Asian Journal of Electrical Sciences
ISSN: 2249-6297 (P) Vol.1 No.1, 2012, pp.58-62

DOI: https://doi.org/10.51983/ajes-2012.1.1.1647

Distance Difference Test for Detection of Malicious User in Cognitive Radio

Seema Rajput, Amol Chaudhari, Pratiksha Landge and Swapnali Kumbhar
Department of Electronics and Telecommunication Engineering,
Sinhgad Academy of Engineering , University of Pune, Pune - 411 048, India
E-mail: shrajput@rediffmail.com, amolchaudhari141@gmail.com, pratiksha.landge27@gmail.com, swapnalikumbhar999@yahoo.com
(Received on 20 December 2011 and accepted on 15 March 2012)

***Abstract* - A number of wireless applications have been growing over the last decade. Most of the frequency spectrum has already been licensed by government agencies, such as Federal Communications Commission (FCC). Therefore, there exists an apparent spectrum scarcity for new wireless applications and services. Cognitive radio(CR) can efficiently utilize the unused spectrum for secondary usage without interfering a primary licensed user. In cooperative environment, a primary licensed user can share spectrum occupancy information with a secondary user to enable dynamic spectrum access. However, a secondary user needs to verify accuracy of the spectrum occupancy information and it comes from the legitimate primary users. Without the verification, a malicious user can falsify the spectrum occupancy information. This can result in Interference to the primary users and Primary User Emulation attack(PUE) which can minimize spectrum occupancy for secondary user. In this paper, we propose to develop an efficient technique to verify the source of the spectrum occupancy information to be from the legitimate primary user thereby maximizing the spectrum utilization efficiency and minimizing any interference to the primary licensed users.**

***Keywords*: Federal Communication Commission, Cognitive Radio, Primary User Emulation**

I. Introduction

There is an ever increasing demand of the spectrum for emerging wireless application and there is shortage of a spectrum for the wireless application. The allocation of radio frequency band is done by Federal Communications Commission (FCC), such as ISM bands around 900MHz, 2.4GHz & 5.8GHz are located for Industrial, Scientific and mechanical purposes which are prone to interference. Recent policy used has forced to use the spectrum as fragmented disk. As a result the existing spectrum is not utilized efficiently. A survey shows that the frequency band below 3Ghz,only about 6% of spectrum is actually utilized. About 70% of the total spectrum is not utilized. So, the spectrum occupancy information must be used between primary users and secondary users [3]. Dr. Joseph Mitola had envisioned a cognitive radio during his Ph.D.studies. Cognitive radio can be defined as a paradigm for wireless communication in which either a network or wireless network changes its transmission or reception parameters to communicate efficiently avoiding interference with licensed or unlicensed users. This alteration of parameters is based on active monitoring of several factors in the external or internal radio environment, such as radio frequency spectrum, user behavior and network state [2]. The radio should sense the environment constantly, based on the result; it needs to change the parameters giving birth to a cognitive cycle . Fig. 1 shows a basic cognitive cycle.There are four basic functions of the cognitive radios for enabling Dynamic spectrum access are as follows:

a. ***Sensing of Spectrum:*** Cognitive radio need to sense unused spectrum for secondary usage without interfering primary user. The concept called 'white holes' is used to refer the unused space in the spectrum.
b. ***Management of Spectrum:*** Cognitive radio need to find the best available spectrum for optimizing the communication requirements.
c. ***Mobility of Spectrum:*** Cognitive radio need to seamlessly transition the spectrum used for communication, when needed to leave the currently used spectrum.
d. ***Sharing of Spectrum:*** Cognitive radio need to fairly share the available spectrum among the coexisting secondary users.There are two types of spectrum sharing cases viz,co-operative sharing and non co-operative sharing. In co-operative sharing the primary user provides all the information about the spectrum occupancy and unused space i.e white spaces in the spectrum to the secondary user so that it can use unused spectrum and will stay away from primary user used spectrum. In non-cooperative sharing, the secondary user has to sense the unused spectrum and use that spectrum without causing any interference to the primary user.

