An Effective Primary User Authentication Mechanism for Denial of Service Attack in Cognitive Radio Networks

Christo Reegan Raj. V
(M.E.) Communication systems,
Communication systems,
Department of ECE,
Sri Krishna College of Engg. and
Tech. Coimbatore.

Sabitha. R M.E.,Ph.D.

Associate professor,
Department of ECE,
Sri Krishna College of Engg. and
Tech. Coimbatore.

Karthikha. C M.E.

Assistant professor,
Department of ECE,
Sri Krishna College of Engg. and
Tech. Coimbatore.

ABSTRACT

The vacant or under-utilized TV bands are resourcefully operated by Cognitive Radio permitted IEEE 802.22 Wireless Regional Area Networks (WRAN). Conversely due to the nature of cognitive radio networks and absence of active security protocols, the IEEE 802.22 networks are exposed to several Denial of Service (DoS) threats. In this work the target band for DoS attack is a particular band called as Most User Band which has maximum number of operators between the existing sub bands in the CR network. A primary user authentication system created on the spreading of "helper" nodes, motionless within the geographic area of the CRN. Our system works on a mixture of physical-layer signatures (link signatures) and cryptographic mechanisms to regularly sense PU action and pass data to the CRN. We suggest a countermeasure strategy (Time concealment strategy), to counter the MUB attack. Simulation results are provided to establish the efficiency of the proposed MUB attack and TCS with attack time control for more survival improvement of secondary nodes.

Keywords

Cognitive radio, most user band attack denial of service attack, interference, authentication

1. INTRODUCTION

A Cognitive Radio (CR) is a radio that can change its transmitter parameters based on interaction with the environment in which it operates. The majority of cognitive radios will probably be SDR (Software Defined Radio) but neither having software nor being field programmable are requirements of a cognitive radio. Adaptive networks and dynamic spectrum access is provided in CR for spectrum utilization [1]. There are several security vulnerability in CR networks. CR first senses for available spectrum holes in the physical layer of the network. The CR network consist of an open access mechanism due to this the medium access control (MAC) layer misuse takes place (e.g., misbehaviour CR, selfish CR or cheating CR [2]). There are several attacks in physical layer those are discussed in [6-13]. The operation policy modified by attacker or misconfiguration is discussed in [6]. The attack can be caused due to several agents in the network which are investigated in [7]. Due to the selfish behaviour of CR the attack can be caused in the network [8]. It is also noted that the vulnerability of CR networks can be due to the fact that even weak attack signal levels could significantly disrupt a CR network [9] as spectrum sensing (low signal level detection) is an essential part of CR operations. DoS attacks and countermeasures in multi-channel CR networks have been reported in [10]. Frequency hopping based countermeasure techniques have been also studied [11], [12].

Cognitive radio technology is expected to increase the spectrum utilization by allowing opportunistic use of the idle portion of the licensed spectrum by Secondary (unlicensed) Users (SUs) [18], [19], [20], [21]. The primary user (PU) transmission such as energy, spectral power density, modulation, cyclostationary features [19], [21] and pilot information which relay on physical layer characteristics for spectrum sensing. However, these methods do not authenticate the PU signal. An adversary equipped with a software defined radio can mimic the transmission characteristics of a PU in order to emulate PU activity on idle portions of the spectrum. The goal of this attack is to block SUs from utilizing the idle channels, thus reducing the available bandwidth and degrading the network performance.

In this paper, we have proposed a type of DoS attack and the countermeasure. We have also provides primary user authentication for securely transmitting the PU information to the SU. In this attack the node senses and monitor the signal activity in each band in the network. We consider first three MUB in this network and perform DoS attack. The band under attack will have primary user and secondary user. Further we introduce a countermeasure strategy as time concealment strategy (TCS) to counter the MUB attack. The physical layer is more vulnerable to primary user emulation (PUE) attack. For this, we provide an authenticating mechanism as primary user authentication to securely transmit the PU information to the SU.

The rest of the paper is organised as follows. Section II present the MUB attack in cognitive radio network. Section III present the time concealment strategy. Section IV present the primary user authentication and the performance and results are shown in V. Conclusions are drawn in section VI.

