

# Lightweight Secondary User Authentication Protocol in Cognitive Radio Networks (CRN)

Aliyu Abubakar

Dept. of Mathematics, Faculty of Science, Gombe State University, Nigeria

## Abstract

The explosive growth of wireless communication nodes has encountered a spectrum scarcity problem which led to emergence of intelligent communication technology known as Cognitive Radio (CR). CR provides opportunistic utilization of spectrum band by unlicensed users when licensed users are idle. Security of Cognitive Radio Networks (CRN) is very challenging which needs to be modelled effectively considering the dynamic nature of the environment. In this study, an effective authentication mechanism is proposed addressing emulation attack, denial of Service attack and withstanding replay attack.

## Keywords

Cognitive Radio (CR), Secondary User (SU), Primary User (PU), Spectrum Band

## I. Introduction

Spectrum allocation has become a challenging aspect to spectrum regulatory agencies today due to proliferation of communication devices. Cognitive Radio is a technology that was discovered and come into existence in the late 90s. This technology was proposed due to high demand of spectrum band because of the proliferation of networking devices [1]. Under-utilization of spectrum band led to the experienced shortage in the availability of such resources, hence posed the need to address the problem in which CRN emerges. The spectrum band was used by the licensed users and most of the assigned spectrum band to the licensed users is underutilized which led to the waste of the resources while the demand for such useful resource is very high.

Unlicensed users are allowed to opportunistically use the unused spectrum band [2] when the channel is idle. In CRN, users are categorised into two: Primary User (PU) and Secondary User (SU). PU is a user in CRN that has full right to use the spectrum band at any time without been interrupted by other users. PU has exclusive right to use the resources whenever it needs to transmit on a channel. In the other hand, SU is a user in CRN that opportunistically accessed and make use of the spectrum band when the channel is idle (i.e. when the Primary User is absent or not transmitting). This implies that SU must listen (sense) to all the transmitting channels to detect the unavailability of PU before transmitting in order to avoid interference or service disruption.

The main concern in this scenario is impersonation attack by SU, where they may disguise and behave like PU thereby causing harm to licensed users. As such, a strong and efficient authentication must be implemented to help identify malicious entities. The objective of this work is to provide a means to preserve confidentiality, integrity, availability (also known as CIA). Confidentiality ensures that information is protected against any intruder who has no right to access it; to preserve the privacy of the network users. Integrity is another requirement that ensures data are not tempered by unauthorized access. Integrity ensures data are not altered by third party who has

zero clearance. Data should be modified by the owner or by authorized entity. Availability ensures that services are provided and received by users at any time it was requested. Any attempt to disrupt the service by denying other users right to use the resources is considered a breach to network availability.

Towards the end, the research in this paper proposes an efficient protocol to preserve CIA, helps in identifying malicious entity and energy efficient. The rest of the paper is organized as follows: section II provides an excerpt from related literatures, proposed protocol is presented in section III, section IV provides the analysis of the protocol's strength, and section V concludes the study.

## II. Literature Review

Das [3], proposed an authentication protocol in Wireless Sensor Networks (WSNs). The protocol has two phases: registration phase and authentication phase. Only authenticated users can participate in message exchange. Additionally, Wong et al [4] proposed a user authentication scheme in WSNs as well. The authors in [4] also provided authentication scheme for wireless sensor networks dynamically. In their work, strong password authentication in wireless network such as hospitals, schools and banks were addressed. Various research has been proposed to address authenticate problems in communication networks as in [5-12] but not strong enough to address impersonation attacks.

In the work carried out by [13], the authentication presented do not consider the energy consumption and the traffic going in and out at the destination node. Both studies proposed an authentication schemes in which the nodes (users) authenticate to the destination node, register itself at the cluster level, before making service/resource request to the destination node. Too many arriving nodes registering themselves at the Base Station might eventually lead to the Denial of Service (DoS) to already registered nodes. Malicious SUs might cooperatively lunch an attack by flooding the base station with registration request.

Sha et al in [14], proposed a lightweight authentication protocol for Cognitive Radio Mobile Ad hoc Network. Every joining node must know the Group ID and the group IP address it belongs. Authentication is performed by a central trusted entity unlike other literatures in which the existing users authenticate new nodes as reported in [15]. Allowing existing nodes in the network to authentication new nodes posed a tremendous effect towards the energy consumption and battery life of the individual nodes [14]. Joining nodes must respond to a small challenge before obtaining a piece of information from the group. However, the work lacks techniques to detect a malicious user trying to replay the messages.