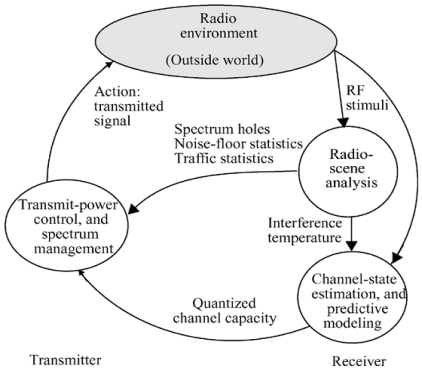

Fig. 1 Basic cognition cycle

Source: (Haykin, 2005)

By enabling secondary utilization of the spectrum, cognitive radios can help in efficient usage of the spectrum. There are different ways to determine the availability of the unused spectrum like, passively sensing the spectrum, using information of the location of the radio to check the database for frequency spectrum usage. There are advantages of cognitive radio like it senses the radio frequency environment for the presence of white spaces. It Manages the unused spectrum and increases the efficiency of the spectrum utilization significantly. It Improves the performance of the overall spectrum by increasing the data rate on good channels and moving away from the bad channels.We can use the unused spectrum for new business propositions,such providing high speed internet in the rural areas and high data rate network applications like video conferencing can be made.

There are different security threats in the Cognitive Radio like Primary User Emulation attack, Malicious Behaviour attack, Denial of Service attack, Actions of Selfish and Malicious users. We are discussing the Primary User Emulation attack and the solution to detect it. Basically in this attack,a malicious user poses as a primary user and transmits signals same as that of Primary User. The Secondary User would blindly believe that the spectrum is occupied by Primary User. In other case, when the Secondary User has occupied the spectrum the malicious tries to access the spectrum by transmitting same characteristics as that of Primary User. The Secondary User therefore has to leave the spectrum. To avoid such situation there need to be a such a permanent characteristic of Primary User known to Secondary User which cannot be copied by any malicious user. The task of distinguishing primary signals from secondary user signals becomes even a greater challenge when one considers the requirement described in FCC's NPRM 03-322 [4], which states that no modification to the incumbent system should be required to accommodate opportunistic use of the spectrum by secondary users. For this reason, conventional approaches, such as embedding a signature in a primary user's signal or employing an interactive protocol between an in primary signal transmitter and a verifier, cannot be used Various methods have been proposed for detecting Primary User Emulation attack like Distance Ratio Test, Distance Difference Test, Finger Print Verification, Joint Position Verification. We are focussing on Distance Difference Test. Basically, the Distance Ratio Test (DRT), uses received signal strength (RSS) measurements obtained from a pair of verifiers to verify the transmitter's location. The second technique, Distance Difference Test (DDT), utilizes the phase difference of the primary user's signal observed at pair of verifiers to verify the transmitter location.

II. Primary User Emulation Attack

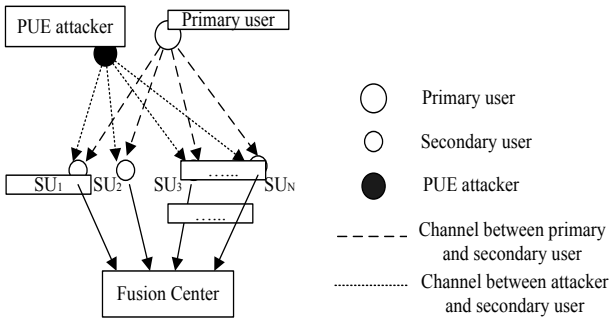

Fig. 2 PUE attack representation

In cognitive radio, when the primary user is not using the spectrum, secondary user sends request for access. The secondary user utilizes the given spectrum until the primary user does not want it for its utilization. Here the malicious user takes the characteristics of the primary user and sends request to leave the respected primary user spectrum. The secondary user therefore leaves the spectrum assuming that it is primary user. This is shown in figure 2.

The major problem in spectrum sensing is to differenciate between primary user and the malicious user. To distinguish between the Primary and Secondary Users, the methods like energy detection, matched filter, cyclostationary process are used. In energy detection method, the Secondary User can recognize only other Secondary User and not of Primary User. When it detects and recognize it concludes that it is Secondary User, otherwise it concludes that it is Primary User. In such situations the Malicious user can send unrecognizable signal and can illegally access the spectrum. The other two methods are capable of recognizing the different parameters and can differenciate between Primary User and Secondary User .But these methods cannot be used to detect Primary User Emulation(PUE) attack. There are two types of PUE attack,viz,Selfish PUE attack and Malicious PUE attack.

