Journal of Theoretical and Applied Information Technology
10th March 2014. Vol. 61 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

EVALUATION OF MOST USER BAND (MUB) ATTACK IN A COGNITIVE RADIO NETWORK BASED ON SUB-NYQUIST SAMPLING

[1]R.SABITHA, [2]Dr.K.R.SHANKAR KUMAR,[3]CHRISTO REEGAN RAJ.V, [4]RAMYA BHARANI.G

[1] Department of ECE, Sri Krishna College of Engineering and Technology, CBE.
[2] Department of ECE, Ranganathan Engineering College, CBE.
[3] Department of ECE, Sri Krishna College of Engineering and Technology, CBE.
[4] Department of ECE, Sri Krishna College of Engineering and Technology, CBE.

E-mail: [1]sabitha@skcet.ac.in

ABSTRACT

The unused or under-utilized TV bands are opportunistically utilized by Cognitive Radio enabled IEEE 802.22 Wireless Regional Area Networks(WRAN). However due to the nature of cognitive radio networks and lack of proactive security protocols, the IEEE 802.22 networks are vulnerable to various Denial of Service (DoS) threats. In this paper the target band for DoS attack is a specific band called as Most User Band which has maximum number of users among the available sub bands in the CR network. We propose a countermeasure strategy (Time concealment strategy), to counter the MUB attack. Simulation results are provided to demonstrate the effectiveness of the proposed MUB attack and TCS with attack time control for further survival improvement of secondary nodes.

Keywords:- *Cognitive Radio, Denial Of Service Attack, Most User Band Attack, Sensing Time, Attack Time Control.*

1. INTRODUCTION

The economical problem with fixed spectrum assignment policy has the suboptimal use of spectrum resource leading to overutilization in some bands and under utilization in others[2-4].This observation has lead to the recent spectrum reforms by the U.S. Federal Communication Commission(FCC)[27]. The Dynamic Spectrum Access(DSA) for enhanced spectrum utilization for adaptive networks is achieved via the CR[5,6].CR is an emerging wireless communication technology aims at using DSA to allow the unused ,licensed TV frequency spectrum to be used by unlicensed users on a non-interfering basis[7]. An essential requirement of CRs is that they must rapidly fill the spectrum holes (ie, portions of the licensed

band unused spectrum) without causing harmful interference to Primary users. To protect the primary incumbent services, IEEE 802.22 devices are required to perform spectrum sensing and evaluate promptly upon the return of the licensed users [8]. However there are security vulnerabilities[28] in CR networks. Attacks at the physical layer and MAC layer including DoS attacks and countermeasures have been investigated in [9-20].

Our work differs from [21] in two ways: First, in [21] the band under attack is the band with most signal activities ie, Most Active Band[MAB]. But in our work we choose a specific band for DoS attack which has most users or maximum number of users than in all the other available bands in the CR network. Second, here spectrum sensing is based on the subnyquist sampling [22] with various sensing time in order to increase the accuracy in secondary node detection depending on that attack time on MUB is decided.

In this paper we investigate a type of DoS attack and evaluate its impacts considering a timely distributed multiband CR network. In this attack, a malicious CR node or agent senses the number of users over each band otherwise called as sub band (spectrum sensing through sub-nyquist sampling and energy detection) and then attack the band with maximum number of users to achieve maximum attack outcome. The band under attack could have either primary or secondary users. We refer this as the Most User Band (MUB) attack. We further introduce a countermeasure against MUB attack

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

known as Time Concealment Strategy (TCS). Our results show that TCS outperforms the CR inherent signal avoidance feature. We also consider the attack time control capability in CR nodes to achieve improved TCS countermeasure. Such a MUB attack scenario could occur in a public service radio with both legacy nodes CR node, where a malicious node or agent exploits the spectrum sensing and cognitive engine capabilities to launch most effective DoS attacks. Also in a CR network at a given time, there will be some sacrificing nodes (nodes in the band under attack) in order to protect survival nodes(nodes not in the attack band). A secondary user node status as sacrificing node or survival node also changes with time. Hence it is necessary to address the Most user band attack with time control with respect to sensing time.

The main contributions of this paper are as follows:

- Formulation of Maximum user band for DoS attack in IEEE 802.22 networks.
- Formulation of sensing time to decide attack time using subnyquist sampling.
- Investigation of MUB attack and its countermeasure.

The rest of the paper is organized as follows: In section II, we formulate the MUB attack in CR network. The TCS is introduced in section III. Formulation of attack time related to sensing time and TCS performance results are presented in section IV. Conclusions are drawn in section V.

2. MOST USER BAND ATTACK

A. Most User Band Attack:

The following assumptions are made, number of primary nodes Np, number of secondary nodes Ns and M number of bands in a CR. Maximum user band which can be allocated with a band capacity C. We implemented subnyquist sampling based energy detection for accuracy in sensing. So that all the nodes are getting separated from band with primary nodes. Let the 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 intentional 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 bands namely Imax ,IImax and IIImax.

In this paper sub-Nyquist sampling known as compressive sampling based energy detection is also used for efficient detection of users in a subband.. Sub-Nyquist sampling refers to the technique of recovering signal from samples obtained using a rate below the nyquist rate.The advantages of sub-nuquist sampling are less memory requirements and low complexity.

