Symmetric Cryptography and Eigen values Based Spectrum Sensing in Cognitive Radio Networks

[1]Sugandh Gupta
[1]Assistant Professor, Department of Electronics and Communication,
Shamli Institute of Engineering & Technology
Shamli, India
sugandhaquarius@gmail.com

[2]Sandip Vijay
[2] Professor, Department of Electronics and Communication
Dehradun Institute of Technology
Dehradun, India
vijaysandip@gmail.com

***Abstract*—Cognitive Radio allows opportunistic spectrum access (OSA) of licensed frequency bands by unlicensed users so as to reduce spectrum scarcity led by the increasing market demands. Spectrum sensing is an essential mechanism for a cognitive radio system. Therefore attention should be given towards the security aspects of spectrum sensing in cognitive radio. This paper analyses the two proposed methods for spectrum sensing, one of which is based on symmetric cryptography and one way functions and other is based on Eigen values.**

Keywords—**Cognitive Radio (CR), primary user (PU), secondary user (SU), maximum eigenvalue (MEV), Authentication, Cooperative sensing.**

I. INTRODUCTION

The need for a flexible and robust wireless communication is becoming more evident in recent times. The requirement of different technologies and market demand leads to spectrum scarcity and unbalanced utilization of frequencies [1]. One promising solution to such problems is the Cognitive Radio. It allows the usage of licensed frequency bands by unlicensed users during the time when they are empty [2]. In this scheme, those who own the license to use the spectrum are referred to as primary users(PU), and those who access the spectrum opportunistically are referred to as secondary users(SU). It has an intelligent layer that performs the learning of environment parameters in order to achieve optimal performance under dynamic and unknown situations. Spectrum Sensing i.e. checking the frequency spectrum for empty bands forms the foremost part of the cognitive radio. It helps one to determine the empty frequency bands in the spectrum and also finds out the state of the channel over which transmission is to occur. Cooperative sensing is preferred over single user sensing where a fusion center is employed and decision from a number of SU's is taken and merged at the fusion center by data fusion techniques to reach a final decision, whether a primary user is operating in that particular frequency band or not. CR terminals form self-organizing networks capable of detecting vacant spectrum bands but performing reliable spectrum sensing is a difficult task. Wireless channels can suffer fading, thus provoking the hidden node problem in which a secondary user fails to detect a primary transmitter. The most important challenge for a CR is to identify the presence of primary users, and, for this reason, secondary users must be significantly more sensitive in detecting primary transmissions than primary receivers. There are two different techniques of cooperative sensing; Hard and soft cooperative sensing. When hard cooperation is employed, radios only exchange their final decision: primary user detected or not detected. On the other hand, soft decision means that radios exchange their local measures and/or test statistics with each other.

To perform cooperative sensing securely, the cooperative system should identify the users that participate in the sensing process, authenticate their claims, and weigh up their contribution to the final decision based on their reputation or probability of successful detection. This paper analyses two protocols. The protocol based on cryptography and one-way functions focuses on the mechanisms required to identify the users and authenticate their sensing results and the other based on eigen values employ revised fusion rules and double thresholds to increase the detection performance.

The protocol based on cryptography and one way function enables the secure authentication of hard decision sensing reports in an efficient way by the use of hash functions. It is divided into three phases. The first phase is the registry of users; the second one the sensing assignment; and finally the third phase is the collection of sensing results.

The protocol based on eigen values aims at the calculation of maximum eigen value which proves to be very effective to detect the presence of PU in given frequency band an also identifies the untrusted users.

II. CRYPTOGRAPHY

The protocol is designed for hard cooperation schemes, as they ensure that the amount of information sent through the network is minimal. The proposed protocol is based on hash functions an symmetric keys. Now the main challenge lies in how to distribute and manage the keys among the users. A

ISBN: 9788175157538

public key infrastructure (PKI) approach is used to initialize the CR network. The fusion centre holds a certificate that is (Web, public directory, etc.) and the users must know and be able to validate it. Likewise, users must hold a valid certificate from a recognized Internet Certification Authority (CA).

A. *Protocol Phase 1*

In the first phase, the user contacts the fusion centre (which can be, for instance, the base station) and asks permission to join the cognitive radio network. Identification keys are taken from a two-dimensional key chain consisting of a high-level (primary) chain and multiple low-level (secondary) chains. Besides, shecommits to a two-dimensional key chain by attaching the top value of the high-level chain in the request. This process requires mutual authentication using digital signatures. At this point, the fusion centre decides whether or not to accept the user into the network. The following are the detailed steps carried out during this phase.

