Digital Signature-based Secure Communication in Cognitive Radio Networks

Sazia Parvin, Farookh Khadeer Hussain
Digital Ecosystems & Business Intelligence Institute,
Curtin University of Technology, Australia
Perth, Australia
sazia.parvin@postgrad.curtin.edu.au, Farookh.Hussain@cbs.curtin.edu.au

***Abstract*— Over the past few years, Cognitive Radio (CR) has been considered as a demanding concept for improving the utilization of limited radio spectrum resources for future wireless communications and mobile computing. Since the member of Cognitive Radio Networks may join or leave the network at any time, the issue of supporting secure communication in CRNs becomes more critical than the other conventional wireless networks. This work thus proposes digital signature-based secure communication in CRNs. Need more to describe. The security analysis is analyzed to guarantee that the proposed approach achieves security proof. (Abstract)**

Keywords-Trust; primary user; secondary user; authentication; secure; cognitive radio networks; raio.(key words)

I. INTRODUCTION (HEADING 1)

With the rapid development of wireless applications, Cognitive Radio (CR) has offered a promising concept for improving the consumption of limited radio spectrum resources for future wireless communications and mobile computing. The primary objective of Cognitive Radio Networks is to scan the spectral band and identity free channels which will be used for opportunistic transmission. Sometimes several frequency bands are not used according to their maximum level. These under-utilized areas are known as spectrum holes or white spaces [1]. So, CRs offer a solution for the scarcity of spectrum by reusing the underutilized spectrum. National regulatory bodies like the Federal Communications Commission (FCC) assign spectrum for particular types of services that are then licensed to bidders for a fee [2]. CR pioneered by Mitola [3] from software defined radio (SDR) was originally considered to improve spectrum utilization. CR on the other hand sits above the SDR and is the "intelligence" that lets an SDR determine which mode of operation and parameters to use. We can get an overview of CR functionalities from Haykins's definition of cognitive radio [4]: "Cognitive radio is an intelligent wireless communication system that is aware of its surrounding environment (i.e., outside world), and uses the methodology of understandings-by-building to learn from the environment and adapt its internal states to statistical variations in the incoming RF stimuli by making corresponding changes in certain operating parameters (e.g., transmit power, carries-frequency, and modulation strategy) in real time, with two primary objectives in mind: highly reliable communication whenever and wherever needed, efficient utilization of the radio spectrum". CR has two main properties: Artificial Intelligence (AI) and Dynamic Spectrum Access (DNS) [5]. AI involves reasoning and learning. This gives CR its 'intelligent' characteristics and allows it to learn about its changing environment. DNS is the processes involved in getting a CR to detect and occupy a vacant spectrum. It involves spectrum sensing, spectrum management, spectrum mobility and spectrum sharing [5]. The Cognitive Radio Networks (CRNs) consists of various kinds of communication systems and networks, and can be viewed as a sort of heterogeneous networks. There are two broad classes of users in CR, the primary user (PU) is a licensed user of a particular radio frequency band and the secondary user (SU) is unlicensed user who cognitively operate without causing harmful interference to the primary user [6]. Since cognitive radios can adapt to their environment and change how they communicate, it is very crucial that they select optimal and secure means of communications. Cognitive radio networks operate on wireless media. Compared to wired network, the nature of wireless network makes the security vulnerability unavoidable. In wireless network, signal has to be transmitted through an open media without real connection. That is to say, the data might be eavesdropped and altered without notice; and the channel might be jammed and overused by an adversary [7]. In addition, the unique characteristics of CRNs make security more challenging. Still there are some crucial issues which have not been investigated in the area of security for cognitive radio networks. When a CR node initially tries to form a CRN or tries to connect a node to join an existing CRN it is practically impossible to implement conventional security functions as CRNs have resource constraints such as power and memory. Typical public key infrastructure (PKI) scheme which achieves secure routing and other purposes in typical ad-hoc networks is not enough to guarantee the security for CRNs under limited communication and computation resources. Therefore, a trusted mechanism is necessary in CRNs, while authentication is a part of trust along with other technical or non-technical factors. To ensure smooth operation of CRN to support ubiquitous computing, trust forms the foundation in security platform of CRNs. However, trust for CRNs is quite different from other wireless scenarios and in other areas of computing trust. Trust is critical in CRNs operation and beyond security design since security usually needs communication

overhead advance. So in this paper, we propose a trust based authentication mechanism for secure communication in cognitive radio networks.