2. MOST USER BAND ATTACK

The following assumptions are made, number of primary nodes Np, number of secondary nodes Ns and number of bands in a CR. Maximum user node which can be allocated with a band capital C. We implemented a combined two stage with CR for accuracy in sensing. So that all the nodes are setting separated from band with primary nodes. Number of band with primary nodes Mp and number of vacant bands (Secondary band) Ms. Mp+Ms=M. The attack for investigation is (DoS) denial of service based attack and an attacker or a malicious CR node emits international interference on one or several bands and denies the service in those band. To maximize its outcome the malicious node targets the band with most user (number of nodes). In this paper we consider a scenario in which the malicious node attack one band out of three at a time and are referred as most user band (I_{max}), (II_{max}) and (III_{max}) etc.

In this paper sub-Nyquist sampling also known as compressive sampling is also used for sensing the signal. Sub-Nyquist sampling referees to the technique of recovery signal from samples obtained using a rate below the nyquist rate. Through applying the location of active primary frequency band has been determined with the prier information of upper found M on the total number of active bands and maximum band width W_{max} of the active sub band. Sub band is selected by MUB attacker. The MUB attacker selects the band (band i*) as MUB,

$$i^* = \{i \mid \max_{i\in\{1,2,....,M\}} (\sum_{j=1}^{Ns} | h_j |^2 \, x_{ij} + \sum_{k=1}^{Np} | h_k |^2 \, x_{ik})\} \quad (1)$$

The MUB attacker targets the most user band (i*) among all M available bands. The energy band comparison where $|h_j|$ and $|h_k|$ represents the channel gain between the attacker and node j and k represents specifies that secondary node operates in one secondary band. Primary node operates in one primary band.

$$\sum_{i=1}^{Ms} x_{ij} = 1, \sum_{i=1}^{Mp} x_{ij} = 0 \quad (2)$$

$$\sum_{i=1}^{Mp} x_{ik} = 1 \quad (3)$$

$x_{ij} \in \{0,1\} = 1$ Indicates that secondary node j operates in band i and $x_{ij} \in \{0,1\} = 0$ indicates, otherwise. $x_{ik} \in \{0,1\} = 1$ Indicates primary node k operates in band i and $x_{ik} \in \{0,1\} = 0$ indicate otherwise. Node capacity consideration in the secondary plus primary band are,

$$\sum_{j=1}^{Ns} x_{ij} \le C, \sum_{k=1}^{Np} x_{ik} \le C \quad (4)$$

For evolutionary the phenomenon of CR network under MUB attack we calculate the number of switching nodes (e.g. node which are not in a targeted band) over the total number of nodes. Here, let $A_{i,i*}^S(j)$ and $A_{i,i*}^S(k)$ to denote that whether a secondary/primary node is under attack, respectively.

$$A_{i,i*}^S(j) = \begin{Bmatrix} 1, x_{ij} = 1 \cap i = i^* \\ 0, otherwise \end{Bmatrix} \quad (5)$$

$$A_{i,i*}^P(k) = \begin{Bmatrix} 1, x_{ik} = 1 \cap i = i^* \\ 0, otherwise \end{Bmatrix} \quad (6)$$

The percentage of surviving secondary nodes and primary nodes V_s and V_p can be obtained by $V_S = \left(\sum_{j=1}^{Ns}(1 - A_{i,i*}^S(j))\right) / N_S$ and $V_P = \left(\sum_{k=1}^{Np}(1 - A_{i,i*}^P(k))\right) / N_p$

Respectively. Further the output of the total surviving nodes in the network V, can be determined by.

$$V = \frac{\left(\sum_{j=1}^{Ns}(1 - A_{i,i*}^S(j))\right) + \left(\sum_{j=1}^{Np}(1 - A_{i,i*}^P(k))\right)}{Ns + Np} \quad (7)$$

Notice that only busy band and hence active primary and secondary band are considered in the network model and in the performance metric (Eq. (5), (6) and (7)).

3. MUB ATTACK COUNTERMEASURES

In this section we introduce MUB countermeasure known as time concealment strategy, which depends on the sensing time based Sub-Nyquist sampling. Alternative the sensing time and improved sensing accuracy because increased sensitivity time result in better detection of CR nodes in the presence of MUB attacker in TCS a few secondary node converge to a single band to create a most user band (e.g. higher number of nodes).