- User U chooses a random number V_N and prepares a high level chain of length N, where N is chosen by the user according to its memory resources.
- U sends the top value of her chain V_0 to the fusion centre FC in a digitally signed message. The signature is computed using U's private key $pv\ k_u$. She also includes information about her identity I d_u (i.e. the unique identifier of her public key certificate).

$$Join\,\mathrm{Re}\,q = \left\{V_0, Id_u, sign_{pvk_u}\left(V_0, Id_u\right)\right\}$$

- FC verifies the signature received from U using U's public key pb k_u .

If the signature is correct, FC decides whether or not to accept U into the network. This decision will be based, for example, on the reputation earned by U in previous processes. The implementation of these mechanisms is out of the scope of this paper. If user U is accepted in the network, FC stores identity I d_u , her MAC-layer address and her top chain value V_0 in a table in the sensing phase to identify the node), and her top chain value V0 in a table paper and style the text.

B: Protocol Phase 2

In the second phase, the fusion centre requests each user to sense a certain set of frequency bands by the submission of a public key digital signed message (SensReq). If users accept to sense the requested bands, they respond with a message in which they bound to a set of low-level key chains, two for each channel they are allotted. The authenticity of user's messages is ensured by made available to the users from different means

a symmetric digital signature. Symmetric digital signatures are generated using a Hash message authentication code (HMAC) function. HMACs provide message authenticity and integrity by calculating a hash of two inputs: the target message and a secret key. In our protocol, secret keys are taken from the pre-computed high-level hash chain.

C. *Protocol phase 3: Collection of local sensing results*

In the third phase, users conduct spectrum sensing using a mechanism based on the energy perceived, cyclo stationary statistics, or any other method, and make a decision whether a channel is occupied or not. These decisions designate which low-level chain has to be used to encode the sensing result of a spectrum band, from the two possible chains linked with each channel. Users publish their results using the elements of the selected low-level chains that are scheduled for the current interval. When the fusion centre receives the reports, it can verify they are authentic and integer since the legitimate user is the only one who has enough data to reveal the hash chain values associated with the present time frame. Users can only send one sensing report in each time interval. The sensing process is repeated until the FC sends a message to stop it, or until exhausting the elements of the low-level hash chain. Then, the protocol returns to the second phase and FC generates a new sensing request.

III. EIGENVALUES BASED MECHANISM

This mechanism identifies two kinds of untrusted secondary users which are called 'Always Yes' users and 'Always No' users. These untrusted secondary users can degrade detection performance greatly, especially when conventional data fusion rules are applied. To counter these threats, for the correlated primary signals [3] [4], an Eigenvalue based detection scheme with double thresholds and revised data fusion rules is proposed. Maximum Eigen values are proved to be very effective to detect the correlated primary signals and to find the untrusted users. In spectrum sensing, two probabilities are of interests which are the probability of detection (P_d) and the probability of false alarm (P_f). P_d indicates how well the PU can be protected while P_f is an error probability which happens when a PU is silent but the spectrum sensor declares the channel is occupied. Untrusted secondary users can be categorized into two cases, namely, 'Always Yes' SU and 'Always No' SU [5]. The outputs from the detector of an 'Always Yes' SU are always

ISBN: 9788175157538

above the given threshold such that this SU declares the presence of a PU all the time even when no PU is active. A main reason to make an 'Always Yes' SU is that a SU suffers from severe interference from other transmitters which operate in the neighboring channels or from some malicious transmitters which send strong signals to attack a CR network in the same operating channel purposely. simulation results show that such malicious incumbent emulation attacks can decrease the amount of available bandwidth greatly. Another, an 'Always No' SU obtains a detection value always below the given threshold such that it reports the absence of a PU even when the PU is operating on this spectrum. Deep fading and shadowing are the main factors to incur this unpleasing result. 'Always Yes' users increase P*f* but 'Always No' users decrease P*d*, as a result, these untrusted users degrade the detection performance greatly.

A. System Model

Consider a CR network with *K* samples used to perform spectrum sensing at the *i*th CR user. Then the received signals at this CR user have two hypotheses as

$$H_0 : x_i(k) = u_i(k)$$
$$H_1 : x_i(k) = (s_i(k) + u_i(k)) \quad (1)$$

where s_i represents the received PU signals by the *i*th SU and u_i is additive white Gaussian noise (AWGN) with zero mean and variance σ_u^2 respectively. H_0 means the primary user is inactive, H_1 denotes the licensed user is operating such that all secondary users working in that channel need to vacate this channel.