Through spectrum sensing the location of active primary frequency band has been determined with the prior information of upper bound M on the total number of active bands and maximum band width Wmax of the active sub band. The MUB attacker selects the band (band i*) as its target if,

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

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 described in (2). Primary node operates in one primary band described in (3).

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

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

$x_{ij}\in\{0,1\}=1$ 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 evaluating the performance of CR network under MUB attack we calculate the number of surviv ing 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.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

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

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

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 percentage 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)).

B. Mub Attack Countermeasures

In this section we introduce MUB countermeasure known as time concealment strategy, which depends on the sensing time based on Sub-Nyquist sampling and attack time. Longer the sensing time leads to 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 to utilize a co-operate CR network in which 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 because 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.

C. Impact Of Most User Band Attack

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 is unable to avoid the attacker since they have no Spectrum sensing and reconfiguration capabilities. Here it is assumed that a assume that the CR has v sub-Nyquist sampling branches, the wideband filter prior to the samplers removes frequencies outside the spectrum of interest and is set to have a bandwidth W. At the ith branch, the low-rate sampler samples the received signal at the sub-Nyquist rate fi(Hz)<2W.The DFT spectrum of the sampled signal is then computed by applying the Fast Fourier Transform(FFT) to the samples in each branch. After that these DFT spectra are used to reconstruct the wideband spectrum and is detected by energy detection approach.

Journal of Theoretical and Applied Information Technology
10th March 2014. Vol. 61 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

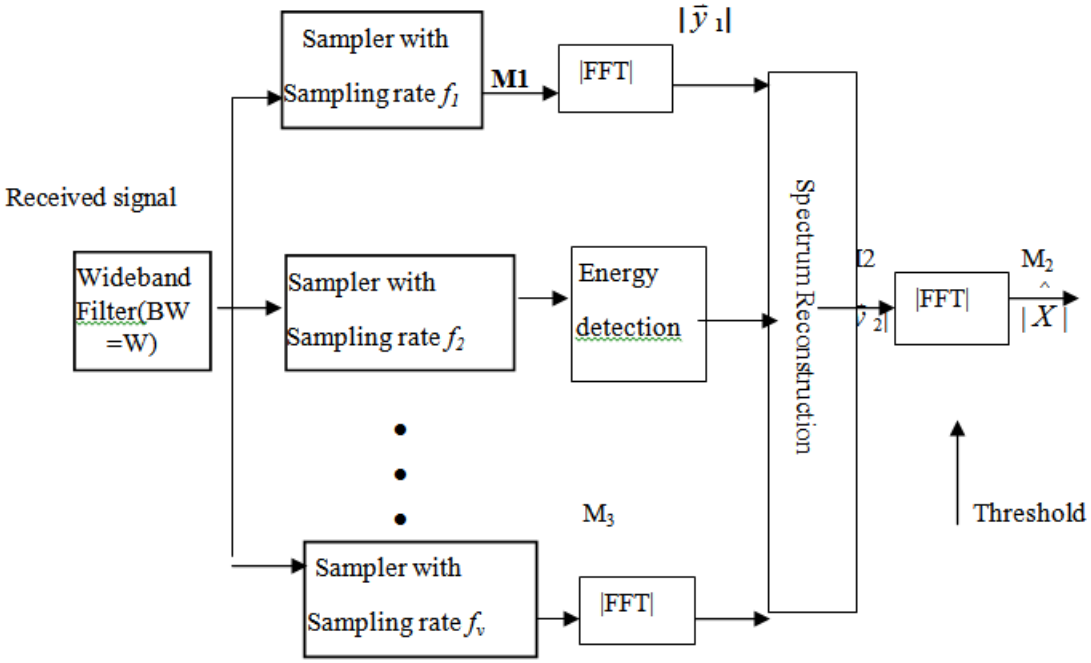


Fig.1.Schematic Illustration Of The Sub-Nyquist Sampling System In One CR Node.

When the MUB attacks target on one secondary band, the secondary nodes could hop to another nodes to avoid the MUB attacker. The MUB attacker could follow the secondary nodes due to its Sub-Nyquist sampling based on energy detection capabilities.Therefore the CR's intended signal 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 it to its new operating band. Hence MUB attack is a 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 sacrificing nodes are derived as follows. To have maximum survivability the number of CR nodes (j) in the attack band i* to be minimum.

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

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

$$\sum_{k=1}^{N_p} x_{i^*k} = 0 \qquad (9)$$

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

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

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

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

Each primary node is operating in one primary band only

$$\sum_{k=1}^{N_p} x_{ik} = 1 \qquad (12)$$

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The node capacity in each band is given by

$$\sum^{N_s} x_{ij} \le c, \sum^{N_s} x_{ik} \le c \quad (13)$$

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 [23].

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

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

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 [24], [25]. Localization of attacker play an important role in CCS implementation and some related studies of attacker localization have been reported in [11] and [26].

