IJCNWC)*, 3(3), pp.312-318.
13. Khare, A., Saxena, M., Thakur, R. and Chourasia, K. (2013). Attacks & Preventions of Cognitive Radio Network-A Survey. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, 2(3), pp.1002-1006.
14. Shan-shan, W., Xing-guo, L. and Bai-nan, L. (2013). Primary User Emulation Attacks Analysis for Cognitive

Radio Networks Communication. *TELKOMNIKA*, 11(7), pp.3905-3914.

15. Sampath, D. and Dharmar, V. (2014). Performance Analysis of Primary user Emulation Attacks in Cognitive Radio Networks. Proc. of Int. Conf. on Advances in Communication, Network, and Computing, CNC.
16. Meghanathan, N. (2013). A Survey on the Communication Protocols and Security in Cognitive Radio Networks. *International Journal of Communication Networks and Information Security (IJCNIS)*, 5(1), pp.19-38.
17. Attar, A., Tang, H., Vasilakos, A., Yu, F. and Leung, V. (2012). *A Survey of Security Challenges in Cognitive Radio Networks: Solutions and Future Research Directions*. [e-book] Proceedings of the IEEE, pp.3172-3186. Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.338.566&rep=rep1&type=pdf [Accessed 24 Aug. 2015].
18. Taheri, S., Sharifi, A. and Berangi, R. (2012). Deal with attacks over cognitive radio networks authentication. *International Journal of Computer Technology & Applications*, 3(6), pp.2027-2032.
19. Rout, A. and Sethi, S. (2013). Throughput Analysis of Spectrum in Cognitive Radio Ad Hoc Network. *International Journal of Application or Innovation in Engineering & Management (IJAIEM)*, 2(6), pp.502-506.
20. Bhrugubanda, M. (2014). A Survey on Simulators for Cognitive Radio Network. *International Journal of Computer Science and Information Technologies*, 5(3), pp.4760-4761.
21. Idoudi, H., Daimi, K. and Saed, M. (2014). Security Challenges in Cognitive Radio Networks. London: Proceedings of the World Congress on Engineering.
22. Maria, A. (1997). Introduction to modelling and simulation. *Proceedings of the 1997 Winter Simulation Conference*, pp.7-13.
23. Clancy, T. and Goergen, N. (n.d.). *Security in Cognitive Radio Networks: Threats and Mitigation*. [e-book] Available at: http://www.ece.umd.edu/~goergen/docs/cr-crowncom08.pdf [Accessed 18 Aug. 2015].
24. Wikipedia, (2015). Response time (technology). [online] Available at: https://en.wikipedia.org/wiki/Response_time_(technology) [Accessed 11 Aug. 2015].
25. Docs.oracle.com, (2015). Performance Overview. [online] Available at: https://docs.oracle.com/cd/A95427_01/httpperf/concpts.htm [Accessed 11 Aug. 2015].
26. Rubinstein, A. (2013). Response time and decision making: An experimental study. Judgment and Decision Making, 8(5), pp.540-551