For the time series $x(k)$ with $k = 1,2,\ldots,K$, we can construct a Hankel matrix with $M = N - L + 1$ rows and L columns illustrated as follows:

Then **X** is an *M* X *L* matrix. Its elements can be found by substitution of $x(k)$

$X_{ml} = (m + l - 1)$, m = 1,2….M l = 1,2….L

We can obtain a covariance matrix as

$$R_r = E\{XX^T\} = E\{(S+U)(S+U)^T\} = R_s + R_u = R_s + \sigma_u^2 I_M \quad (2)$$

where **S** and **U** are the Hankel matrices from $s(k)$ and $u(k)$, and **IM** is a unit matrix with *M* dimensions. Denote α and β be the maximum eigen values of **R**r and **R**s, respectively, we have

$\alpha > 0$, $\beta > 0$ and $\alpha = \beta + \sigma_u^2$.

As a result, the maximum eigenvalue of the covariance matrix **R**r can be used to detect the PU's presence. Cooperative sensing is performed by fusing sensing results from respective CR users and making a final decision at the fusion center [6]. In general, three kinds fusion rules are often used which are AND, OR and Majority fusion rule. Assume d_i is the i_{th} decision and it can be expressed as $d_i = 1$ if H_1 is declared and $d_i = 0$ if H_0 is declared then the final decision *D* of *N* secondary users for the three fusion rules have the forms D = 1 for the following three conditions.

$\sum_{i=1}^{N} d_i \geq 1$,OR Rule

$\sum_{i=1}^{N} d_i = N$, AND Rule

$\sum_{i=1}^{N} d_i \geq \frac{1}{2} N$, Majority Rule and D=0 otherwise

Let $P_{d,,i}$ and $P_{f,,i}$ denote the probability of detection and false alarm corresponding to the i_{th} CR user, P_d and P_f be the cooperative probability of detection and false alarm, then P_d and P_f for OR fusion rules can be expressed as

$$P_d = 1 - \prod_{i=1}^{N} (1 - P_{d,i}) \text{ and } P_f = 1 - \prod_{i=1}^{N} (1 - P_{f,i}) \quad (3)$$

For AND fusion rule, P_d and P_f have the form as

$$P_d = \prod_{i=1}^{N} P_{d,i} \text{ and } P_f = \prod_{i=1}^{N} P_{f,i} \quad (4)$$

For Majority rule, these two probabilities can be represented as

$$P_d = 1 - \sum_{K=0}^{\frac{N}{2}-1} \binom{N}{K} \prod_{i=1}^{K} P_{d,i} \prod_{i=K+1}^{N-K} (1 - P_{d,i}) \text{ and} \quad (5)$$

$$P_f = 1 - \sum_{K=0}^{\frac{N}{2}-1} \binom{N}{K} \prod_{i=1}^{K} P_{f,i} \prod_{i=K+1}^{N-K} (1 - P_{f,i}) \quad (6)$$

IV. DOUBLE THRESHOLDS AND REVISED FUSION RULES

The basic idea of our scheme is to partition all *N* CR users into three groups according to the maximum eigen values of all sensing secondary users. We represent the groups as G1, G2 and G3 and the two partition thresholds as λ_1 and λ_2 where $\lambda_1 < \lambda_2$

In G1, each user has an MEV above λ_2 such that it will transmit "1" to the fusion center to declare the presence of a PU. All CR users in G1 are either untrusted users which receive strong interference signals even when the PU is inactive or CR users which are in favorable positions and can receive strong primary signals when a PU is present. In G2, the MEV of each SU is below λ_1, as a result, all secondary users send "0" to report the absence of the PU. It is assumed that all users in G2 are either untrusted secondary users which are in deep fading such that their MEVs are very low even for an active PU or some entrusted CR users which can detect absence of a PU when PU is

ISBN: 9788175157538

inactive. In G3, users have their MEVs between λ_1 and λ_2 and they are considered as trusted users but can not give a reliable local decision independently. For the users in G3, they are required to send their MEVs to the fusion center where these values are combined to give a "1" or "0." Let *N1*, *N2* and *N3* respectively denote the SU numbers in G1, G2 and G3, then *N*1 + *N*2 local decisions and *N*3 observed MEVs can be received by the fusion center. At last, the

fusion center can fuse all *N*1 + *N*2 + 1 decisions to derive a final decision according to a revised OR, AND or Majority

