Matched-Filter-based Spectrum Sensing for Secure Cognitive Radio Network Communications

Fatty M. Salem
Helwan University
1, Sherif st., Helwan, Cairo, Egypt

Maged H. Ibrahim
Helwan University
1, Sherif st., Helwan, Cairo, Egypt

Ihab A. Ali
Helwan University
1, Sherif st., Helwan, Cairo, Egypt

I. I. Ibrahim
Helwan University
1, Sherif st., Helwan, Cairo, Egypt

ABSTRACT

The increasing demand for wireless communication introduces efficient spectrum utilization challenge. To address this challenge, Cognitive Radio (CR) has emerged as the key technology, which enables opportunistic access to the spectrum. However, security is a very important issue but not well addressed in CR networks. In this paper, we focus on security problems arising from Primary User Emulation (PUE) attacks in CR networks where the selfish or malicious node emulates primary user's signals to prevent other secondary users from accessing that frequency band. Our system is based on the deployment of multiple stages of "helper" nodes, helper nodes in the first stage are stationary, close to primary user and responsible for detecting and authenticating primary user's signal based on matched filter spectrum-sensing technique. However, helper nodes in the next stages are placed within the primary user's coverage area and serve as bridges for forwarding the spectrum status information to enable secondary users to verify the cryptographic signature carried by the helper nodes' signals. Moreover, the effect of PUE attack on the performance of matched-filter-based spectrum-sensing technique is illustrated.

Keywords- Matched Filter, Spectrum Sensing, Cognitive Radio Networks, Primary User Emulation, Authentication

1. INTRODUCTION

Increasing usage of wireless communications triggered the development of dynamic spectrum access schemes. To address the increasing demand for wireless bandwidth, cognitive radio networks (CRNs) have been proposed to increase the efficiency of channel utilization under the current static channel allocation policy [1]. CRNs [2] are composed of Software Defined Radios (SDRs) [3] capable of changing their configurations on the fly based on the spectral environment. This capability opens up the possibility of designing flexible and dynamic spectrum access strategies with the purpose of opportunistically reusing portions of the spectrum that are temporarily vacated by licensed primary users.

In licensed bands, legitimate users with a specific license to communicate over the allocated band, i.e., the Primary Users (PUs), have the priority to access the channel. Cognitive radio users, called secondary users (SUs), can access the channel as long as they do not cause interference to the PU.

An essential issue in CRNs is the primary user detection, in which the SUs monitor for the presence of PU's signal on the target channels [1]. If a PU's signal is detected, the SU should not use those channels to avoid interfering with the transmission of the primary user.

The nature of CRNs presents significant challenges in designing security schemes. CRN is a special network that has many constraints and many different features compared to traditional wireless networks. One such difference is that malicious nodes can use the dynamic reconfiguration to create new attacks such as Primary User Emulation (PUE). PUE is a new attack where a malicious node transmits signals that emulate the signal characteristics of primary signals with the purpose of using the radio spectrum for its own interest or denying the access to other nodes.

Hence, It is necessary to have a secure PU detection method that can authenticate the PU in the presence of attackers. At first glance, a cryptographic signature seems to be a good candidate for this task. Unfortunately, Federal Communications Commission (FCC) states that "no modification to the incumbent system (i.e., primary user) should be required to accommodate opportunistic use of the spectrum by secondary users" [4]. As a result, any solution that requires changes to PUs is not desirable.

In this paper, the effect of PUE attack on the performance of matched-filter-based spectrum-sensing technique is investigated. Matched filter detection is better than energy detection as it starts working at lower SNR. Additionally, a complete system is described to determine the threshold of the matched filter to obtain stricter requirements of the probability of false alarm and the probability of miss-detection. In this management framework, a deployment of multiple stages of stationary "helper" nodes over the coverage area of PUs is proposed. Helper nodes in the first stage are close to the PU and responsible for detecting the presence of the PU's signals based on the matched-filter spectrum-sensing technique. However, helper nodes in the next stages are distributed over the coverage area of the PU and responsible only for forwarding the spectrum information to the next stage of helper nodes and/or to SUs inside their coverage area.