Wideband spectrum sensing based on Sub-Nyquist sampling is used to derive the signal presence. Based on that a central agency or node 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 decrease 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

$$\sum_{j=1}^{N_S} x_{i*j} T_j + \sum_{k=1}^{N_P} x_{i*k} \ge \sum_{j=1}^{N_S} x_{ij} T_j + \sum_{j=1}^{N_P} x_{ik} \forall i \in \{1,2....,M\} \quad (16)$$

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 Tu and minimum attack time T_L, the attack time control range of secondary nodes.

$$T_L \le \forall T_j \le T_U \quad (17)$$

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

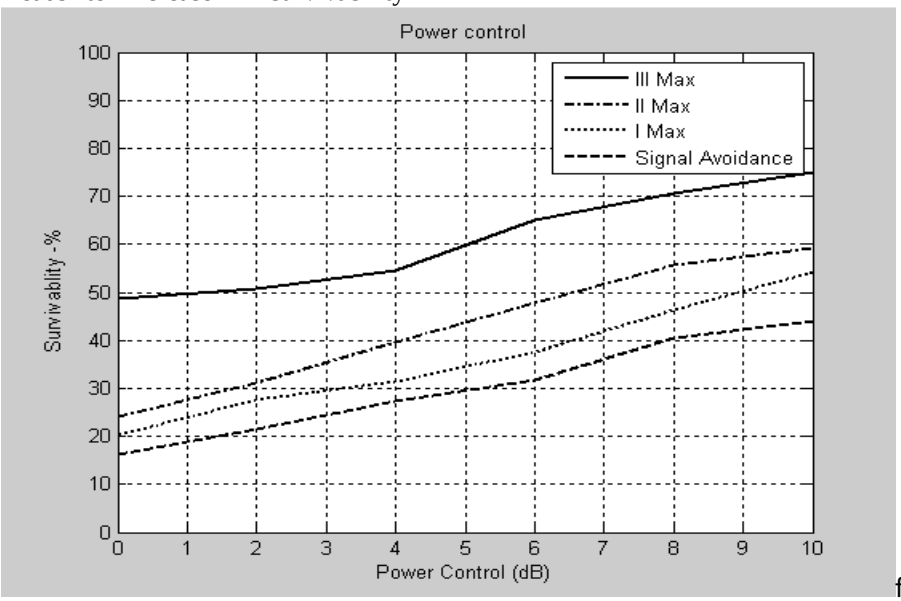
$$\sum_{j=1}^{Ns} T_j = Ns \quad (18)$$

4. SIMULATION RESULTS

We provide 3 simulation setups for calculating sensing time and hence attack time by varying the down sampling factor. We assume that there are M=5 sub bands in the frequency range (0, f_{max}) = [0, 1.0]GHz. hence the nyquist rate is f_{max} =1/To=1GHz.the bandwidth of each sub band are 5MHz.The down sampling factor is chosen as L=20,corresponding to the Sub-Nyquist rate of 1/LTo=75MHz(>B_{max}=5MHz). FFT size considered here is N=12000, corresponding to the sensing time Z=NLTo =12000x20x (1/1.0) GHz and 240 us. The second and third attack times are calculated by considering the down sampling factor of L=12and 15.The sensing times are calculated and the attack times are taken to be the multiples of sensing times. The results are obtained using Matlab simulation. The geographical locations of primary and secondary node are determined by (14) and (15) with R=1000m and Ro=10m we place the attacker in the centre of a simulated network. Where 50 primary nodes are operating within one band (M_P=1).the capacity of each band C is assumed to be 70. The number of nodes varies from 30 to100. The probability of detection at a particular sensing time is assumed to be included a path loss with exponent of 3 with Rayleigh fading. There are several essential elements in CR networks including the dynamic primary user (ON/OFF or presence or absence). This paper investigates a DOS attack/counter measures or strategies after

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

successful spectrum sensing on or primary user determinations (identification of channel occupied by primary nodes). A fixed upper and lower power levels are maintained for each subband. Hence as the MUB is attacked with increased power level, only less number of nodes are enough to contribute to power level, hence there are more surviving nodes which leads to increase in survivability percentage. Investigations are done for more user bands also ie, IImax and IIImax. As the number of nodes in a band decreases sacrificing nodes also decreases with variation in power level, hence we can say Imax is producing maximum net outcome for attack. This is graphically plotted in figure 2 before countermeasure.



fv

Figure 2.Survival Percentage Of Both Primary And Secondary Users Vs Power Control Graph For MUB Attack. The Number Of Frequency Bands M=5; Maximum Node Capacity C=70. Imax=70,Iimax=50 And Iiimax=35 Number Of Users.