The organization of this paper is as follows: In section 2, related works is reviewed. In section 3, our proposed scheme is described. In section 4, we show the security proofs of our proposed scheme. We conclude the paper in section 5 including future remarks.

II. Related Works

To ensure smooth operation of CRNs to support ubiquitous computing, establishing trust for CRNs is an open and challenging issue. Trust has been widely mentioned in the existing literatures in relation to trusted computing and web computing, ad hoc networks and even social science [8]. However, trust for CRNs is completely different from all of these scenarios. Trust is critical in CRNs operation and beyond security design, as security usually needs communication overhead in advance. The authors [9] describe the trust in CRN as an essential part in the following phases:

- A cognitive radio senses a spectrum hole and to dynamically access the spectrum for transmission requires "trust" from originally existing system (i.e. primary system) and regulator, even without creating interference to PS.
- A cognitive radio may want to leverage another existing cognitive radio to route its packets, even though another CR is not the targeted recipient terminal. It requires "trust" from another CR.
- A cognitive radio can even leverage PS to forward its packets to realize the goal of packet switching networks. It needs "trust" from the PS, not only at network level but also in service provider

A Markov chain based trust model has been proposed for analyzing trust value in distributed multicasting mobile ad hoc networks [10]. They also proposed the approach for selecting the Certificate Authority (CA) and Backup CA (BCA) [10]. The impact of trust model in CRNs is discussed briefly in [11]. The authors in [12] integrated trust and reputation for the threat mitigation of Spectrum Sensing Data Falsification (SSDF) attack on CRNs. However, they did not propose any trust modeling for CRNs. The authors suggested potential ways for incorporating trust modeling to CRNs including identity management, the trust building process and possible mechanisms for disseminating the trust information [11]. Furthermore, no experimental results were established for these discussions. A trust aware model was proposed for spectrum sensing in CRNs but the authors fail to evaluate the system [13]. A Trust Value Updated Model (TVUM) is proposed in layered and grouped adhoc network for ensuring the authentication [14]. In this paper, we propose a trust based authentication mechanism for secure communication in CRNs. We also propose the trust table update procedure when one new CR node wants to join the network or leave the network. We here discuss how this joining and leaving event impacts on the trust table in CRNs.

III. Secure Communication in Cognitive Radio Networks

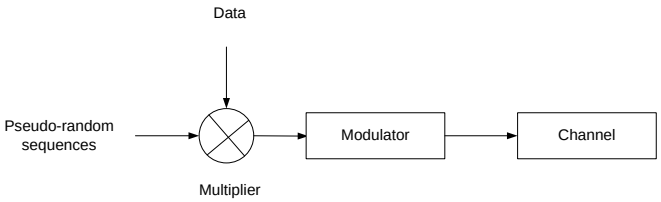
To ensure the secure communication of CRNs is a big challenging issue. Like all other wireless networks, some techniques are used to make the communication insecure from the hacker side. In this section, we want to discuss some possible techniques that are required for secure communication in CRNs.

A. Existing solutions for secure communication

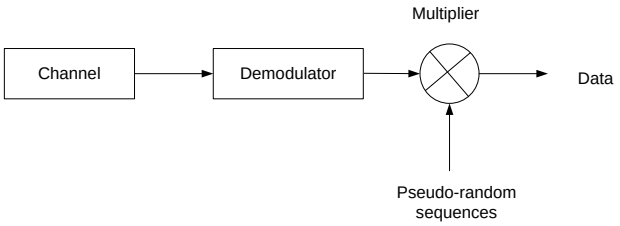
Many existing solutions which are being used for other wireless communication can be easily applied to the cognitive radio technology with a view to provide a secure communication against different types of security threats. Spread spectrum modulation [15] is one of them. Basic encryption technologies such as public key and private key encryption can be easily applied to CRNs for the security purpose.