This paper is organized in six sections as follows: Section 2 summarizes previous works proposed in the area of spectrum sensing. The system model and the adversary model are described in section 3. The proposed authentication protocol based on matched-filter spectrum-sensing technique is discussed in section 4. The complete system is described in section 5. Finally, this paper is concluded in section 6.

2. RELATED WORK

A number of different methods have been proposed for identifying the presence of signal transmissions. Transmitter detection techniques are further classified into energy detection, matched filter detection and cyclostationary feature detection [5].

Energy Detection: Energy detection (ED), also denoted as a non-coherent detection, is the signal detection technique using an energy detector to detect the presence or absence of signal in the band. Energy detection approaches are based on the Neyman-

Pearson (NP) lemma. The NP lemma criterion increases the probability of detection P_d for a given probability of false alarm P_f . To adjust the threshold of detection, energy detector requires knowledge of the noise power in the band to be sensed. ED is not optimal but simple to implement, so it is widely adopted. Due to its simplicity and non requirement of a priori knowledge of PU's signal, ED is the most popular sensing technique in cooperative sensing [6]. It estimates the presence of the signal by comparing the output of energy detector with a known threshold derived from the statistics of the noise [2, 7, 8, 9].

However, ED is always accompanied by a number of disadvantages: i) sensing time taken to achieve a given probability of detection may be high. ii) detection performance is subject to the uncertainty of noise power. iii) ED cannot be used to detect spread spectrum signals [8].

Matched Filter Detection: The matched filter detector that can be used for CRNs has been first proposed in [8].The matched filter (also referred to as coherent detector), is known as the optimum method for detection of PUs when the transmitted signal is known. It is very accurate since it maximizes the received signal-to-noise ratio (SNR). Matched filter correlates the signal with time shifted version and compares between the final output of matched filter and predetermined threshold to decide the PU presence or absence. However, matched-filtering requires CR to demodulate received signals. Hence, it requires perfect knowledge of the PUs' signaling features such as bandwidth, operating frequency, modulation type and order, pulse shaping, and frame format [2, 8, 10].

Cyclostationary Feature Detection: The cyclostationary feature detector, being first presented in [11], is a spectrum sensing technique which can differentiate the modulated signal from the additive noise. A signal is said to be cyclostationary if its mean and autocorrelation are periodic functions. Feature detection denotes extracting features from the received signal and performing the detection based on the extracted features. The periodicity is commonly embedded in sinusoidal carriers, pulse trains, spreading codes, hopping sequences, or cyclic prefixes of the primary signals. Due to the periodicity, these cyclostationary signals exhibit the features of periodic statistics and spectral correlation, which are not found in stationary noise and interference. Cyclostationary feature detection, used at very low Signal to Noise Ratio (SNR), can distinguish PU signal from noise by using the information embedded in the PU signal that are not present in the noise. The main drawback of this method is high computational complexity and long sensing time [2, 8, 9, 10].

Many other techniques have been proposed to enhance the detection of PU's signals in CRNs. As an example, the mathematical model in [12] takes into account multiple antennas at SUs and uses energy detection (ED) with selective combining (SC) scheme. The maximum allowable transmit power at SU transmitter, to guarantee decodability of PU transmitter signal at PU receiver, is calculated by using the distance between PU transmitter and SU transmitter. However, the covariance-based detection scheme proposed in [13] exploits space-time signal correlation that does not require the knowledge of noise and signal power unlike energy detection method which suffers from noise uncertainty problem. Furthermore, hybrid detection methods [14, 15] are proposed to exploit the advantages of covariance based and energy detection methods for detecting licensed user.

A CR's ability to distinguish between PU's signals and SU's signals is the key to the implementation of Opportunistic Spectrum Sensing (OSS) paradigm. Distinguishing the two signals is nontrivial, but it becomes especially difficult when the CRs operate in hostile environments. In a hostile environment, an attacker may modify the air interface of its own CR to mimic a primary-user-signal's characteristics, thereby causing legitimate secondary users to erroneously identify the attacker as a primary user.

Hence, a scheme that can reliably distinguish between legitimate primary signal transmitters and other transmitters launching PUE attacks is needed. In hostile environments, such a scheme should be integrated into the spectrum sensing mechanism to enhance the trustworthiness of the sensing result.

3. THE MODEL

In this section, system model and adversary model will be described.