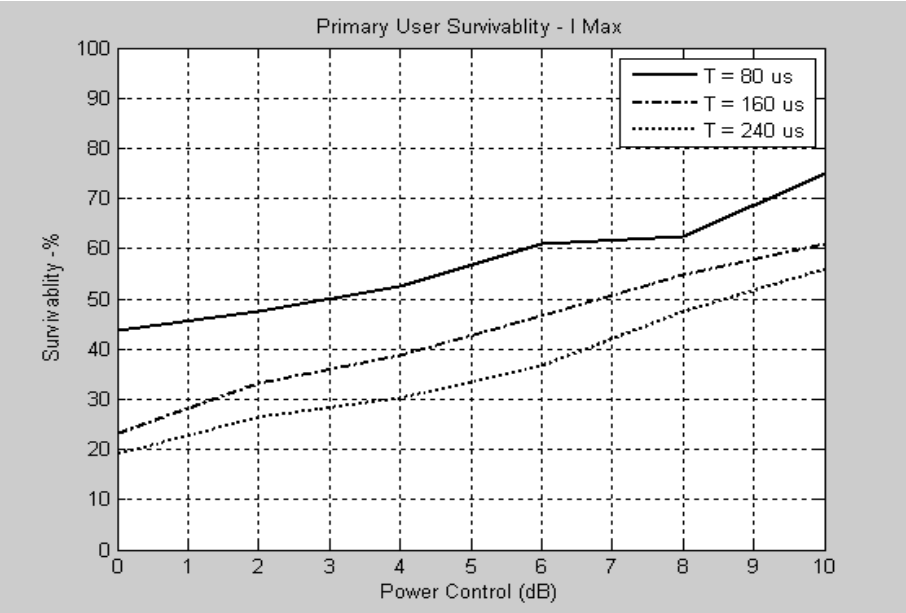


Figure 3: Survival Percentage Of Primary Users Vs Power Control Graph For MUB Attack. The Number Of Frequency Bands M=5; Maximum Node Capacity C=70. Imax=70 Number Of Users.

Journal of Theoretical and Applied Information Technology
10th March 2014. Vol. 61 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

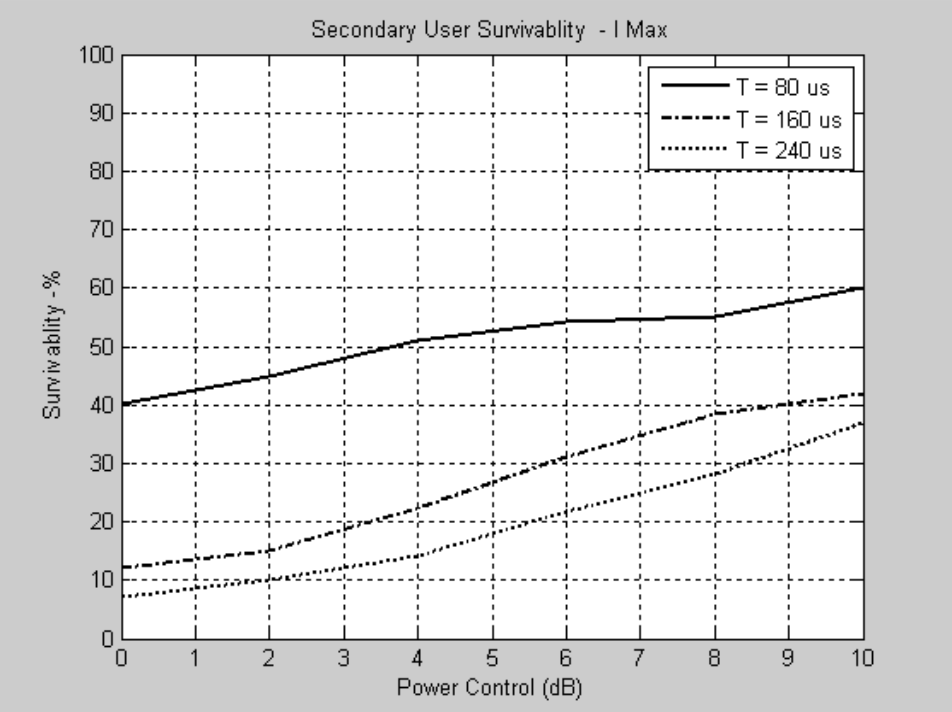


Figure 4: Survival Percentage Of Secodary Users Vs Power Control Graph For MUB Attack. The Number Of Frequency Bands M=5; Maximum Node Capacity C=70. Imax=70 Number Of Users. T Represents Attack Time In Microseconds.

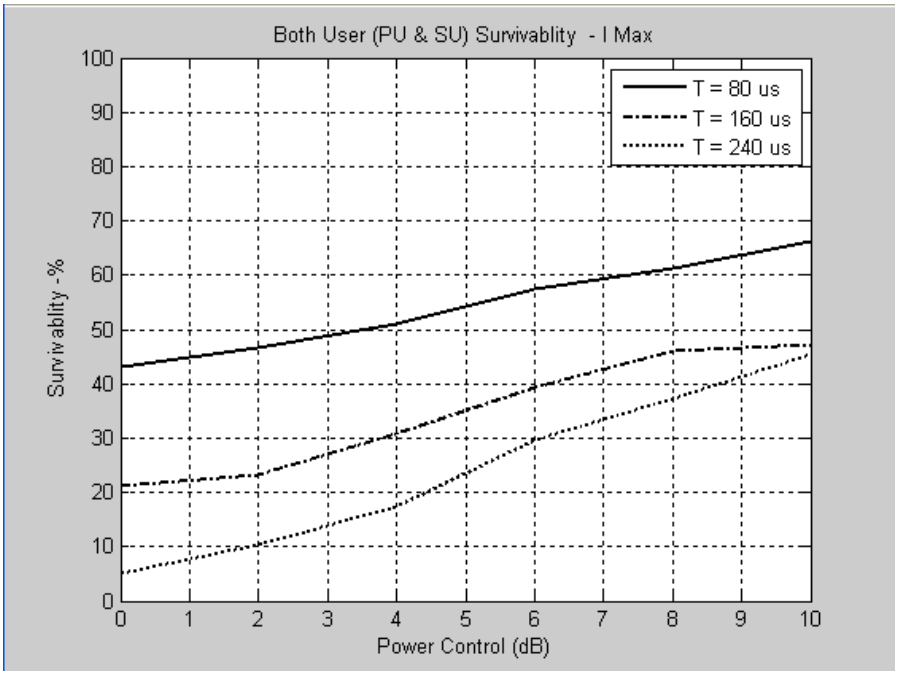


Figure 5: .Survival Percentage Of Both Primary User Sand Secondary Users Vs Power Control Graph For MUB Attack. The Number Of Frequency Bands M=5; Maximum Node Capacity C=70. Imax=70 Number Of Users. T Represents Attack Time In Microseconds.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