A. Selfish PUE Attack: This attack is usually made by two secondary users competing for spectrum access.The attacker wants to access more spectrum for its own utilization and disallow other secondary user from access.Therefore the attacker sends same signal as that of the primary user which restricts other secondary user to access that spectrum.

B. Malicious PUE Attack: The objective of this attack is to obstruct the OSS process of legitimate secondary users i.e., Prevent legitimate secondary users from detecting and using fallow licensed spectrum bands.The attacker might not use the spectrum for its own.

III. Distance Ratio Test and Distance Difference Test

To detect the transmitter sending signals, [5] two location verifiers (LV) are used. The fundamental requirement is that no modification to the primary signal sending system should be required to accommodate opportunistic use of the

spectrum by secondary users as stated by FCC. Therefore the verification needs to be noninteractive i.e the LV's will passively verify the signal transmitted by the user. Let us see how the DRT and DDT method works. We need to make certain assumptions for both the methods like a faithful or properly working location verifier(LV's) is used. Two types of LV's are used viz, Master LV which has a 2-dimensional database of the existing primary and secondary users in surrounding .each LV is assumed to know its location [7] and all LV's can communicate with each other through a common control channel.

A. DRT Method: DRT employs a cooperative distance ratio verification scheme, which is independent of parameters affecting RSS.

In this scheme LV1 and LV2 measures the RSS of the transmitter.LV1 and LV2 both have same parameters except the distance from the source signal.The master LV calculate distance between the source signal(base station) and two LV's using distance co-ordinates. It also calculates the measured distance ratio from the RSS measurement. If the measured distance belongs to calculated distance using coordinates including maximum error then it concludes that user is primary user otherwise it is PUE attacker. The master LV has to check the distance from the whole database and find out the suitable match. If not found then conclude that it is a PUE attacker. The drawback of this method are that the fluctuations due to small scale fading are not considered even if the receivers position changes by one lambda the RSS changes by three to four order of magnitude due to small scale fading. Second, DRT does not consider the fact that the radio propagation model is affected by various environmental variables. Different propagation environments may require the use of different parameters, and may even require the use of totally different propagation models .Practically if an attacker is at location that induces a similar distance ratio as that of the primary user location then the DRT may fail detect the attacker.To avoid this multiple DRT iterations must be used each using different pair of LV's.

B. DDT: The difference in distance can be measured by measuring the phase shift.It does not suffer from the drawback of DDT. In analog stationary system a synchronization pulse is sent periodically which has some specific deviation.In digital stationary system each symbol spans for some period.The distance difference between a signal source and two LVs can be estimated by calculating the time difference in which each LV sees the same synchronization pulse. The time difference is readily converted to distance difference by multiplying the speed of light to the time difference. The analog TV signal have such synchronization pulse which periodically appears every 64ps, with a maximum deviation of 0.25 ts [5] is shown in Figure 3.

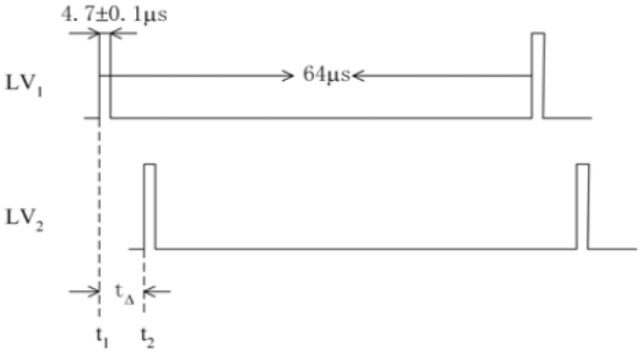

Fig 3.Time gap between two LV's

But if the separation between two consecutive pulses is too small,the DDT scheme might not properly work.The value of Δt is calculated by the difference between the lengths of two paths i.e |α-β|<δ.c/2 then only DDT is feasible as shown in figure 4.