3.1 System Model

Entities in CRNs can be classified as follows:

Primary Users: They are the legitimate users who have the license to use a fixed spectrum, which can be divided to a set of *n* orthogonal frequency bands, referred to as channels. However, following the FCC rules, no modifications to PUs are permitted in order to provide secure communication in CRNs. Here, the PU is a TV tower, and a number of TV towers are transmitting their signals with an Effective Radiated Power of *1000 kW* (like WCTV and KTVY towers).

Secondary Users: They are the unlicensed users who are allowed to use the channels assigned to a PU. However, SUs should constantly monitor the usage of the spectrum to avoid interference with the PU.

Helper Nodes: They are the stationary nodes distributed over the coverage area of SUs in multiple stages. Helper nodes in the first stage are responsible for detecting the presence of the PU's signals and broadcasting the spectrum status information to next stage of helper nodes and/or SUs in their coverage area. However, helper nodes in next stage serve as bridge to deliver spectrum status information to next stage of helper nodes and/or SUs in their coverage area. Finally, to securely communicate with SUs, Helper nodes are initialized with public/private keys and certificates from a trusted authority.

3.2 Adversary Model

In the adversary model, the objective of the adversary is to deny using licensed spectrum to SUs in CRNs by emulating PU's signals. Depending on the motivation behind the attack, a PUE attack can be classified as a selfish PUE attack and a malicious PUE attack [16].

Selfish PUE Attackers: A selfish attacker aims at stealing bandwidth from legitimate SUs to maximize its own usage of spectrum resources. The attacker will monitor the spectrum, and once an unoccupied spectrum band is discovered, it will compete with the legitimate SUs by transmitting signals that emulate primary-user-signal's characteristics.

Malicious PUE Attackers: The purpose of a malicious attacker is to disturb the dynamic spectrum access of legitimate SUs but not to exploit the spectrum for its own transmissions. Being different from a selfish attacker, the malicious attacker may emulate a primary signal in both an unoccupied spectrum band and a band currently used by legitimate SUs.

4. PU's AUTHENTICATION PROTOCOL

In this section, the hypothesis testing and the proposed matched-filter-based spectrum-sensing in the presence of PUE attack are described.

4.1 Hypotheses Testing

The signal detection problem is solved by the decision between the three hypotheses:

$$\begin{aligned} &H_0 : \text{Noise} \\ &H_P : \text{Primary user present} \qquad (1) \\ &H_A : \text{PUE attacker present} \end{aligned}$$

The signal under each hypothesis takes the form:

$$x[n] = \begin{cases} w[n], & H_0 \quad n = 0,1,...,N\text{-}1 \\ s_P[n] + w[n], & H_P \quad n = 0,1,...,N\text{-}1 \\ s_A[n] + w[n], & H_A \quad n = 0,1,...,N\text{-}1 \end{cases} \qquad (2)$$

where $s_P[n]$ is the Primary-user's signal to be detected, $s_A[n]$ is the PUE-attacker's signal that emulates the PU's signal, and $w[n]$ is a zero mean Additive White Gaussian Noise (AWGN) with variance σ^2. N is the number of samples of the received signal used in the spectrum sensing process. As it is known, PUE attack transmits signal that emulates primary-user-signal's characteristics with relatively low power to operate on frequencies shared with authorized services as provided by FCC rules [4] for the operation of unlicensed radio transmitters in Part 15 of its rules. Hence, the received signal at the first stage of helper nodes can be written as:

$$x[n] = \begin{cases} w[n], & H_0 \quad n = 0,1,...,N\text{-}1 \\ s_P[n] + w[n], & H_P \quad n = 0,1,...,N\text{-}1 \\ ks_P[n] + w[n], & H_A \quad n = 0,1,...,N\text{-}1 \end{cases} \qquad (3)$$

Where k is the ratio between PUE-attacker's signal and PU's signal. The decision between the hypotheses is made by comparing a test statistic *T(x)* with a threshold γ. The matched filter performance is mainly characterized by two metrics: the probability of detection and the probability of false alarm. Low probability of detection increases the interference inflicted on PUs, whereas high probability of false alarm increases the amount of missed spectral opportunities in the secondary network.