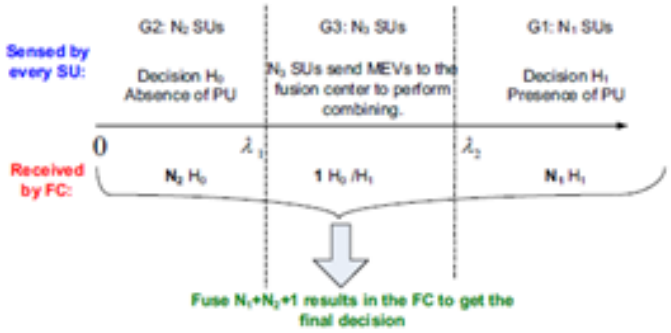

Figure1. Scheme of eigenvalues based detection with double thresholds to counter untrusted secondary user.

fusion rule which will be explained in the next section. The scheme of our method can be illustrated in Fig.1.
In order to accommodate the proposed double-thresholds detector, a revised fusion rule is suggested to eliminate the impact from untrusted secondary users and this revised rule can be represented as D=1 for the following conditions:

If $\sum_{i=1}^{N_1+N_2+1} d_i \geq 1+v$, Revised OR Rule

$$\sum_{i=1}^{N_1+N_2+1} d_i = N_1 + N_2 + 1 - v \ ,$$

Revised AND Rule

$$\sum_{i=1}^{N_1+N_2+1} d_i \geq \frac{1}{2}\left(N_1 + N_2 + 1 + v\right) \ ,$$

Revised Majority Rule And D=0 otherwise where v is the number of untrusted CR users. Considering it occupies a small proportion in all secondary users, it can be obtained by v = ***min*** (*N*1, *N*2) where ***min*** (●) represents the operation to take the minimum between *N*1 and *N*2.

A. Derivation of thresholds

When the PU is inactive, the received signal *x*(m) is AWGN and the covariance matrix **R**r is nearly a wishart random matrix[7]. The two thresholds λ_1 and λ_2 are obtained as:

$$\lambda_1 \approx \delta_{ML} F_1^{-1}\left(P_1\right) + \mu_{ML}$$

$$\lambda_2 \approx \delta_{ML} F_1^{-1}\left(1 - P_2\right) + \mu_{ML}$$

where μ and δ are called the center constant and scaling Constant P_1 and P_2 be the probability of 'Always No' under H_1 and 'Always Yes' under H_0, respectively

V. RESULTS AND DISCUSSION

The protocol based on cryptography proves to b a secure protocol for centralized based systems that essentially uses symmetric signatures and one-way chains. The protocol enables the fusion centre to verify the identity of network members and to ensure the received sensing information is really originated from the claimed source. One of the main features of the proposal is the fact that is computationally efficient and introduces a very small bandwidth over head.

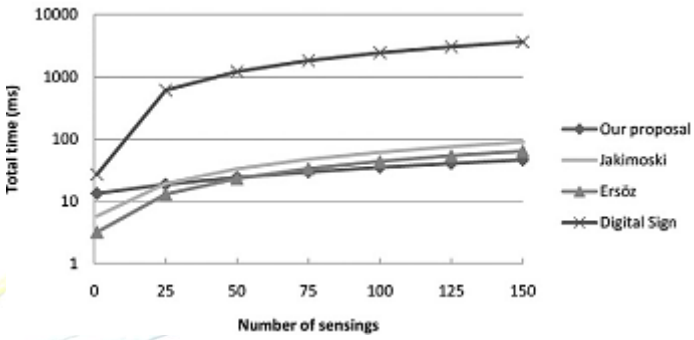

Figure 2. Graph between Number of sensing and total log time.

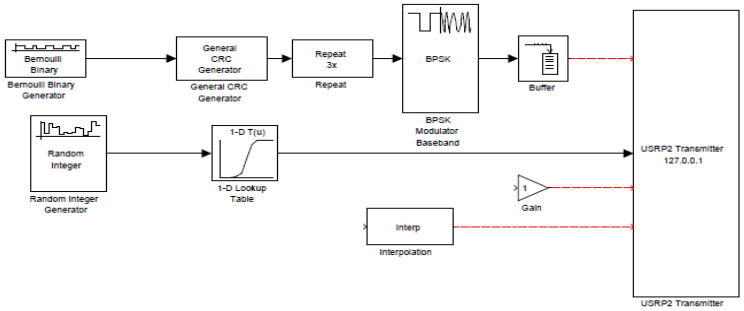

Figure 3. Cognitive radio spectrum adaptation (management)

The spectrum management includes time, frequency and transmit-power controls and dynamic spectrum management allowing the radio terminals to operate in the best available frequency spectrum. SDR provides a software control for a variety of modulation method, filtering, wideband or narrowband operations, spread spectrum techniques and wave form requirements etc. For SDR reconfigurability; a cognitive radio looks naturally to a software-defined radio to perform its task (Fig. 3) The method based on cryptography is highly effective against untrusted users in cognitive radio network.