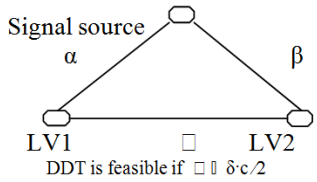

Fig 4. DDT

Figure 5 shows the flow chart of the Distance Difference Test.

The algorithm for DDT are as follows.

1. Whenever a transmitter sends a signal for spectrum access it is considered as the suspicious signal.
2. Whenever such signal is detected then it is checked whether the signal characteristics match with those of primary signal.If not then it is verified whether it matches with that of secondary user.
3. This is done by verifying whether the signal location match with that of the primary user transmitter or secondary user transmitter using DDT method. If yes then conclude that it is primary user or secondary user.
4. If not then then it is concluded that it is a illegitimate user(PUE attacker).

C. Security Issues in DRT and DDT: There are two security issues related to these methods.The first one is that if the attacker knows the position of the LV then it can purposefully send signal from such location which will give the same distance difference or same distance ratio present in database and thus attacker will pass the location verification test.To prevent this location of LV should be known to only to main authority controlling the location verification process.

Another security issue is the secure communication between all the LV's i.e specially between master LV and slave LV.The data should be encrypted and authenticated so that it should not get modified, interfered. Therefore publickey cryptography should be used for secure communication.

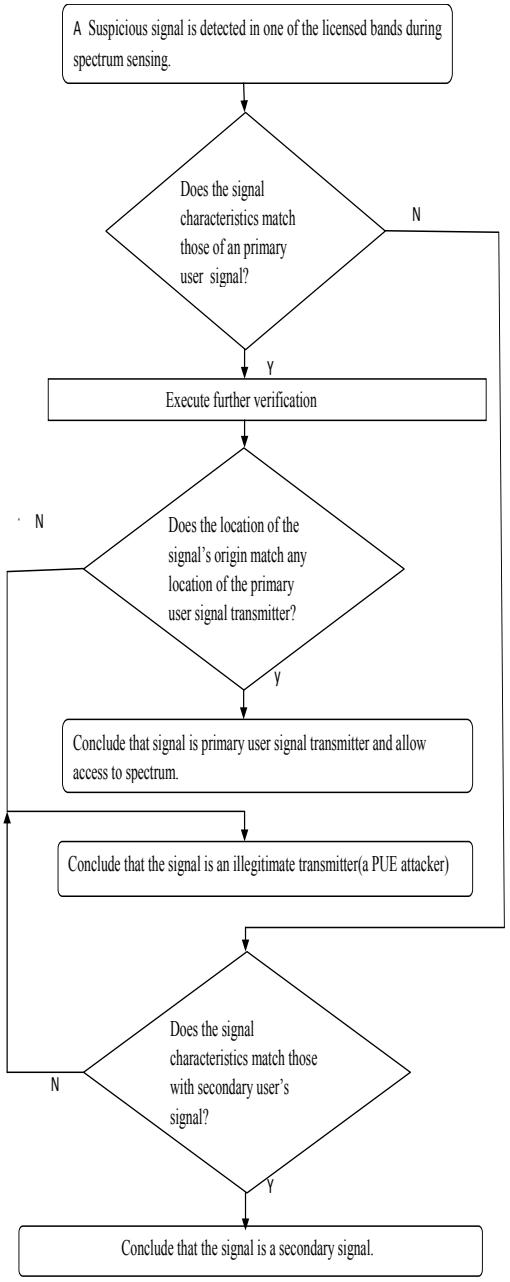

Fig 5.Flowchart for DDT Method

IV. Simulation Results

Matlab Result

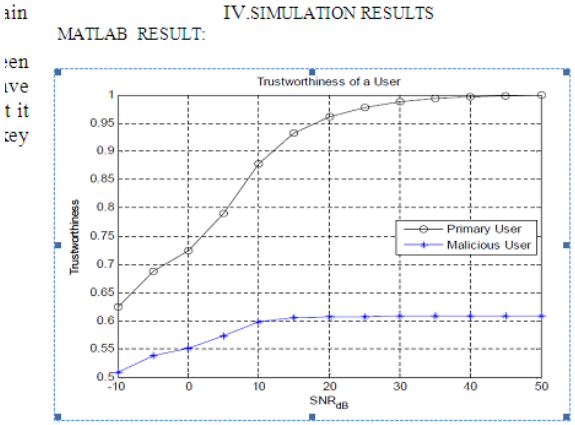

Fig. 6 Trustworthiness of a Primary and Malicious User for various SNR.