4.2 Secure Matched-Filter-Based Spectrum-Sensing in the Presence of PUE Attack

Matched filter is a coherent detection technique that employs a correlator matched to the signal of interest or certain parts of it, such as pilots, preambles, spreading codes and training sequences. It shows optimal performance results making it a good choice for applications where the transmitted signal is known a priori like radar signal processing. The correlation can be viewed in terms of a filtering process of the data. Since we have a summation of a finite number of samples, we take a FIR filter into considerations. If we now let $x[n]$ be the input to such a filter, then the output $y[n]$ at time n is given by the convolution operation, i.e.

$$y[n] = \sum_{k=0}^{n} h[n-k]x[k] \qquad (4)$$

where $h[n]$ is the impulse response the FIR filter. The proper choice of the impulse response is the "flipped around" version of the signal [17], and it is denoted as:

$$h[n] = s_P[N-1-n] \qquad n = 0,1,..., N-1 \quad (5)$$

Hence, Inserting (5) into (4) and sampling the output of the FIR filter at time $n = N-1$ yields:

$$y[N-1] = \sum_{n=0}^{N-1} x[n]s_P[n] = x^T s_P = T(x) \quad (6)$$

It is known that the noise is Gaussian and $x[n]$ is deterministic and known by the receiver. Matched filter can be constructed using known sequences employed by the PUs for control. For instance, digital TV transmissions consist of a sequence of segments. For every *313* segments, a Data Field Sync segment of one known *511*- bit PN sequence, and three known *63*-bit PN sequences is used for synchronization [18]. *T(x)* is a linear combination of Gaussian random variables, hence *T(x)* is also Gaussian. If the expected value and the variance of the test statistic are computed, we get:

$$T(x) \sim \begin{cases} N(0,\sigma^2\varepsilon_P), & H_0 \\ N(\varepsilon_P,\sigma^2\varepsilon_P), & H_P \\ N(k\varepsilon_P,\sigma^2\varepsilon_P), & H_A \end{cases} \qquad (7)$$

where ε_P is the PU's signal energy. Here, we decide between three hypotheses that differ by a shift in the mean of *T(x)*. More precisely, the corresponding PDFs have the same shape (same variance) but are displaced against each other. To show the performance of the matched filter with the signal to noise ratio (ε_P/σ^2), (7) is divided by $\sqrt{\sigma^2\varepsilon_P}$. Hence, the scaled test statistic $T'(x) = T(x)/\sqrt{\sigma^2\varepsilon_P}$ has the PDF:

$$T'(x) \sim \begin{cases} N(0,1), & H_0 \\ N(\sqrt{\varepsilon_P/\sigma^2},1), & H_P \\ N(k\sqrt{\varepsilon_P/\sigma^2},1), & H_A \end{cases} \qquad (8)$$

The probability of detection can be defined as:

$$\begin{aligned} P_D &= P(T > \gamma \mid H_P) \\ &= P\left(T' > \frac{\gamma}{\sqrt{\sigma^2\varepsilon_P}} \mid H_P \right) \\ &= Q\left(\frac{\gamma - \varepsilon_P}{\sqrt{\sigma^2\varepsilon_P}} \right) \qquad (9) \\ &= Q\left(\frac{\gamma}{\sqrt{\sigma^2\varepsilon_P}} - \frac{\varepsilon_P}{\sqrt{\sigma^2\varepsilon_P}} \right) \\ &= Q\left(\gamma' - \sqrt{\frac{\varepsilon_P}{\sigma^2}} \right) \end{aligned}$$

where $\gamma' = \gamma/\sqrt{\sigma^2\varepsilon_P}$. The probability of missing is expressed as:

$$P_M = 1 - P_D \qquad (10)$$

However, the total probability of false alarm results in the noise and the PUE attack presence. Hence, the total probability of false alarm may be written as follows:

$$P_F = P_{F0}.P(0) + P_{FA}.P(A) \qquad (11)$$

where *P(0)* is the priori probability of the noise, *P(A)* is the priori probability of the PUE attackers, and P_{F0} can be defined as:

$$\begin{aligned} P_{F0} &= P\left(T > \gamma \mid H_0\right) \\ &= P\left(T' > \frac{\gamma}{\sqrt{\sigma^2 \varepsilon_P}} \mid H_0\right) \qquad (12) \\ &= Q\left(\frac{\gamma}{\sqrt{\sigma^2 \varepsilon_P}}\right) \\ &= Q(\gamma') \end{aligned}$$