This band will be attacked by the malicious CR node (A MUB attacker) and those secondary nodes will be sacrificing nodes. All remaining nodes and all primary nodes will operate in other bands and will be surviving nodes. The basic idea of TCS is unlike consider a co-operate CR network which is unhold at a given time there will be some sacrificing nodes to protect survival nodes. The secondary nodes raises as a sacrificing or survival nodes also changes with sensing time block of the relation of random distribution and movement of secondary nodes. Hence attacking time can be chosen as a multiple of sensing time to produce maximum attack outcome. In the TCS process due to the variability of each node, different nodes have different detection capability in each band.

Number of sub band=3, Frequency range=0-1.5GHz. Therefore Nyquist rate f_{max}=1/T=1.5GHz. As a DoS based attack a MUB attacker could internally choose primary/ secondary band as a target band depend on the number of users sensed during the sensing time which in turn depends on maximum frequency of the band. Down sampling factor and the FFT size used during sampling. When a MUB attacker targets one primary band, the primary node under attack are unable to avoid the attacker size they have no Spectrum sensing and reconfiguration capabilities.

When the MUB attacks target on one secondary band, the secondary nodes under attack could hop to another nodes to avoid attacks the MUB attacker could follow the secondary nodes due to its Sub-Nyquist sampling based on energy detection capabilities. Therefore the CR's intend signals interference avoidance capabilities is no longer effective on countering the MUB attack. Because the communication efficiency is reduced and there exist extra synchronization complexity through centre signalling during the process of signal or interference avoidance process.

The conventional frequency hopping methods are no longer effective since, the MUB attack can follow the CR to its new operating band. Hence MUB attack is realistic and significant threat. With its cognitive capability of Sub-Nyquist sampling, energy detection based MUB attack is able to launch targeted attack. Its impact can be sustainable as CR inherent interference avoidance capabilities or existing anti attack methods no longer effective on countering MUB attack. The TCS algorithm or the selection of the sampling nodes are desired as follows. To have maximum survivability the number of CR nodes (j) in the attack band i* to be minimum.

$$Max(Vs) \equiv \min_{A_{i,j}(j)} \sum_{j=1}^{N_s} x_{i*j} \quad (8)$$

Protect all primary nodes from the attack. There won't be any primary node in the attack band i*.

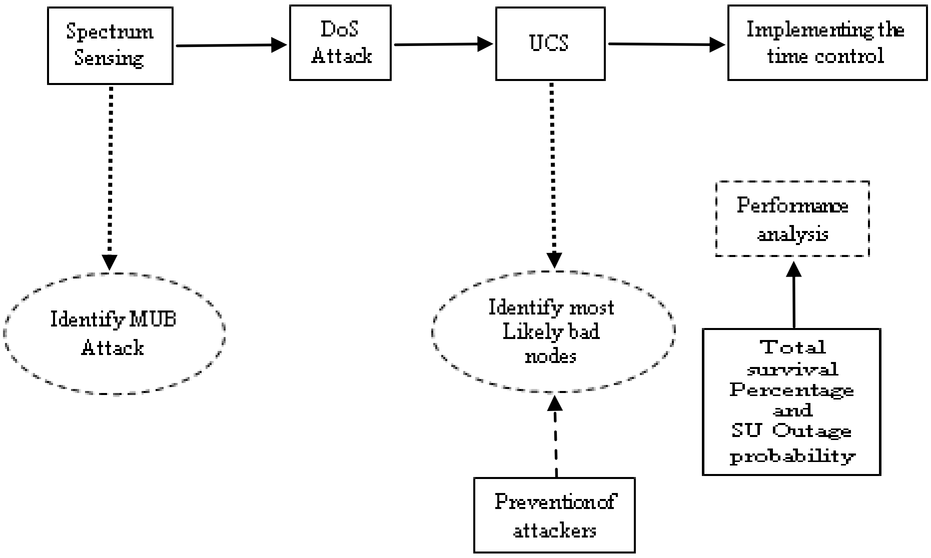
Spectrum Sensing
DoS Attack
UCS
Implementing the time control
Performance analysis
Identify MUB Attack
Identify most Likely bad nodes
Total survival Percentage and SU Outage probability
Prevention of attackers