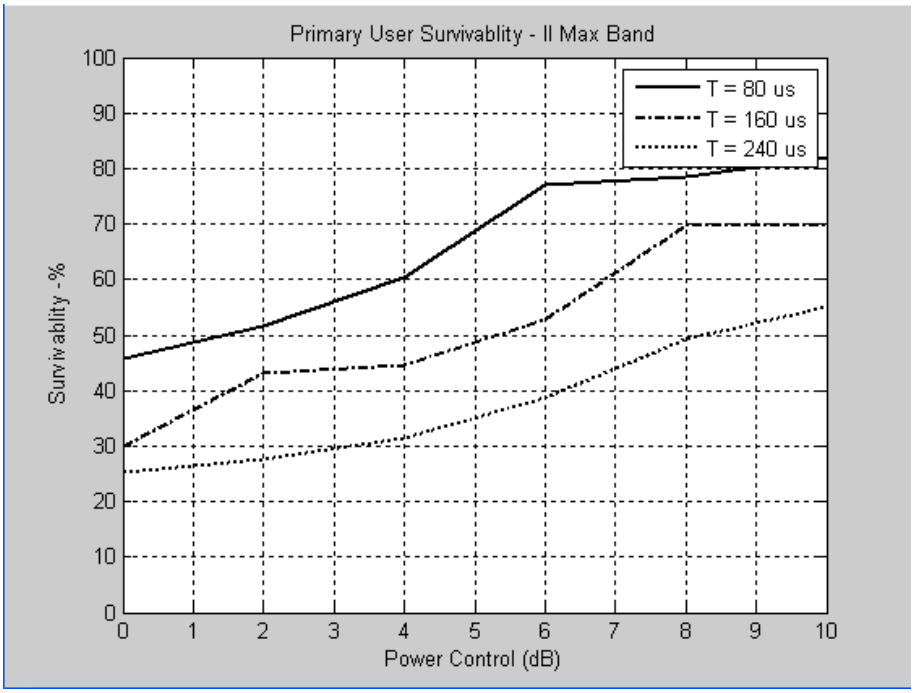


Figure 6:.Survival Percentage Of Primary User Vs Power Control Graph For MUB Attack. The Number Of Frequency Bands M=5; Maximum Node Capacity C=70. Iimax=50 Number Of Users. T Represents Attack Time In Microseconds.

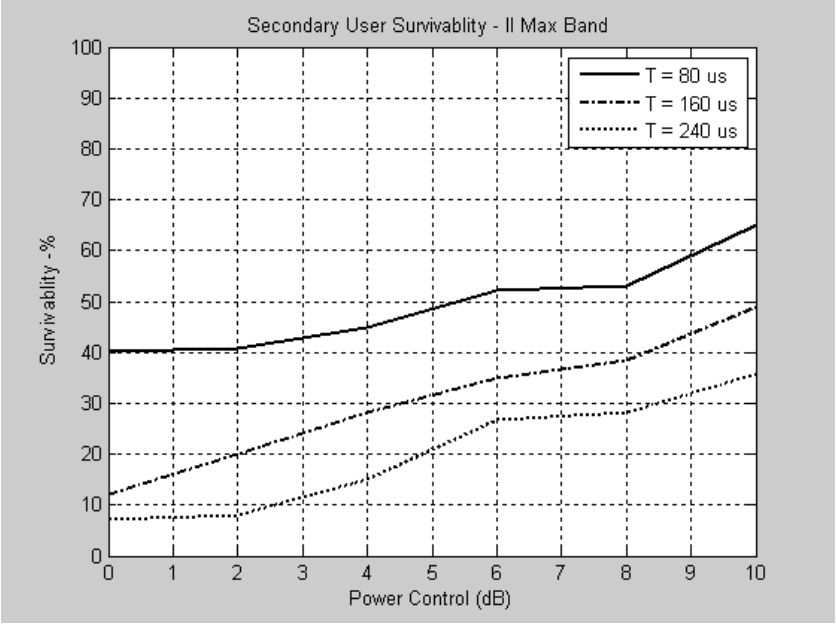


Figure 7:.Survival Percentage Of Both Primary User And Secondary Users Vs Power Control Graph For MUB Attack. The Number Of Frequency Bands M=5; Maximum Node Capacity C=70. Iimax=50 Number Of Users. T Represents Attack Time In Microseconds.