The Figure 6 shows the trustworthiness of a user. If the SNR value increases then correspondingly the trustworthiness increases. If the trustworthiness reaches to 1, then we can conclude that we are communicating with the primary user and not with the malicious user. Even if the trustworthiness is approximately equal to 1, we can trust the primary user, because there may be some interfering noise that will reduce the trustworthiness. As SNR value increases, the trustworthiness also increases and reaches to 1 when SNR=5. Whereas, malicious users trustworthiness remains constant at 0.6, even though the SNR value increases

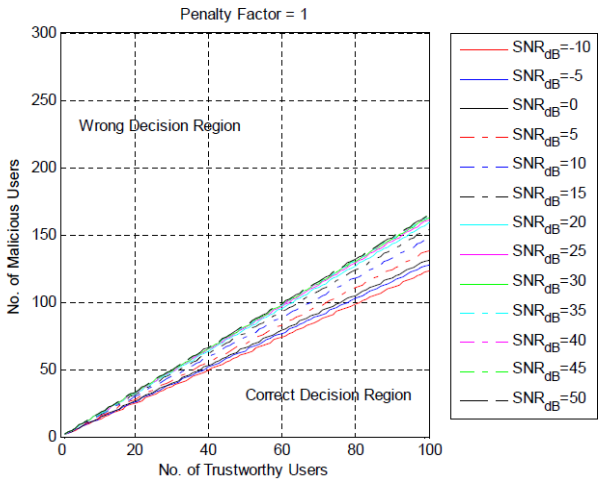

Fig 7.Trust metrics for penalty factor 1.

The above figure indicates the trust metrics for the number of malicious users and the number of trustworthy users. If the penalty factor is equal to 1, the number of trustworthy users is equal to 20 and if the number of malicious users is equal to 40, a correct decision can be made. As the value of

SNR increases, we may end up taking a wrong decision as the number of malicious users is more and the number of trustworthy users is less. Thus, we may end up listening to the malicious user.

As the penalty factor increases the number of malicious user for particular number of trustworthy users increases.

V. Conclusion

Cognitive radio is an efficient solution to the spectrum scarcity problem. It senses the unused spectrum of the licensed users and provides that unused spectrum to the secondary users without causing any interference between primary user and the secondary user. Cognitive radio increases the efficiency of the spectrum significantly.The DDT is an efficient technique to differenciate between primary or secondary user and malicious user as it gives results based on distance coordinates which cannot be changed malicious user. Thus we can conclude that our algorithm is an efficient technique to authenticate the legitimate primary user.

References

[1] S. Capkun, M. Cagalj, and M. Srivastava, "Secure localization with hidden and mobile base stations," *IEEE INJOCOMR,* 2006.

[2] S. Haykin, "Cognitive Radio: Brain-Empowered Wireless Communications", *IEEE Journal on Selected Areas in Communications,* Vol. 23, No.2, pp. 201-220, 2005.

[3] Wikipedia-The online encyclopedia. 2009. Retrieved from http://en.wikipedia.org/wiki/ROI.

[4] Federal Communication Commission, "Notice for Proposed Rulemaking (NPRM 03- 22): Facilitating Opportunities fbr Flexible,Efficient, and Reliable Spectrum Use Employing Cognitive Radio Technologies," *ETDocket,* No. 03-108, Dec. 2003.

[5] E. P. J. Tozer, *Broadcast Engineer Reference Book,* Elsevier,2004.

[6] Federal Communications Commission, "'Unlicensed operation in the TV broadcast bands and additional spectrum for unlicensed devices below 900 MHz in the 3GHz band," ETDocket No. 04-186,May 2004.

[7] M. G. Kuhn, An asymmetric security mechanism for navigation signals, Information Hiding Workshop, May 2004, pp.239-252.