Fig. 1. Most user band attack scenario

$$\sum_{k=1}^{N_p} x_{i*k} = 0 \tag{9}$$

The most user band must have maximum number of nodes sensed at a given band.

$$\sum_{j=1}^{N_s} x_{i*j} + \sum_{k=1}^{N_p} x_{i*k} \geq \sum_{j=1}^{N_s} x_{ij} + \sum_{k=1}^{N_p} x_{ik} \tag{10}$$

In order to avoid the duplication of nodes in other bands that each secondary nodes is operating in one secondary band only.

$$\sum_{j=1}^{N_s} x_{ij} = 1 , \sum_{j}^{N_p} x_{ij} = 0 \tag{11}$$

Each primary node is operating in one primary band only

$$\sum_{k=1}^{N_p} x_{ik} = 1 \tag{12}$$

The node capacity in each band is given by

$$\sum^{N_s} x_{ij} \leq c, \sum^{N_s} x_{ik} \leq c \tag{13}$$

We denote r_j as the distance between a secondary node j to the most user band attacker and r_k as the distance between a primary node k to the most user band attacker. We assume that $r_j + r_k$ follow the distribution below [14].

$$\Pr(r_j) = \begin{cases} \dfrac{2r_j}{R^2 - {R_0}^2}, r_j \in [R_0, R] \\ 0, otherwise \end{cases} \tag{14}$$

$$\Pr(r_k) = \begin{cases} \dfrac{2r_k}{R^2 - {R_0}^2}, r_k \in [R_0, R] \\ 0, otherwise \end{cases} \tag{15}$$

With the MUB attacker being in the centre and R being the radius of the circular grid of a CR network, which includes all the nodes and the attacker. Also, there is no node presence within a radius R_0 around the centre (attackers).

In implementing TCS, the distance between nodes and the attacker (r_j+r_k) can be estimated based on signal strength information [15], [16]. Localization of attacker play an important role in CCS implementation and some related studies of attacker localization have been reported in [5] and [17].Wideband spectrum sensing based on Sub-Nyquist sampling is used to derive the signal presence. Based on that a central agency or node and perform optimisation in determining sacrificing nodes and if time control is implemented, required transmit time level. As described in TCS algorithm the sub sampling sensing time and node distribution in the sub band play roles in determining the TCS performance accuracy of our objective is to maximize the detection of surviving nodes. The TCS algorithm as defined in (8) through (13) can be further improved by incorporating attack time control in the secondary nodes. This is to deserve the number of some secondary nodes in one particular band, thus increasing the number of surviving nodes needed in TCS. The TCS algorithm with time control can be defined using (8) through (13), substituting (10) with

$$\sum_{j=1}^{N_S} |h_j|^2 x_{i*j} P_j + \sum_{k=1}^{N_p} |h_k|^2 x_{i*k} \geq \sum_{j=1}^{N_S} |h_j|^2 x_{ij} P_j + \sum_{j=1}^{N_p} |h_k|^2 x_{ik} \forall i \in \{1,2,...,M\} \tag{16}$$

We have the following constraint in implementing time control because larger the sensing time higher the sensing accuracy of nodes in CR network. Considering maximum attack time and minimum attack time, the attack time control range of secondary nodes.

$$At_L \le \forall At_j \le At_U \qquad (17)$$

The total attack time per the network (all secondary nodes) is assumed to be constant.

$$\sum_{j=1}^{Ns} At_j = Ns \qquad (18)$$

4. PRIMARY USER AUTHENTICATION

4.1 System Architecture

The problem of authenticating the PU signal at the SU can be modelled as a two-party authentication problem. We propose a PU authentication system that securely and reliably delivers PU activity information to SUs. Provision of robust sensing information is facilitated by the deployment of a set of “helper” nodes. These nodes are responsible for authenticating the PUs and providing channel status information to the PU activity and transmit channel availability information to the SUs. The helper nodes authenticate the PU using a link signature which is a channel property between two nodes. The SUs authenticate the helper nodes by verifying their cryptographic signatures. Helpers are deployed within the area of the PU network, independent of the location of the PUs, and can be relatively cheap low-power devices. Moreover, the location of the PUs need not be known. We also make use of a reputation based system to detect compromised helpers that provide erroneous spectrum information.