Journal of Theoretical and Applied Information Technology
10th March 2014. Vol. 61 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

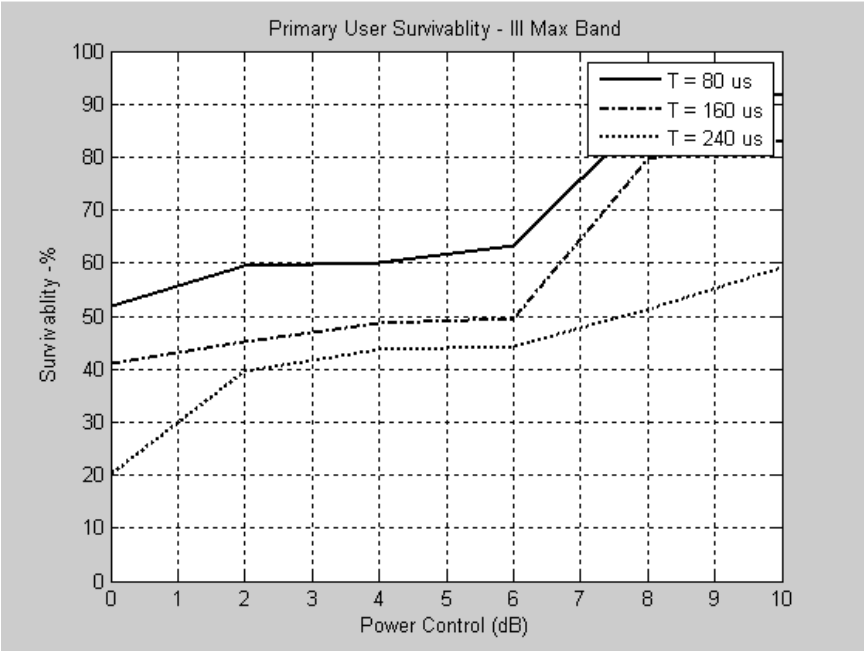


Figure 8: Survival Percentage Of Primary User Vs Power Control Graph For MUB Attack. The Number Of Frequency Bands M=5; Maximum Node Capacity C=70. Iiimax=35 Number Of Users. T Represents Attack Time In Microseconds.

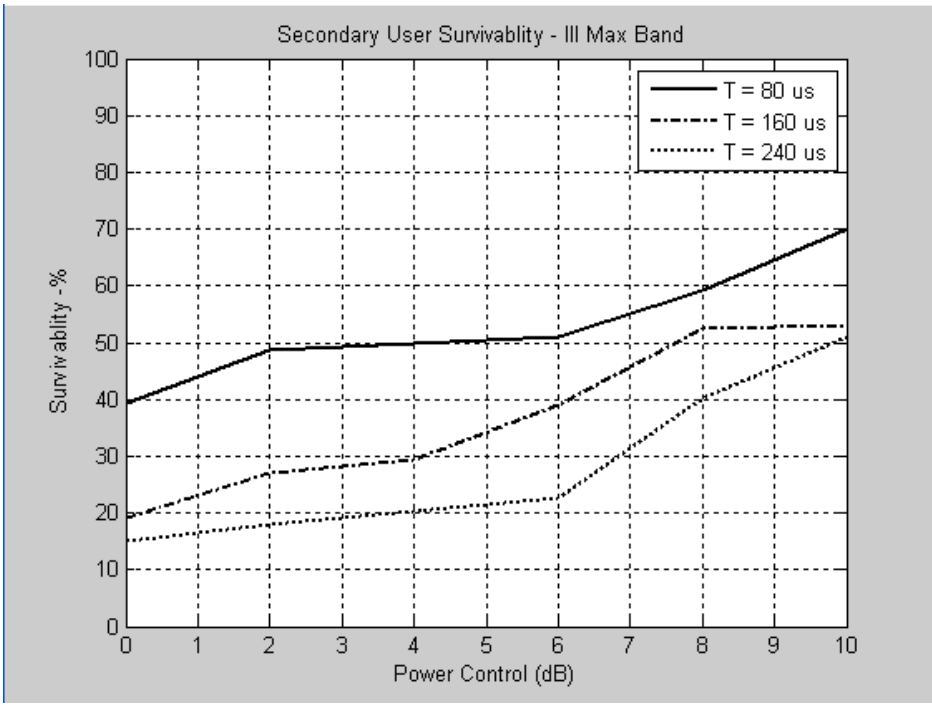


Figure 9: .Survival Percentage Of Secondary User Vs Power Control Graph For MUB Attack. The Number Of Frequency Bands M=5; Maximum Node Capacity C=70. Iiimax=35 Number Of Users. T Represents Attack Time In Microseconds.