B. Spread spectrum modulation

We discuss the spread spectrum modulation here from [15]. According to the standard definition [15], " Spread spectrum (SS) is a means of transmission in which a signal occupies a bandwidth in excess of the minimum necessary to send the information: the band spread is accomplished by means of a code which in independent of the data, and synchronized reception with the code at the receiver is used for de-spreading and subsequent data recovery". At the transmitter side, at first the data signal is multiplied with a pseudo-random sequence known as spreading code and then a modulation technique is applied as shown in the figure X . At last, the modulated data is transmitted through the channel.



At the receiver side, the received signal is checked to remove noise. If there exists any noise associated with the signal, the noise is removed by applying noise cancellation techniques [] and then the signal is demodulated. The demodulated signal is multiplied with the pseudo-random sequence to obtain the final signal as shown in the figure X. Spread spectrum modulation technique can be further improved for making a reliable and secure communication environment.



C. Encryption Techniques

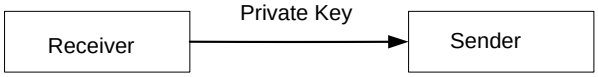
Encryption is used to protect data in transit and keep data hidden from the malicious users to maintain security. Different types of encryption techniques [] such as: symmetric and asymmetric have been proposed to maintain security. In a symmetric encryption technique, , for example data being transferred via networks (e.g. the Internet, e-commerce), mobile telephones, wireless microphones, wireless intercom systems, Bluetooth devices and bank automatic teller machines. A symmetric encryption technique is known as the private key encryption algorithm. In this algorithm, only a single key is used for the secure communication between sender and receiver. In this technique, both sender and receiver have a private key and they share the key before the communication starts between them. Some techniques such as RSA, Elliptic, and SHA etc use symmetric encryption algorithm.

Asymmetric encryption technique is known as public key encryption. RSA, ElGamal, Rabin and Elliptic curve cryptosystems are well known public key encryption techniques.

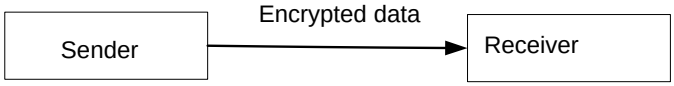
Private Key Cryptography:

In private key cryptography techniques, the data is encrypted with the private key of the receiver and the receiver decrypts the data using the same private key. So, there are two stages involved in private key cryptography technique.

Stage 1: Receiver sends its private key to the sender.



Stage 2: Sender encrypts the data with the receiver's private key and sends back to the receiver.



So, the encryption and decryption algorithms of private key cryptography satisfy the following properties:

$$M = D_{PR}[E_{PR}[M]]$$

Here, M is a message which consists of different letters.

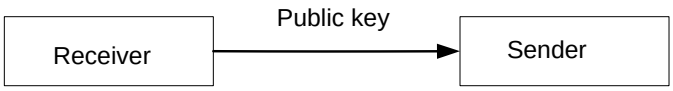
E and D are encryption and decryption algorithms respectively.

PR is private key.

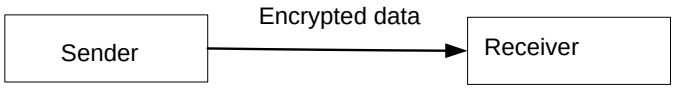
Public Key Cryptography:

In public key cryptography, both sender and receiver have a set of public and private keys. These public keys are transmitted to other members of the network before the data transmission starts. Sender also receives the receiver's public key. So, sender encrypts the data with public key of the receiver and sends to receiver. The receiver decrypts the data with its own private key. So, there are three stages involved in public key cryptography technique.

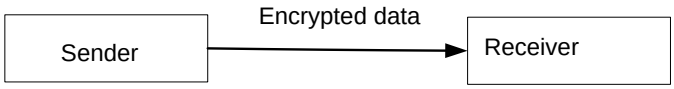
Stage 1: Receiver sends its public key to the sender.



Stage 2: Sender encrypts the data with receiver's public key and sends it to the receiver.



Stage 3: Receiver receives and decrypts the data with its own private key.



So, the encryption and decryption algorithms of private key cryptography satisfy the following properties:

$$M = D_{PU}[E_{PR}[M]]$$

$$M = D_{PR}[E_{PU}[M]]$$

Here, M is a message which consists of different letters.