and;

$$\begin{aligned} P_{FA} &= P\left(T > \gamma \mid H_A\right) \\ &= P\left(T' > \frac{\gamma}{\sqrt{\sigma^2 \varepsilon_P}} \mid H_A\right) \qquad (13) \\ &= Q\left(\frac{\gamma - k\varepsilon_P}{\sqrt{\sigma^2 \varepsilon_P}}\right) \\ &= Q\left(\frac{\gamma}{\sqrt{\sigma^2 \varepsilon_P}} - \frac{k\varepsilon_P}{\sqrt{\sigma^2 \varepsilon_P}}\right) \\ &= Q\left(\gamma' - k\sqrt{\frac{\varepsilon_P}{\sigma^2}}\right) \end{aligned}$$

The threshold γ' can be determined based on the requirement for the probability of missing and the probability of false alarm. For practical applications, the IEEE 802.22 standard suggests both probabilities of false alarm and missing be less than *0.1* in terms of detecting PUs [19]. Herein, a stricter requirements that P_M and $P_F \leq 0.02$ were assumed, and thus from figure 1 and 2 at SNR $(\varepsilon_P / \sigma^2)$ = *15dB*, the threshold γ' could be determined to be *3.57* to obtain probability of detection *0.98* and hence, the probability of missing will be *0.02*. However, Figure 3 shows that the probability of false alarm due to noise at γ' = *3.57* will be *0.0001785*.

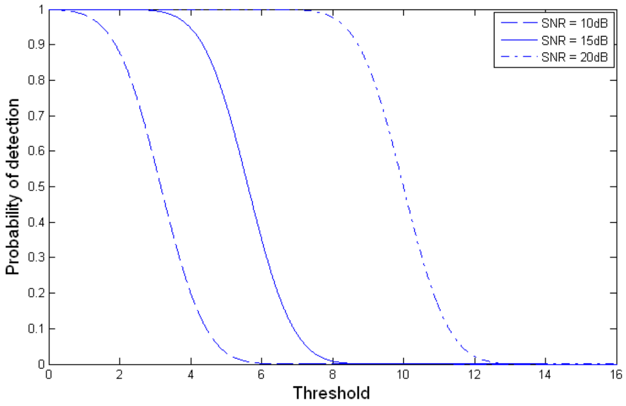

Fig 1: Probability of detection versus threshold γ'

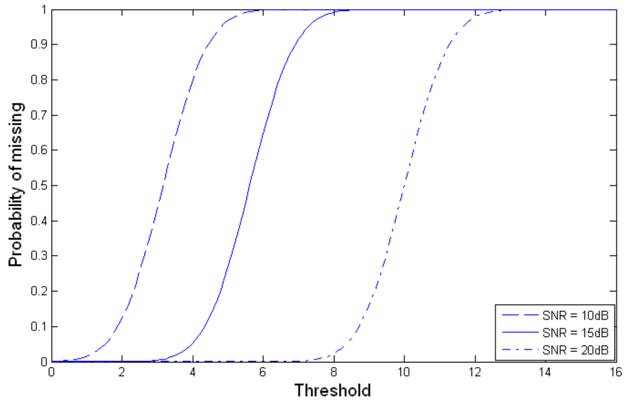

Fig 2: Probability of missing versus threshold γ'

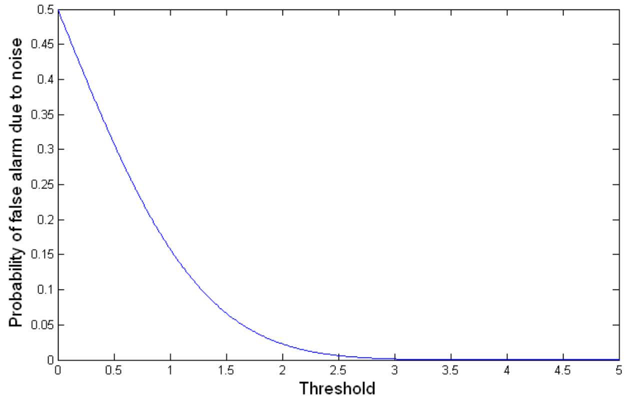

Fig 3: Probability of false alarm due to noise versus threshold γ'

Figure 4 plots the probability of false alarm due to PUE attack versus the threshold γ'. At *k=1/5* (typically small value i.e., high power of the received PUE attacker's signal), the probability P_{FA}= *0.007236*. Hence, the total probability of false alarm is kept less than *0.01*.