4.2 Authentication Mechanism

In this section, we describe the two steps of the spectrum authentication mechanism, i.e., the authentication of the PU signal at the helpers and the secure broadcasting of spectrum status information from the helpers to the SUs.

4.2.1 PU Signal Authentication at the Helpers

To authenticate PU signals, a location distinction mechanism using multipath-based link signatures is employed. During Phase I, helpers sample PU activity on every channel of the PU network in order to create a link signature for each channel. The helpers utilize known pilot signals typically transmitted by the PUs for synchronization purposes. We briefly describe the link signature mechanism proposed in [22], in the context of PU-helper authentication. When PU i transmits a signal $s_i(t)$, helper j receives signal

$$r_j(t) = h_{ij}(t) * s(t) = \sum_{l=1}^{L} \alpha_l e^{j\phi l} s_i(t - t_l) \qquad (19)$$

To obtain the impulse response, the helper samples the PU signal during the transmission of the known sequence and stores the necessary samples to robustly “fingerprint” the fixed RF channel. During this training phase, which needs to be performed only once, it is assumed that no adversary is present to emulate PU. Once a link signature for a given PU has been constructed, the helper can authenticate subsequent transmissions by comparing their characteristics to the stored link signature. To obtain the desired impulse response, operations in the frequency domain yield

$$H_{ij}(f) = \frac{1}{P_s}\left|S_i(f)\right|^2 R_j(f) = \frac{R_j(f)}{S_i(f)} \qquad (20)$$

Where P_s denotes the transmission power at the sender, and $X(f)$ denotes the Fourier transform of a signal $x(t)$. To construct a link signature represented by $H_{ij}(f)$, the $s_i(t)$ must be known at the helper.

It has been mandated by FCC that if a PU starts transmission on a channel, the SU occupying that channel should vacate it within two seconds. Therefore, the helper nodes continuously sense the channels for detecting a valid PU signal. In case the helper node senses PU activity on a free channel, or senses a previously occupied channel to become idle, it updates its occupancy vector to all the neighbouring SUs.

4.2.2 Secure Distribution of Spectrum Information to the SUs

Algorithm 1 Spectrum Authentication (SA) Algorithm

```
1: SU $j$ collects all messages $m_{i,}\ i = 1,........,k$ from the set of helpers $k$ within its range.
2: For each $m_i \in K$ SU $j$ verifies the authenticity and integrity of $m_i$ using $sig_i m(i)$. Messages $m_i$ that fail to be authenticated are discarded.
3: SU $j$ checks if the transmission sequence number $SN_i s$ of each $m_i$ is current. $m_i s$ With older $SN_i s$ are discarded.
4: SU $j$ performs a location consistency test by checking if $|L_a - L_b| \le 2r \quad \forall a,b \in K$. Here, $r$ denotes the communication range of the helpers.
5: If the location test is consistent $\forall a,b \in K$, the occupancy vector $V$ of SU $j$ is computed using an OR operation between all legitimate $V_i$'s. That is, $V = \cup V_i$.
6: If $m_{a,} m_b$ are found such that, $|L_a - L_b| > 2r$ SU $j$ employs the Helper Resolution (HR) algorithm to discard rogue $m_i s$ .
7: Once all inconsistent messages have been discarded, the occupancy vector $V$ is computed as in Step 5.
```

The helpers distribute spectrum information to the SUs. Contrary to the work in [1], in our design, this is achieved using solely cryptographic methods. This is preferred to avoid the need for frequent SU training due to mobility. To update the spectrum state to nearby SUs, a helper transmits the following information.

$$g_i : m_i \parallel sig_{sk_i}(m_i),\ m_i : V_i \parallel L_i \parallel SN_i \qquad (21)$$

In (equ 21), V_i is the occupancy vector of helper i, $L_i = (X_i, Y_i)$ is the location of helper i, SN_i is the transmission sequence number used for verifying the freshness of V_i, and $sig_{sk_i}(m_i)$ is the signature of i on m_i using i′s private key sk_i. To avoid the frequent broadcast of spectrum information, the helpers update the SUs if, (a) a change in PU activity has been sensed, or (b) an SU moving to a new location has requested for an update. Note that for PUs such as TV stations, the dynamics of PU activity is expected to be low (in the order of hours). Therefore, while the helpers continuously monitor the spectrum status, a frequent update of the SUs may not be necessary. On the other hand, for other types of PU networks such as cellular networks, PU activity can be more dynamic.