Chandrashekar and Lazos [16] proposed an authenticating mechanism to prevent malicious users emulating primary users' activity. Primary User Emulation (PUE) affect the SUs adversely by denying them the little opportunity to utilise the idle channels. They used a third entity (called 'helper') deployed in SUs environment to update SUs regarding PUs activities and broadcast the information to SUs nodes. The

helper node authenticates the PU signals and its location, so whenever PU is transmitting, information will be made available to SUs. The SU must be authenticated and monitored because they pose a considerable number of threats apart from PUE. PUE attack can also be mitigated if we know the Angle of Arrival (AoA) of the signal and the distance from where the signal is emanating [17]. Although location table must be updated all the times whenever PU changes location.

Similarly, Khasawneh and Agarwal [18] took advantage of both public key infrastructure based and symmetric key cryptography to provide secured means of communication CRNs. The communication between network users used public key until the symmetric key is generated which will be used in the subsequent communication.

### III. Proposed Authentication Protocol

We made the following assumptions in our work:

- The cluster head (CH) is a trusted user among other cluster members
- The cluster head is a trusted party by the Fusion centre
- Fusion centre is a trusted by the Base Station; the operation performed by the fusion centre in authenticating users is synchronized to the BS
- Cluster(C) comprises of the cluster members (Secondary Users) and the Cluster Head (trusted SU)
- Asymmetric key cryptography is used by the cluster members and the cluster head

The model of the network is depicted in Fig. 1 which illustrates the network scenario of our proposed protocol. A Fusion Center (FC) which might be interacting with two or more clusters. Each cluster may have several cluster members (SU). Among the cluster members, there exist a powerful designate trusted entity which has capacity to accommodate many users within the cluster.

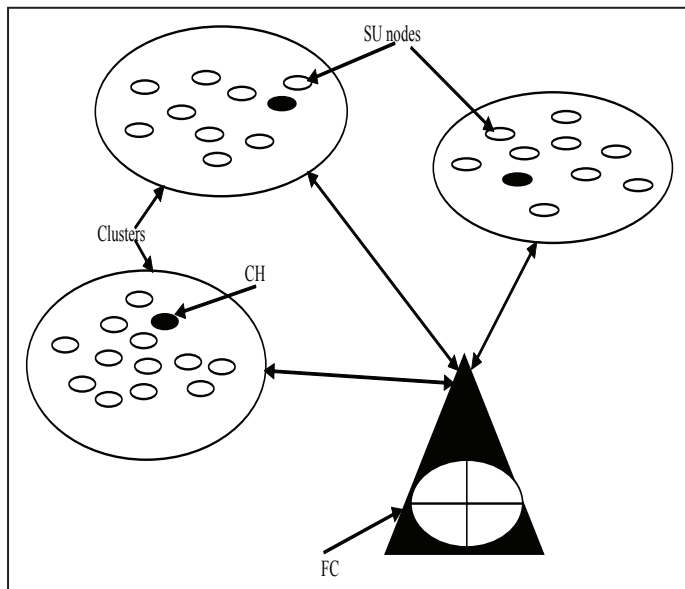


Fig. 1: Illustration of Network Model

All requests from new users are directed to the CH for authentication purposes. The details of the proposed authentication protocol are presented in sub-section A and B. It is also assumed that cluster head shared a secret key with the Fusion Centre (FC), and a shared a secret key with Base Station.

Table 1: Notations used and their Description

Notation	Description
SU	Secondary User
CH	Cluster Head
FC	Fusion Centre
$SU_i$	Secondary User identity
$C_i$	Cluster identity
$U_{id}$	Unique user identity
$P_{SU}$	Public key of Secondary User
$P_{CH}$	Public key Cluster Head
$K_{CHSU}$	Session key between CH & SU
$K_{CHFC}$	Session key between CH & FC
$N_{SU}$	Random nonce chosen by SU
$N_{CH}$	Random nonce chosen by CH
$M_{FC}$	Master key of FC
$CH_i$	Cluster Head identity
$D_s$	Location of SU in the cluster
$T_s$	Time Stamp
T	Token

#### A. Registration Phase

All the notations used in the protocol are very simple to comprehend and their descriptions are presented in Table 1.