E and D are encryption and decryption algorithms respectively.

PR is private key which is kept secret and PU is public key which is revealed over the network.

Private Key Vs Public Key Encryptions:

Though the private key encryption algorithms are fast but public key encryption techniques are more reliable from the security perspective. Public key encryption is used in those applications where it is needed to provide confidentiality such as digital signature and secret keys. Digital signature is one of the applications of Public Key Encryptions. Public key encryption can be used as digital signature in the following ways:

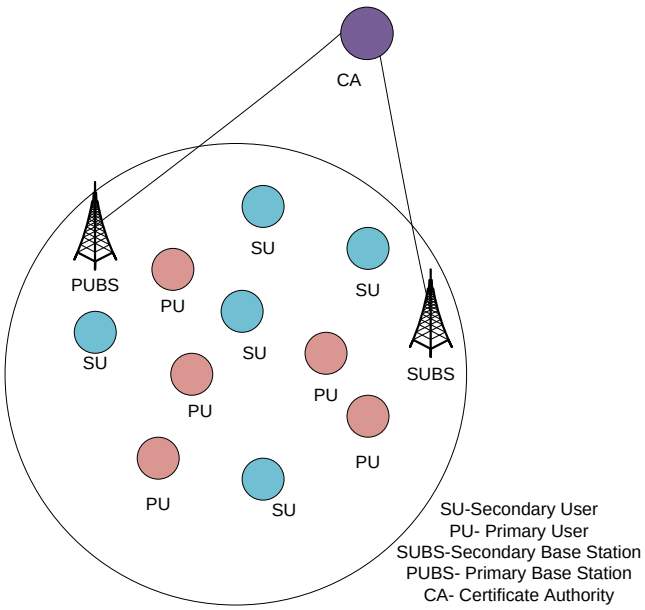
Stage 1: the sender signs message using its private key and sends to the receiver.

Stage 2: the receiver receives message and verifies it using the sender's public key.

In this process, as the sender signs the message using its private key, so it is not computationally feasible to others to sign the sender's message.

IV. PROPOSED SCHEME

In this section, we proposed digital signature for secure communication in cognitive radio networks. We proposed digital signature for secure communication in CRNs as digital signature posses all the features of public key encryption as well as it has some technical advantages such as it is light weight, the key management is not complex and it can easily detect if any unwanted accidental asynchrony occurs in secondary users.



In our system architecture, there are five entities:

1. Primary User (PU)
2. Primary User Base Station (PUBS)
3. Secondary User (SU)
4. Secondary User Base Station (SUBS)
5. Certificate Authority (CA)

Certification Authority's Activities:

In our architecture, a certification authority is an entity which is connected to the PUBS and SUBS through wired connection in the network. Certificate authority is responsible to maintain all public keys used by primary users used in the network. If any key is changed, the CA will update the key as soon as possible.

Primary User's Activities:

The primary user uses key generation algorithm [] to generate a pair of private and public keys. After generating the public keys, the keys are sent to the CA and the corresponding CA securely registered the public keys of primary users.

The primary user generates digital signature, by encrypting its identity and the time stamp with its private key.

$$Digital\ Signature, S = E_{PR}(ID \| TS)$$

Here ID is primary User's identity and TS is the timestamp.

Now, the primary user signed the message and transmitted over the wireless media.

$$Message_{signed} = Message \| S$$

The Primary User sends this singed message for its purpose over the wireless medium.

If the primary user changes its private and public keys, it must inform the CA through the PUBS about the new public key. Then the new public keys are securely registered with the CA.

Primary User Base Station's Activities:

If there is any change of primary user's public key, the PUBS is informed. Then the PUBS sends the new public key to CA and the CA securely registers the new public key.

Secondary User's Activities:

The secondary user uses sensing algorithm to detect the presence of primary user's transmission. If the transmission is detected, then the secondary user decodes the primary user's signed message. After decoding the message, the message is detached from the signature. Primary users transmit these stored signatures to the Secondary User Base Station through an established control channel.