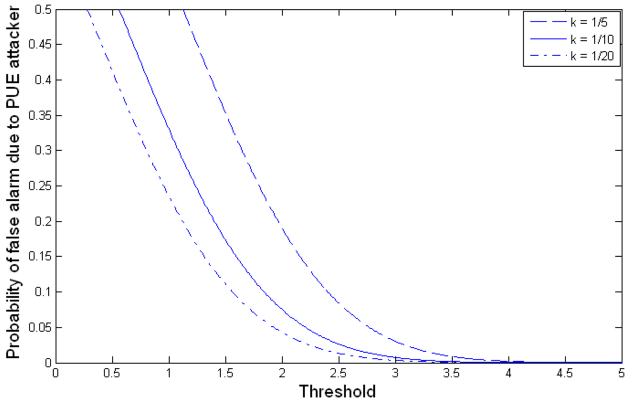

Fig 4: Probability of false alarm due to PUE attack versus threshold γ'

5. THE COMPLETE SYSTEM

In this section, the distance between the PU and the first stage of helper nodes will be determined, and the interaction between CR entities will be described.

5.1 Distance between PU and First Stage of Helper Nodes

To determine the distance between the PU and the first stage of helper nodes, we consider a ground reflection (two-ray) model for calculating the power level of a received signal over a distance, *d*. The received power level is given by [20]:

$$P_r(d) = P_t G_t G_r \frac{h_t^2 h_r^2}{d^4 L} \qquad (14)$$

where P_t is the transmitted power, $P_r(d)$ is the received power which is a function of the T-R separation, G_t, h_t are the transmitter gain and height, respectively, G_r, h_r are the receiver antenna gain and height, respectively, *d* is the T-R separation distance in meters, and *L* is the system loss factor not related to propagation *(L≤1)*. Following the FCC rules [4], the height of the antenna of helper nodes (and attacker) in the system is assumed to be *30 meter* as the commission is limiting the maximum antenna height of fixed unlicensed TV Band Devices (TVBDs) to *30 meters* above ground level.

Figure 5 plots the received power versus the distance between the PU and the first stage of helper nodes. However, Figure 6 plots the SNR $(\varepsilon_p / \sigma^2)$ versus the distance between the PU and the first stage of helper nodes at different values of noise variance.

To obtain our target probability of detection (calculated previously at $(\varepsilon_p / \sigma^2)$ *=15dB*), the first stage of helper nodes can be positioned *4310 meter* away from the PU to achieve the required signal to noise ratio (SNR=*15dB*) at σ^2 *= 17dBm*. Hence, the maximum possible distance between the PU and the first stage of helper nodes could be extended more than that of the scheme in [21] to obtain the same probabilities of detection and smaller probability of false alarm.

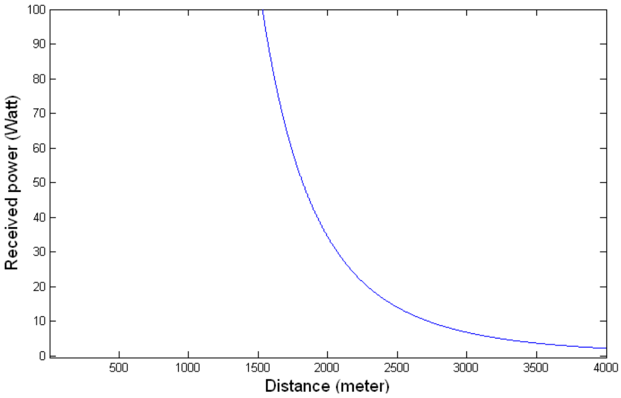

Fig 5: Received power versus distance between PU and the first stage of helper nodes