1. To become a member of a cluster, user sends the request to its cluster head

$$SU \text{ ----> } CH: \{SU_i, P_{su}, N_{su}\}P_{CH} \quad (1)$$

2. After successful delivery of the message, cluster head must establish a secure means of communication between them. It must contact the FC to obtain a secret shared key with SU. It sends the message below to the FC, encrypted with the shared secret key between them.

$$CH \text{ ----> } FC: \{SU_i, CH_i, C_{id}, N_{SU}, D_s\} K_{CHFC} \quad (2)$$

3. FC decrypts the message with the shared secret key, generate a new shared key between SU and CH;  $K_{CHSU} = [NSU \ominus N_{PU}]$  then encrypt it with the shared key between itself and the cluster head and sends it to the cluster head.

$$FC \text{ ----> } CH: \{SU_i, CH_i, C_{id}, K_{CHSU}\} K_{CHFC} \quad (3)$$

4. Upon arrival of the message from FC to the cluster head, it extracts the shared key between itself and the joining SU using the shared key between itself and the FC. Note, this shared key between SU and CH is unique for every SU node. So, the shared key can only be received by node that possesses a secret key that correspond to the public key used to encrypt the message.

$$CH \text{ ----> } SU: \{SU_i, N_{su}, K_{CHSU}\} P_{SU} \quad (4)$$

**B. Token Generation**

A registered user must possess a token to begin exchanging messages with the destination node (BS). The token is used by the BS to determine the legitimacy of the users.

- The User sends a message encrypted with a session key shared between itself and the cluster head to the cluster head.

$$SU \text{ -----} CH: \{SU_i, N_{SU}\}K_{CHSU} \quad (5)$$

- CH receives the message encrypted with the session key shared with the SU. CH decrypts the message using its own key and extract the identity of the sender. This verifies the sender because only the user with such identity shared the session key used in encrypting the message. CH then encapsulates a package encrypted with the session key shared between itself and the FC. Then send the message to FC.

$$CH \text{ -----} FC: \{SU_i, P_{SU}, N_{SU}, C_{id}\}K_{CHFC} \quad (6)$$

- The FC decrypts the arrived message, generates a token, encrypt it with its secret key and sends it to CH. Timestamp (T) is used to estimate the delivery time from the moment SU seizes an opportunity to use a channel and starts transmitting. T is used to verify the freshness of the message.

$$FC \text{ -----} CH: \{SU_i \{T\} M_{FC}\}K_{CHFC} \quad (7)$$

Where  $U_{id} = K \Theta (SU_i \parallel N_{SU})$   
 $T = \{U_{id}, P_{SU}, N_{SU}, C_{id}, T_{SU}\} M_{FC}$

- The CH decrypts the message and encrypts the received token with its shared key between itself and the SU and send it to SU for which it was intended to. Note that, because the token cannot be decrypted by any user including the cluster head, the FC attached the SU's identity to allow the CH to identify who owns the token among its members.

$$CH \text{ -----} SU: \{\{T\} M_{FC}\}K_{CHSU} \quad (8)$$

- The received message at the SU's side can be decrypted to extract the licence (token) to participate in the communication process with the destination node.

$$SU = [\{U_{id}, N_{SU}, P_{SU}, C_{id}, T_{SU}\} M_{FC}] \quad (9)$$

Now, SU has been registered successfully as a member of the cluster, authenticated at the cluster level, and assigned a pass phrase (token) to be used when communicating at BS level. This token assumed to have been communicated to the base station by the FC. The equivalent of this protocols is represented in sequence diagram for easy understanding in Fig. 2.

**C. Authentication Phase**

The registered cluster member initiates the communication process between itself and the Base Station by sending its unique assigned token.

$$SU \text{ -----} FC: \{SU_i \{U_{id}, N_{SU}, P_{SU}, CH_i, T_{SU}\} M_{FC}\}K \quad (10)$$

After the received of the message by BS. It decrypts the message and verify the parameters contained. It checks the identity of the sender, checks the validity period of the token (this is done by checking the timestamp). When the token passes the verification

check, the BS sends an acknowledgement (ACK) back to the SU, and the communication commences between the two. However, in order to ensure only the legitimate user gets the message (ACK), the message is encrypted with the recipient public key, so that the node that possessed the secret key can decrypt the message.

$$BS \text{ -----} SU: \{ACK\}P_{SU} \quad (11)$$

It implies that,  $SU = [ACK]$

Fig. 2 recaps the authentication processes presented.