Secondary User Base Station's Activities:

As Secondary User Base Station is connected to the CA, so it can securely obtain the identity and public keys of the primary user from the CA. Whenever, the secondary users detect transmissions with signatures during their sensing periods, the corresponding signatures are transmitted to the secondary base

station []. The Secondary User Base Station maintains only one copy of signature that is received from the secondary user. Then the Secondary User Base Station decrypts the signature with the Primary user's public key.

$$ID \parallel TS = D_{PU}(S)$$

The Secondary User Base Station has the full list of all primary users' identities which is obtained from the CA. After decrypting the primary user's identity, the Secondary Base Station will check whether this identity matches with one of the primary user identities in the list or not. It also checks the validity of the time stamp. To check the time stamp, the base station selects a network time delay, δ. If the difference between the decrypted time stamp and the base station's current time is δ and the base station gets the primary user's identity in the list, then the base station is assured about the validity of the time stamp as well as the presence of a licensed primary user. The whole secure communication approach by digital signature can be stated by the following algorithm:

Input: CRN, Key generation Algorithm, Time Stamp, network time delay, δ

Output: Secure Communication

Procedure:

1. Establish a wired connection with CA to both PUBS and SUBS.
2. Primary user will use key generation algorithm to compute private and public key.
3. Primary user will send public key to CA through PUBS.
4. Primary user will produce digital signature by encrypting its identity with time stamp.

   $Digital\ Signature, S = E_{PR}(ID \| TS)$
5. Primary user sign message with its signature and transmit over wireless media.

   $Message_{signed} = Message \parallel S$
6. Secondary user will decode the signature and sends to SUBS.
7. SUBS will decrypt the signature with primary user's public key received from the CA and discovers primary user's id and time stamp.

   $ID \parallel TS = D_{PU}(S)$
8. **If** $(\delta = SUBS's\ current\ time - Time\ Stamp)$ **then**

   If ID exists in the Primary User's identity list **then**

   There is presence of licensed primary user.

   Else

   No presence of licensed primary user.

Else

No presence of licensed primary user.

V. Security Proofs (Need to Improve)

The proposed scheme is secure as long as malicious entity is unable to get access in the CRN. The following services ensure the security proofs of our proposed scheme:

A. Authentication

This service provides the assurance that the requesting entity is the one that it claims to be. We propose authentication by establishing trust value of every CR nodes which is stored to CA. Whenever a SU wants to access the PU's free spectrum band, the SU shows its good manners in order to get the spectrum access. Then the PU accesses the trust table to CA and then the PU takes decision whether the SU can get access to the free spectrum or not. So we propose a trust based authentication scheme for secure communication in CRN.

B. Availability

This service ensures that the desired system or system resources are accessible and usable upon demand by an authorized entity, according to performance specification for the system [9]. We propose availability here by establishing first backup of CA and second backup of CA. The trust table which contains the trust information of every node is stored to CA. So, in our proposed approach, CA is executing a major role. If the CA becomes malicious or attacked by any hacker, then first backup of CA will take the role of main CA. In such a case, the backup CA assumes the role of Primary CA. From amongst the available nodes, based on their trust value and reputation, a backup CA is chosen. So in our proposed approach, we are ensuring the service availability in terms of security.

C. Non-repudiation

This service provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication [9]. In our proposed scheme, when one new CR node wants to join and leave the network, the shared key is securely transmitted to the new entity and revoked from the leaving entity. The security is ensured here by secure joining to the network or leaving from the network. If the CR node maintains the normal joining or leaving event, the trust value is incremented by one which ensures the security purpose. If the CR node follows the abnormal joining or leaving event, the trust value is decremented by one which is indicated that the CR node might be malicious entity.

D. Access Control

This service prevents the unauthorized use of resources [9]. In our proposed scheme, the authenticity is ensured by

checking the trust value in the trust value in CA. So if one CR node has low value and wants to get access to the network, it is not allowed.

E. Dara Integrity

This service provides the assurance that data received are exactly as sent by an authorized entity. In our proposed scheme, we are using trust table in CA in two formats. One is Public which could be accessed by any CR member in the network, and the other one is Private. Only CA has access to the Private part of the trust table. CA always compares the private trust value with the public trust value. If any discrimination appears, then the CR node whose trust value is changed or by whom the trust value is changed is detected as a malicious node. Later on, the malicious nodes are listed in the blacklist and their own trust value is decremented as well.