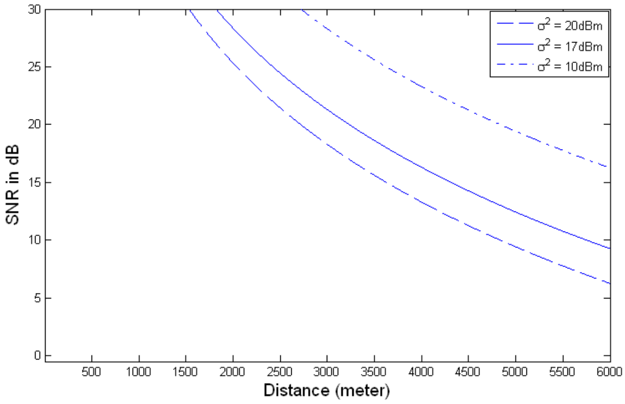

Fig 6: PU's SNR versus distance between the PU and the first stage of helper nodes

5.2 Interactions between CR Entities

Helper nodes at the first stage are responsible for detecting the presence of PU's signal based on matched-filter-based spectrum-sensing technique and then forwarding the spectrum status information to helper nodes in next stages and/or SUs in their coverage area. When the test statistic *T(x)* at first stage of helper nodes exceeds the threshold *γ'*, helper nodes detect PU's signal, otherwise, it is either due to noise or PUE attack. Helper nodes can differentiate between noise and PUE attack using cyclostationary spectrum sensing method [22].

However, following the FCC rules [23], all fixed devices (including helper nodes) are permitted to transmit up to *30dBm* (*1 watt*) with up to *6dBi* antenna gain. Hence, helper nodes in the first stage are NOT able to deliver the spectrum information directly to all SUs existing in the wide coverage area of PUs. Hence, it is the essential need for multiple next stages of helper nodes.

For broadcasting the spectrum status information to helper nodes in the next stage and/or to SUs within their coverage area, each helper node *i* in the first stage periodically transmits the following information: m_i || $Sig_i(m_i)$ where || denotes concatenation, m_i is an *n*-bits occupancy vector indicating the set of *n*-channels where legitimate PUs are active, while $Sig_i(m_i)$ denotes the cryptographic signature of helper node *i* on the message m_i using the DSS algorithm [24] (as the recommended standard digital signature algorithm).

When receiving spectrum information, helper nodes in the next stage or/and SUs will verify the authenticity and integrity of the received message m_i by verifying the validity of the cryptographic signature $Sig_i(m_i)$. Message m_i that fails to be authenticated will be discarded. If the message is verified, SUs will accept the contents of the message while each helper node *j* in the next stage will retransmit the received spectrum information to the next stages of helper nodes as follows: m_j || $Sig_j(m_j)$.

6. CONCLUSION

In this paper, a new secure authentication protocol based on matched filter spectrum sensing technique was proposed. In the proposed secure authentication protocol, the cryptographic digital signature and the matched-filter-based spectrum-sensing technique have been integrated. Helper nodes at the first stage can detect the presence of PU's signals based on matched filter spectrum sensing and securely deliver the signed spectrum status information to next stage of helper nodes and/or SUs in their coverage area. The PU's presence is detected by the first stage helper nodes, while mobile SUs with limited battery are responsible only for verifying the cryptographic signature carried by the helper-nodes' signals. In this paper, the performance of the matched-filter-based spectrum-sensing technique in the presence of the PUE attack has been investigated. Moreover, a stricter requirements of the probability of a false alarm and the probability of missing can be obtained.

7. REFERENCES

[1] Chen, R., Park, J., and Reed. J. H. 2008. Defense against primary user emulation attacks in cognitive radio networks. IEEE Journal on Selected Areas in Communications; 26(1):25–37.

[2] Akyildiz, I.F., Lee, W., Vuran, M., and Mohanty, S. 2006. NeXt generation/dynamic spectrum access/cognitive radio wireless networks: a survey. Computer Networks; 50(13):2127–2159.

[3] Ulversoy, T. 2010. Software defined radio: Challenges and opportunities. IEEE Communications Surveys & Tutorials; 12: 531 – 550.

[4] Federal Communications Commission. Facilitating opportunities for flexible, efficient, and reliable spectrum use employing spectrum agile radio technologies. ET Docket, (03-108), Dec. 2003.

[5] Bhargavi, D., and Murthy, C. R. 2010. Performance comparison of energy, matched-filter and cyclostationarity-based spectrum sensing. IEEE Eleventh International Workshop of Signal Processing Advances in Wireless Communications (SPAWC), Marrakech, 1-5.