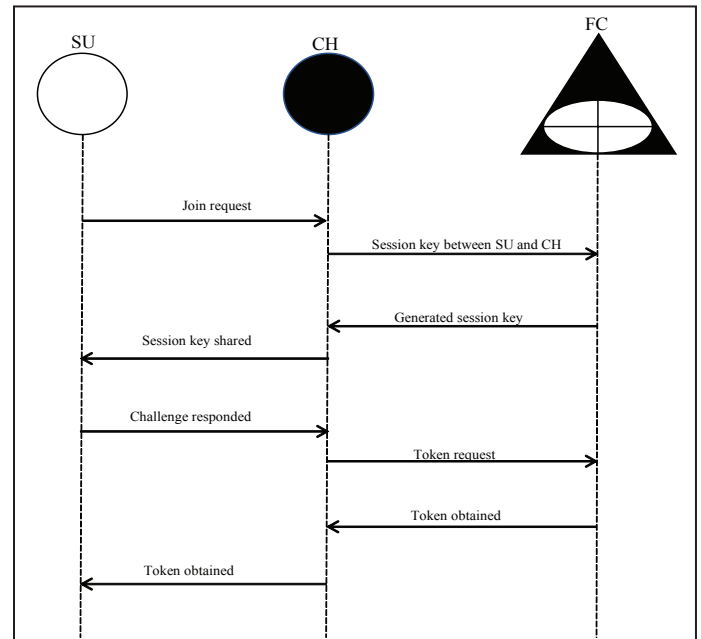


Fig. 2: Sequence Diagram of the Proposed Authentication Protocol

**IV. Security Analysis**

Our proposed authentication protocol for Cognitive Radio Network is resilient to the following attacks

**A. It is expected to withstand user impersonation attack.**

For an adversary to impersonate a legitimate user, the secret token must be known. Assuming the attacker was able to successfully intercept the token, however, it is impossible to break the token to get the user identity  $[U_{id}]$  because of the encryption key used to protect the token which is only known by FC;  $U_{id}$  is however composed of the chosen user identity  $[S_{U_i}]$  XORed with the key (K) from the FC. Additionally, attacker may attempt to change the user identity which is appended to the token but the knowledge of how  $U_i$  is generated will make it the attack difficult.

**B. The proposed protocol provides a secured means to protect session key compromise.**

Let assume there is a compromised member within the cluster whose target is to hijack the session keys of other members. Our proposed protocol shows the impossibility of launching such an attack because the attacker must first of all know the nonce chosen by the targeted member; must also know the key used to generate the session key, which also prove to be very difficult because only the FC has the key; and above all, the session key is transmitted securely protected by targeted member's public key.

### C. Prevent Denial of Service (DoS) attack.

Our proposed protocol is expected to mitigate the threat of launching DoS attack that might arise as a result of cooperative registration request from SUs to the BS as depicted in figure 3. Therefore, the protocol provides a lightweight and secured authentication at the lower level. In a nutshell, FC serves as the firewall to all authentication requests, only authenticated users have exclusive permission to communicate to the BS.

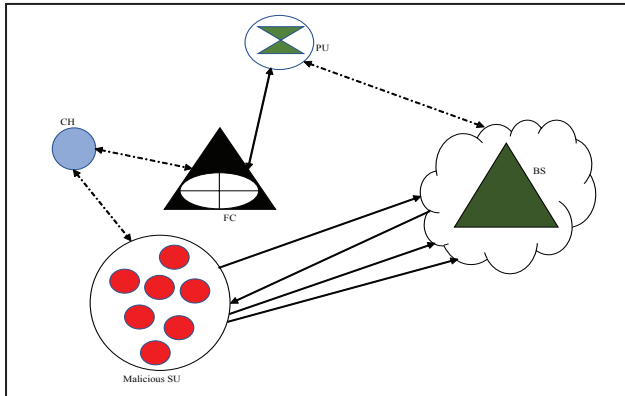


Fig. 3: Dos attack on BS

### V. Conclusion

In conclusion, we presented a simple and efficient authentication protocol for cognitive network users that ensures the preservation of their privacies was presented. The protocol can be used to protect the networks against primary user emulation attack, detecting replay attacks, and mitigation of service disruption by fraudulent request at to BS node. The study has also shown that SU behaviour and fraudulent activities can be detected at cluster level thereby giving full chances of exploring BS service by PU. Availability of unused spectrum band are control by FC and CH. Future work is concentrating on protocol implementation using Generative Adversarial Network (GAN).