.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

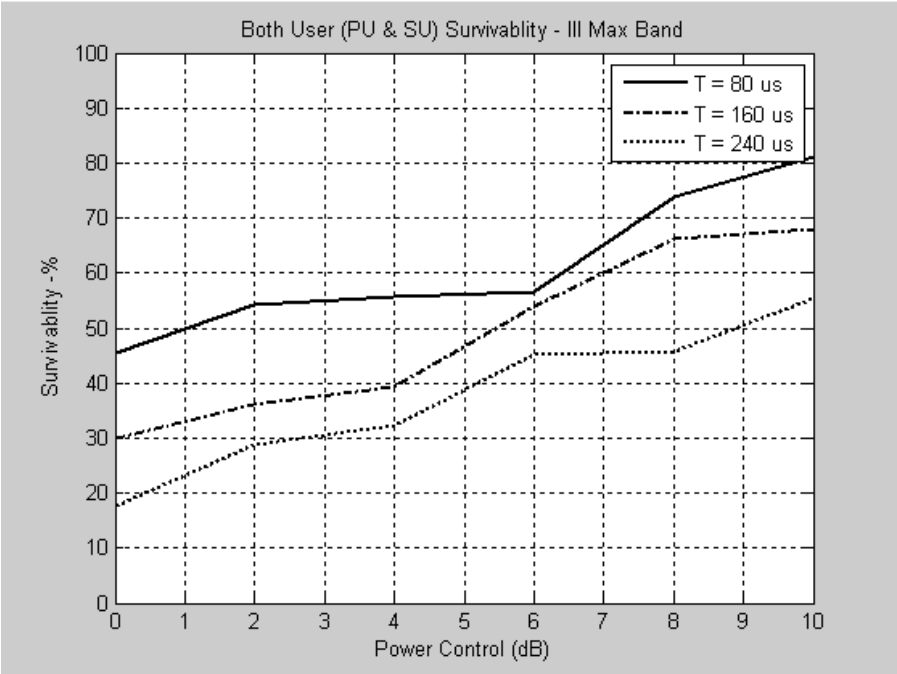


Figure 10:.Survival Percentage Of Both Primary Users And Secondary Vs Power Control Graph For MUB Attack. The Number Of Frequency Bands M=5; Maximum Node Capacity C=70. Iiimax=35 Number Of Users. T Represents Attack Time In Microseconds.

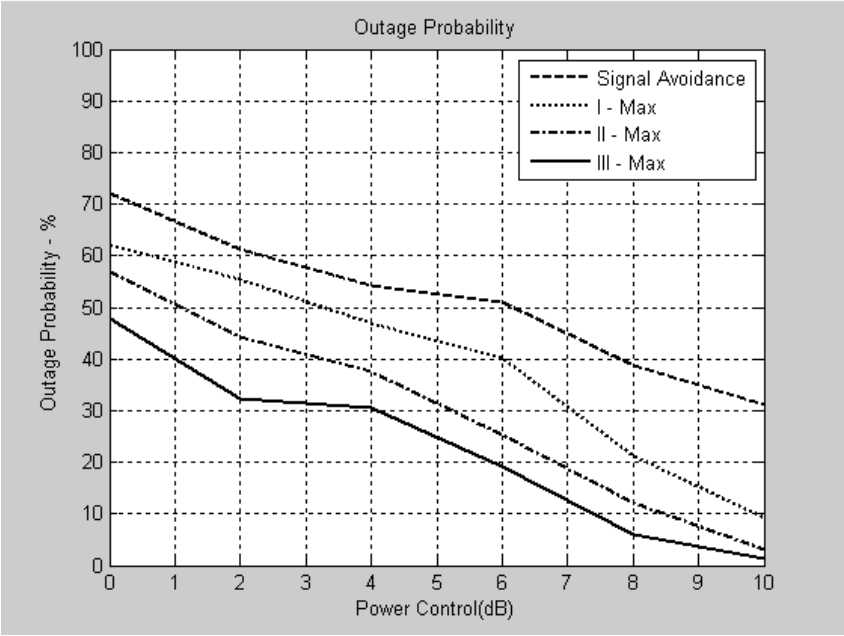


Figure 11: Outage Probability Percentage Of Primary And Secondary Users Vs Power Control Graph For MUB Attack. The Number Of Frequency Bands M=5; Maximum Node Capacity C=70. Imax=70,Iimax=50 And Iimax=35 Number Of Users

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

All figures show the survivability percentage and outage probability measures obtained for primary and secondary users individually and for both primary and secondary users combined under Most User Band (MUB) attack. The measures obtained for varying number of users such as Imax,IImax and IIImax is compared with Signal Avoidance feature of Cognitive Radio Network. Also same performance measures is obtained for varying number of users and are compared individually at different attack times. From the above graph, it is clear that the proposed method is better than the inheritance signal avoidance feature of CRN.

Figure 2 shows the survivability percentage obtained for both primary and secondary users combined under Most User Band (MUB) attack. The measure obtained for varying number of users such as Imax, IImax and IIImax is compared with Signal Avoidance feature of Cognitive Radio Network. From the above graph, it is clear that the proposed method is better than the inheritance signal avoidance feature of CRN.

Figure 3 shows the survivability percentage obtained for primary users under Most User Band (MUB) attack. The performance measure is obtained for Imax=70 and is compared individually at different attack times T=80us,160us and 240us. From the above graph, it is clear that the survivability percentage increases by lowering the attack time.

Figure 4 shows the survivability percentage obtained for secondary users under Most User Band (MUB) attack. The performance measure is obtained for Imax=70 and is compared individually at different attack times T=80us,160us and 240us. From the above graph, it is clear that the survivability percentage increases by lowering the attack time.

Figure 5 shows the survivability percentage obtained for both primary and secondary users under Most User Band (MUB) attack. The performance measure is obtained for Imax=70 and is compared individually at different attack times T=80us,160us and 240us. From the above graph, it is clear that the survivability percentage increases by lowering the attack time.