Once an SU node j has obtained the occupancy vectors V_i from nearby helpers, it executes the Spectrum Authentication (SA) algorithm shown in Algorithm 1. Here, we assume that the network of helpers is loosely synchronized to the same transmission sequence number. The SA algorithm includes several cryptographic and topology consistency checks to ensure that the spectrum information obtained by SUs is authentic and fresh.

5. SIMULATION RESULTS

In this we evaluate the countermeasure performance of the proposed TCS method. The results are obtained using NS-2 simulator. We place an attacker in the centre of the network, considering a three band CR network where 50 primary nodes are operating in one band. The number of secondary nodes can be varied from 50 to 200. This paper investigate DoS attack countermeasures after successful spectrum sensing. The Fig 2 and Fig 3 shows the survival percentage of primary and secondary users for a single attacker. The Fig 4 shows the total survival percentage of all the nodes in the network with respect to time. The Fig 5 and Fig 6 shows the outage probability of primary and secondary user in the network. The results of primary user authentication performance will be also shown in this network.

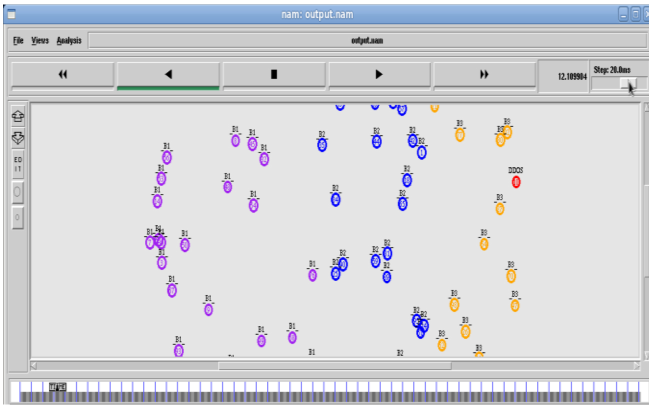

Fig 1: MUB network with B1, B2 & B3

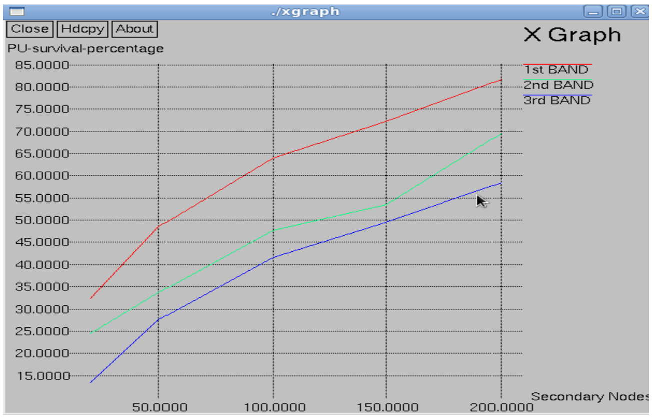

Fig 2: Survival percentage of primary nodes

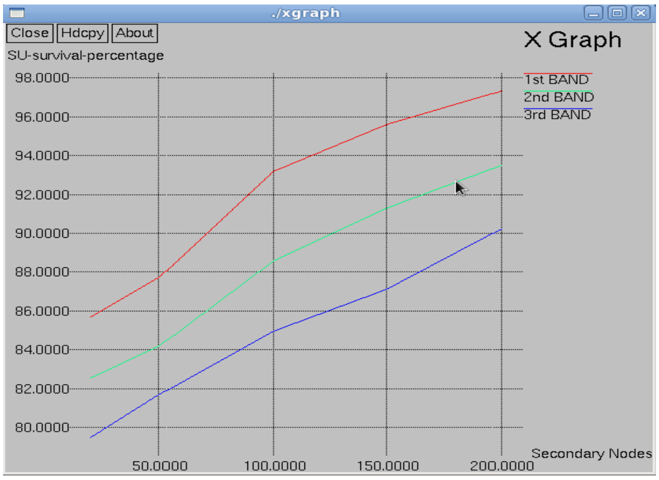

Fig 3: Survival percentage of secondary nodes

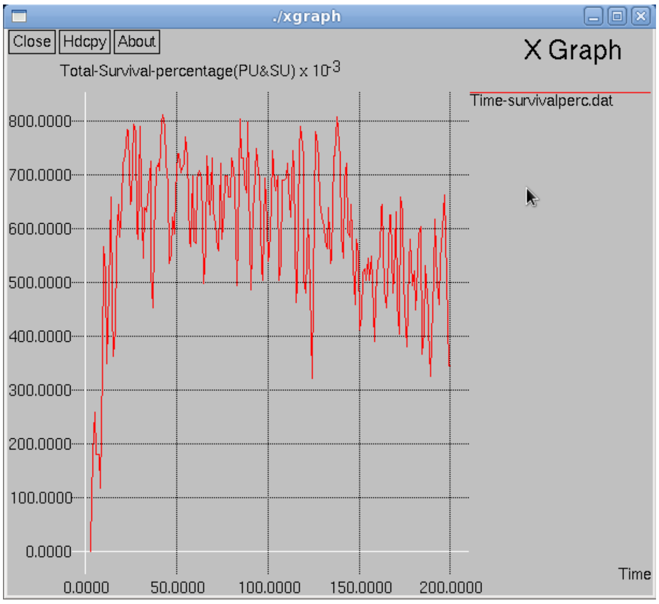

Fig 4: Total survival percentage of all nodes

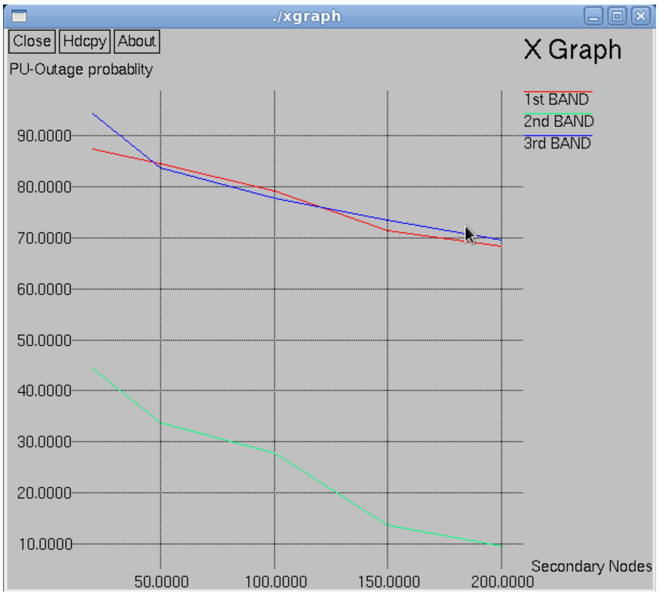

Fig 5: Outage probability of primary nodes

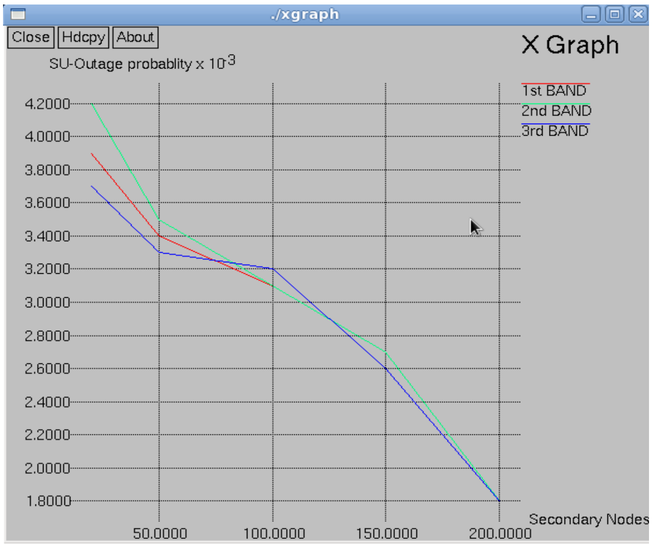

Fig 6: Outage probability of secondary nodes

6. CONCLUSION

In this paper, we introduce a MUB attack and have shown the impact on CR network. We then proposed a MUB attack countermeasure, TCS and then an authentication system that relies on the deployment of a network of helper nodes for verifying the availability of idle spectrum. The helper nodes authenticate the PU using link signatures which is a channel property between any two nodes. The SUs authenticate the helper nodes by verifying their cryptographic signatures. Our security analysis showed that our authentication system can withstand impersonation attacks of the PUs as well as of the helper nodes. Numerical result shows that TCS outperforms CR's inherent signal avoidance features.