VI. CONCLUSION

In cognitive radio networks, some non-compliant Cognitive Radio users may create interference by accessing the primary user's available spectrum band. Such malicious users can seriously break down the whole network performance possibly resulting in the collapse of the CRN. It is critical to consider that Cognitive Radio Netwoks operate under resource constraints. As CRNs has dynamic hebaviours, the member of Cognitive Radio Networks may join or leave the network at any time. So the issue of secure communication in CRNs becomes more important than the other conventional wireless networks. So in this paper, we propose trust based authentication scheme for secure communication in CRNs. This secure authentication reduces the relative calculating overheads and communication cost. This work thus proposes a secure trust based authentication approach for CRNs. Moreover, we propose security proof of our proposed scheme. In this paper, we overlook the biasing between the CA and other nodes, so the some specific node's trust value will be always higher. In the future work, we will focus on the trust by biased nodes in CRNs.

REFERENCES

[1] Chaczko, Z., et al., *Security threats in Cognitive Radio applications*, in *Intelligent Engineering Systems (INES), 2010 14th International Conference on*. 2010. p. 209-214.

[2] O.Leon, J.H. Serrano, and M.Soriano, *Securing Cognitive Radio Networks.* International Journal of Communication Systems, 2010. **23**(5): p. 633-652..

[3] Mitola, J., *Cognitive Radio: An Integrated Agent Architecture for Software Defined Radio. PhD thesis,*, in *Royal Institute of Technology (KTH).* 2000.

[4] S.Haykin, *Cognitive radio: brain-empowered wireless communications* IEEE Journal on Selected Areas in Communications, 2005. **23**(2): p. 201-220.

[5] Zhang, Y., G. Xu, and X. Geng, *Security Threats in Cognitive Radio Networks*, in *Conference on High Performance Computing and Communications*. 2008.

[6] Mathur, C.N. and K.P. Subbalakshmi. *Digital Signatures for Centralized DSA Networks*. in *Consumer Communications and Networking Conference, 2007. CCNC 2007. 4th IEEE*. 2007..

[7] X. Zhang, C.L., *The security in cognitive radio networks: a survey*, in *International Conference On Communications And Mobile Computing* 2009, ACM: Leipzig, Germany p. 309-313.

[8] Naldurg, P. and R.H. Campbell. *Dynamic Access Control: Preserving Safety and Trust in Network Defense Operations*. in *Proceedings of the Eighth ACM Symposium in Access Control Models and Technologies (ACM SACMAT 2003)*. 2003

[9] K.-C. Chen , Y.-J.P., N. Prasad ,Y.-C. Liang ,S. Sun and *Cognitive radio network architecture: part II -- trusted network layer structure*, in *Conference On Ubiquitous Information Management And Communication* 2008, ACM: Suwon, Korea p. 120-124

[10] Ben-Jye, C., et al. *Markov Chain-Based Trust Model for Analyzing Trust Value in Distributed Multicasting Mobile Ad Hoc Networks*. in *Asia-Pacific Services Computing Conference, 2008. APSCC '08. IEEE*. 2008.

[11] T.C.Clancy, N.G., *Security in Cognitive Radio Networks: Threats and Mitigation*, in *Cognitive Radio Oriented Wireless Networks and Communications, 2008. .* 2008. p. 1-8

[12] R.Chen, J.-M.P., Y. T. Hou,J. H. Reed, *Toward secure distributed spectrum sensing in cognitive radio networks*, in *IEEE Communications Magazine Special Issue on Cognitive Radio Communications*. 2008. p. 50-55

[13] Parvin, S., et al. *Towards Trust Establishment for Spectrum Selection in Cognitive Radio Networks*. in *Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on*. 2010

[14] Yang, Y.-t., et al. *A Novel Authentication Scheme Based on Trust-value Updated Model in Adhoc Network*. in *Computer Software and Applications Conference, 2007. COMPSAC 2007. 31st Annual International*. 2007.

[15] Sanyal, S., R. Bhadauria, and C. Ghosh. *Secure communication in cognitive radio networks.* in *Computers and Devices for Communication, 2009. CODEC 2009. 4th International Conference on*. 2009.