Figure 6 shows the survivability percentage obtained for primary users under Most User Band (MUB) attack. The performance measure is obtained for IImax=50 and is compared individually at different attack times T=80us,160us and 240us. From the above graph, it is clear that the survivability percentage increases by lowering the attack time.

Figure 7 shows the survivability percentage obtained for secondary users under Most User Band (MUB) attack. The performance measure is obtained for IImax=50 and is compared individually at different attack times T=80us,160us and 240us. From the above graph, it is clear that the survivability percentage increases by lowering the attack time.

Figure 8 shows the survivability percentage obtained for primary users under Most User Band (MUB) attack. The performance measure is obtained for IIImax=35 and is compared individually at different attack times T=80us,160us and 240us. From the above graph, it is clear that the survivability percentage increases by lowering the attack time.

Figure 9 shows the survivability percentage obtained for secondary users under Most User Band (MUB) attack. The performance measure is obtained for IIImax=35 and is compared individually at different attack times T=80us,160us and 240us. From the above graph, it is clear that the survivability percentage increases by lowering the attack time.

Figure 10 shows the survivability percentage obtained for both primary and secondary users under Most User Band (MUB) attack. The performance measure is obtained for IIImax=35 and is compared individually at different attack times T=80us,160us and 240us. From the above graph, it is clear that the survivability percentage increases by lowering the attack time.

Figure 11 shows the outage probability percentage obtained for both primary secondary users under Most User Band (MUB) attack. The measure obtained for varying number of users such as Imax, IImax and IIImax is compared with Signal Avoidance feature of Cognitive Radio Network. From the above graph, it is clear that the proposed method is better than the inheritance signal avoidance feature of CRN

5. CONCLUSION

In this paper, we propose a new attack called as MUB attack and its impacts on a CR network are investigated for three different bands namely Imax,IImax and IIImax. It is compared with the inherit signal avoidance feature of CRN.The MUB attack countermeasure based on sub-nyquist sampling ,TCS is also proposed. Numerical results indicate that TCS performs better than other signal avoidance technique. For this reason the this countermeasure has more accuracy and less complexity.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

REFERENCES

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

[2] F.C.C.,"Spectrum policy task force," *IEEE Trans. Inf. Forens. Security*, pp. 02-155,Nov 2002.

[3] F.C.C., "In the matter of unlicensed operation in the TV broadcastbands," *Second Report and order and Memorandam opinion and Order,no*. FCC-08-260A1, Nov.2008.

[4] C.Bazelon, "Licensed or unlicensed: The economic considerations in increment spectrum allocations," New Frontiers in Dynamic Spectrum Access Networks, *2008 DySPAN 2008. 3rd IEEE Symposium on*, pp1-8, Oct. 2008.

[5] I. Mitola, J. and J.Maguire, G.Q., "Cognitive Radio: making software radios more personal," *IEEE Pers., Commun*. Vol6, no 4,pp. 13-18, Aug. 1999.

[6] I.F. Akyildiz, W.Y.Lee, M.C.Vuran, and S.Mohanty, "Nextgeneration/dynamic spectrum access/Cognitive radio Wireless Networks:a Survey," *Comput. Netw*., vol 50, no.13, pp.2127-2159,2006

[7] C.R. Stevenson, G.Chouinard, Z.Lei, W.Hu, S.J.Shellhammer, and W.Caldwell, IEEE 802.22: The first cognitive radio wireless regional area network standard," *IEEE Commun. Mag*., Jan 2009.

[8] IEEE 802.22 WG, "IEEE p802.22/d0.1 draft standard for wireless regional ares networks part:22 Cognitive Radio ran Medium Access Control (MAC) and Physical layer (PHY) specifications: *Policies and procedures for operation in the TV bands", IEEE docs*, May 2006.

[9] 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*.

[10] 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*.

[11] 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*.

[12] 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.

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

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

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

[16] 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*.

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

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

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

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

[21] Nansai Hu,Yu-Dong Yao and Joseph Mitola, "Most Active Band (MAB) Attack and Countermeasures in a Cognitive Radio Network," *IEEE Transactions on Wireless Communications*, vol.11, no.3, pp-898-902. 2012.

[22] Hongjian Sun, Wei-Yu Chiu, Jing Jiang,Arumugam Nallanathan and H.Vincent Poor,"Wideband Spectrum Sensing with Sub-Nyquist Sampling in Cognitive Radios" *IEEE Transactions on Signal processing*, vol.16,no.11,pp-6068-6073.

[23] Z. Jin, S. Anand, and K. Subbalakshmi, "Mitigating primary user emulation attacks in dynamic spectrum access networks using

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

hypothesis testing," *ACM Mobile Computing and Commun. Rev.*, vol. 13, 2009.

[24] 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.

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

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

[27] Md.AliHussain, Md. Mastan and Syed Umar, "Quality of Service Issues in Wireless Ad-Hoc Network (IEEE 802.11B*)", International Journal of Computer Science & Information Security (IJCSIS),* Vol.8 No.3 June 2010, ISSN: 1047 – 5500.

[28] Muazzam A. Khan, Ghalib A. Shah, Muhammad Sher, "A QoS Based Multicast Communication Framework for Wireless Sensor Actor Networks (WSANs)", *International Journal of Innovative Computing, Information and Control*, Volume 7, Number 1, January 2011.