7. REFERENCES

[1] J. Mitola and G. Maguire, "Cognitive radio: making software radios more personal," *IEEE Personal Commun.*, vol. 6, 1999.

[2] S. Arkoulis, L. Kazatzopoulos, C. Delakouridis, and G. F. Marias, "Cognitive spectrum and its security issue," *2008 International Conference on Next Generation Mobile Applications, Services and Technologies*.

[3] J. L. Burbank, "Security in cognitive radio network: the required evolution in approaches to the wireless network security," *2009 International Conference on Cognitive Radio Oriented Wireless Networks and Communications*.

[4] T. C. Clancy and N. Goergen, "Security in cognitive radio network: threat and mitigation," *2008 International Conference on Cognitive Radio Oriented Wireless Networks and Communications*.

[5] R. Chen, J. M. Park, and J. H. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 26, pp. 25–37, 2008.

[6] Y. Zhang, G. Xu, and X. Geng, "Security threats in cognitive radio networks," *2008 IEEE International Conference on High Performance Computing and Communications*.

[7] T. X. Brown and A. Sethi, "Potential cognitive radio denial of service attacks and remedies," *2007 International Symposium on Advanced Radio Technologies*.

[8] W. Wang, "Denial of service attacks in cognitive radio networks," *2010 International Conference on Environmental Science and Information Application Technology*.

[9] C. Cordeiro, K. Challapali, D. Birru, and N. S. Shankar, "IEEE 802.22: the first worldwide wireless standard based on cognitive radios," *2005 IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks*.

[10] H. Li and Z. Han, "Dogfight in spectrum: jamming and anti-jamming in multichannel cognitive radio systems," *2009 IEEE Global Telecommunications Conference*.

[11] L. Wang and Y. Wang, "Method for security enhancement of cognitive radio system," *2009 International Symposium on Intelligent Ubiquitous Computing and Education*.

[12] J. Ma, Y. Zhong, and S. Zhang, "Frequency-hopping based secure schemes in sensornets," *2005 International Conference on Computer and Information Technology*.

[13] K. Bian and J.-M. Park, "Security vulnerabilities in IEEE 802.22," *2008 International Wireless Internet Conference*.

[14] Z. Jin, S. Anand, and K. Subbalakshmi, "Mitigating primary user emulation attacks in dynamic spectrum access networks using hypothesis testing," *ACM Mobile Computing and Commun. Rev.*, vol. 13, 2009.

[15] K. Whitehouse, C. Karlof, and D. Culler, "A practical evaluation of radio signal strength for ranging-based localization," *ACM Mobile Computing and Commun. Rev.*, vol. 11, 2007.

[16] N. Li and P. Li, "A range-free localization scheme in wireless sensor networks," *2008 IEEE International Symposium on Knowledge Acquisition and Modeling Workshop*.

[17] Y. Chen, W. Trappe, and R. P. Martin, "Attack detection in wireless localization," *2007 IEEE International Conference on Computer Communications*.

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

[19] H. Kim and K. Shin. In-band spectrum sensing in cognitive radio networks: energy detection or feature detection? In *Proceedings of MOBICOM*, pages 14–25, 2008.

[20] B. Wild and K. Ramchandran. Detecting primary receivers for cognitive radio applications. In *Proceedings of IEEE DySPAN*, pages 124–130, 2005.

[21] Q. Yuan, P. Tao, W. Wenbo, and Q. Rongrong. Cyclostationarity based spectrum sensing for wideband cognitive radio. In *Proceedings of the WRI International Conference on Communications and Mobile Computing*, volume1, 2009.

[22] N. Patwari and S. Kasera. Robust location distinction using temporal link signatures. In *Proceedings of MOBICOM*, page 122, 2007.