[6] Cabric, D., Tkachenko, A., and Brodersen, R. 2006. Spectrum sensing measurements of pilot, energy, and collaborative detection. Proc. IEEE Military Communication Conference, Washington, D.C., USA, 1–7.

[7] Pawełczak, P. 2011. Cognitive Radio: Ten Years of Experimentation and Development. IEEE Communications Magazine; 49(3): 90-100, IEEE DOI: 10.1109/MCOM.2011.5723805.

[8] Akyildiz, I.F., Lo, B.F., and Ishnan., R. B. 2011. Cooperative spectrum sensing in cognitive radio networks: A survey. Physical Communication; 4(1): 40-62. Elsevier DOI: 10.1016/j.phycom.2011.12.003

[9] Ziafat, S., Ejaz, W., and Jamal, H. 2011. Spectrum sensing techniques for cognitive radio networks: Performance analysis. 2011 IEEE MTT-S International Microwave Workshop Series on Intelligent Radio for Future Personal Terminals, 1-4. IEEE DOI: 10.1109/IMWS2.2011.6027191.

[10] Sahai, A., Hoven, N.,and Tandra, R. 2004. Some fundamental limits in cognitive radio. In Proceedings of the Allerton Conference on Communication, Control, and Computing, Monticello, Ill, USA.

[11] Cabric, D., Mishra, S. M., and Brodersen, R. W. 2004. Implementation issues in spectrum sensing for cognitive radios," in Proceedings of the 38th Asilomar Conference on Signals, Systems and Computers; 1: 772–776.

[12] Jain, S. K., Bharti, M. R., and Kumar, A. 2013. Distance based an Efficient Transmit Power Control Scheme in Cognitive Radio System with Multiple Antennas. International Journal of Computer Applications; 72(21): 32-37.

[13] Dhope, T., Simunic, D. 2012. Performance analysis of covariance based detection in cognitive radio. In Proceeding of 35th Jubilee International Convention MIPRO, Opatija, 737 - 742.

[14] Dhope, T., Simunic, D. 2011. Hybrid detection method for cognitive radio. 19th International Conference on Software, Telecommunications and Computer Networks (SoftCOM), Split, 1-5.

[15] Dhope, T., Simunic, D. 2012. Hybrid detection method for spectrum sensing in cognitive radio. 35th Jubilee International Convention MIPRO 2012, 765 - 770.

[16] Chen, R., and Park, J. M. 2006. Ensuring Trustworthy Spectrum Sensing in Cognitive Radio Networks. IEEE Workshop on Networking Technologies for Software Defined Radio Networks, 110-119.

[17] Haykin, S.. 2001. Communication Systems, Fourth Edition, Wiley.

[18] A.T.S. Committee. ATSC digital television standard (a/53) revision e, with amendments no. 1 and 2,. http://www.atsc.org/cms/, 2006.

[19] Cordeiro, C., Challapali, K., and Ghosh, M. 2006. Cognitive phy and mac layers for dynamic spectrum access and sharing of tv bands. In Proceeding of the first international workshop on Technology and policy for accessing spectrum, ACM.

[20] Rappaport, T. S. 2002. Wireless communications principles and practice, Prentice Hall, 2nd edition.

[21] Salem, F. M, Ibrahim, M. H., and Ibrahim, I. I. 2012. A primary user authentication scheme for secure cognitive TV spectrum sharing. International Journal of Computer Science Issue; 9(4) : 157-166.

[22] Thamizharasan, S., Saraswady, D., and Saminadan, V. 2013. Periodicity based Cyclostationary Spectrum Sensing in Cognitive Radio Networks". International Journal of Computer Applications; 68(6):6-9.

[23] Second Report and Order and Memorandum Opinion and Order In the Matter of Unlicensed Operation in the TV Broadcast Bands, Additional Spectrum for Unlicensed Devices Below 900 MHz and in the 3 GHz Band, Federal Communication Commission, Document 08-260, Nov. 14, 2008.

[24] Gennaro, R., Jarecki, S,. Krawczyk, H., and Rabin, T. 1996. Robust Threshold DSS Signatures. EURO-CRYPT; Lecture notes in computer science1996; 1070 : 354-371.