### References

- [1] Ejike, C., D. Kouvatsos, "Combined sensing, performance and security trade-offs in cognitive radio networks", In Network Computing and Applications (NCA), 2017 IEEE 16th International Symposium on. 2017. IEEE.
- [2] Ho-Van, K., et al., "Security performance analysis of underlay cognitive radio systems under interference from primary network and channel information inaccuracy", In Advanced Technologies for Communications (ATC), 2017 International Conference on. 2017, IEEE.
- [3] Das, M.L., "Two-factor user authentication in wireless sensor networks", IEEE transactions on wireless communications, 8(3), pp. 1086-1090, 2009.
- [4] Wong, K.H., et al., "A dynamic user authentication scheme for wireless sensor networks. in Sensor Networks, Ubiquitous, and Trustworthy Computing, 2006. IEEE International Conference on. 2006. IEEE.
- [5] Jan, M., et al., "PAWN: A payload-based mutual authentication scheme for wireless sensor networks", Concurrency and Computation: Practice and Experience, 29(17), 2017.
- [6] Jiang, Q., et al., "Lightweight three-factor authentication and key agreement protocol for internet-integrated wireless sensor networks", IEEE Access, 5: pp. 3376-3392, 2017.
- [7] He, D., et al., "Anonymous authentication for wireless body area networks with provable security", IEEE Systems Journal, 11(4): pp. 2590-2601, 2017.

- [8] Li, X., et al., "A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments", Journal of Network and Computer Applications, 103: pp. 194-204, 2018.
- [9] Wu, F., et al., "An improved and anonymous two-factor authentication protocol for health-care applications with wireless medical sensor networks", Multimedia Systems, 23(2): pp. 195-205, 2017.
- [10] Das, A.K., "A secure and effective biometric-based user authentication scheme for wireless sensor networks using smart card and fuzzy extractor. International Journal of Communication Systems, 30(1), 2017.
- [11] Shen, J., et al., "A lightweight multi-layer authentication protocol for wireless body area networks", Future Generation Computer Systems, 78: pp. 956-963, 2018.
- [12] Jung, J., et al., "Efficient and security enhanced anonymous authentication with key agreement scheme in wireless sensor networks", Sensors, 17(3): pp. 644, 2017.
- [13] Das, A.K., et al., "A dynamic password-based user authentication scheme for hierarchical wireless sensor networks", Journal of Network and Computer Applications, 35(5): pp. 1646-1656, 2012.
- [14] Shah, M.A., et al., "A novel symmetric key cryptographic authentication for cooperative communication in cognitive radio networks", In Automation and Computing (ICAC), 2013 19th International Conference on. 2013. IEEE.
- [15] Nesargi, S., R. Prakash, "MANETconf: Configuration of hosts in a mobile ad hoc network", In INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE. 2002. IEEE.
- [16] Chandrashekar, S., L. Lazos., "A primary user authentication system for mobile cognitive radio networks", In Applied Sciences in Biomedical and Communication Technologies (ISABEL), 2010 3rd International Symposium on. 2010. IEEE.
- [17] Jain, S., M. Hussain, R.M. Garimella, "Primary user authentication in cognitive radio network using authentication tag", In Recent Advances and Innovations in Engineering (ICRAIE), 2016 International Conference on. 2016. IEEE.
- [18] Khasawneh, M., A. Agarwal, "A secure and efficient authentication mechanism applied to cognitive radio networks", IEEE Access, 5: pp. 15597-15608, 2017.



**Aliyu Abubakar** is Lecturer II with Dept. of Mathematics, Gombe State University Nigeria. He has a first class BSc Honours degree in Computer Science from Gombe State University Nigeria in 2012 and MSc degree in Cyber Security at faculty of Engineering & Informatics from University of Bradford, United Kingdom in 2015. He is a student member of Institute of Electrical and

Electronics Engineers (IEEE) and currently pursuing his PhD degree in Visual Computing at University of Bradford UK. His research interest includes Computer Vision, Image Analysis and Machine Learning.