ISBN: 9788175157538

The proposed method based on eigenvalues is highly effective against untrusted users in cognitive radio network. Q_d and Q_f denote the cooperative probability of detection and false alarm, a graph(figure 4) has been obtained. This graph shows a great improvement in Q_d and Q_f of proposed method as compared to the Q_d and Q_f of conventional method. Similar improvements were also observed through the graphs obtained for AND Rule and Majority Rule.

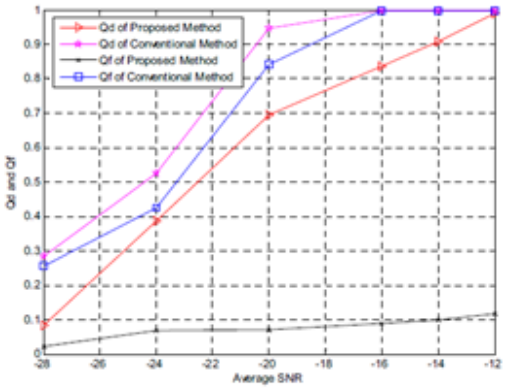

Figure 4. Q_d and Q_f of proposed method and conventional method under OR Rule.

VI. CONCLUSION

The protocol based on cryptography and one way function identifies the users and authenticates the local sensing reports. Public key operations must be performed to register the users. But this phase has to be executed only once and for this reason it does not suppose a problem, not even for mobile users that operate in different CRNs. This protocol is mainly designed for hard cooperation schemes as they ensure that the amount of information sent through the network is minimal. The presented protocol is designed for an open network in which cooperative sensing is performed with the users that are active and close to one another in a particular moment. As a result, the group of users collaborating in the sensing is very dynamic. The challenge of using hash chains to provide security in this scenario is that the participation of the users in the sensing tasks is very irregular. thus the protocol cannot be used with a single chain.

The eigenvalues based detector uses double thresholds and revised data fusion rules to counteract untrusted secondary users in a CR network. The analysis and simulation results show that our method is very useful to find untrusted CR users and to eliminate their deleterious impact. By comparing the detection performance, we conclude that our approach Out performs the conventional cooperative algorithm. Our method is robust and effective and it can be a possible counter measure against untrusted secondary users in a cognitive radio network. This protocol assumes the primary singals to be correlated.

REFERENCES

[1] Federal Communications Commission, Spectrum policy task force report, Tech. rep., ET Docket No. 02-135, 2002.

[2] J. Mitola III, G. Maguire Jr., Cognitive radio: making software radios more personal, IEEE Personal Communications 6 (4) (1999) 13–18I. S. Jacobs and C. P. Bean, “Fine particles, thin films and exchange anisotropy,” in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[3] Y. H. Zeng, C. L. Koh, and Y-C. Liang, “Maximum Eigenvalue Detection: Theory and Application,” *2008 IEEE International Conference on Communications*, May 2008, pp. 4160–416R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.

[4] S. M. Kay, Fundamentals of Statistical Signal Processing: Detection Theory. Upper Saddle River, NJ: Prentice-Hall, 1998M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[5] R. L. Chen, J. M. Parkand, and J. H. Reed, “Defense against Primary User Emulation Attacks in Cognitive Radio Networks,” *IEEE Journal on Selected Areas in Communications*, vol. 26, pp. 25–37, Jan. 2008.

[6] S. M. Mishra, A. Sahai, and R.W.Brodersen, “Cooperative Sensing among Cognitive Radios,” *2006 IEEE International Conference on Communications*, vol. 4, June 2006, pp. 1658–1663.

[7] I. M. Johnstone, "On the distribution of the largest eigenvalue in principle components analysis," *The Annals of Statistics*, vol. 29, no.2,pp.295–327,2001.

[8] P. Kaligineedi, M. Khabbazian, V. Bhargava, Secure cooperative sensing techniques for cognitive radio systems, in: IEEEInternational Conference on Communications (ICC), 2008, pp. 3406–3410.

[9] G. Jakimoski, K.P. Subbalakshmi, Towards secure spectrum decision,in: IEEE International Conference on Communications, IEEE Press,Piscataway, NJ, USA 2009, pp. 2759–276.S.D. Ersoz, S. Bayhan, F. Alagoz.

[10] Secure spectrum sensing and decision in cognitive radio networks, in: A. Ozcan, N. Chaki, D. Nagamalai (Eds.), Recent Trends in Wireless and Mobile Networks, Communications in Computer and Information Science, vol. 84, Springer, Blin Heidelberg, 2010, pp. 99–111.

ISBN: 9788175157538