

FINDING AN EMULATION ATTACK IN COGNITIVE RADIO

S. Umanayaki¹, M. Sabari Devi², S. Regina³

^{1,2} PG Scholar, ³Associate Professor, Raja College of Engineering and Technology,
Madurai, Tamilnadu,(India)

ABSTRACT

Cognitive radio, the recent emerging software enabled radio system, which is capable of self-tuning frequency band and setting suitable parameters for utilizing a channel freed or unused by licensed primary user . The cognitive radio which utilize unused channel, are called secondary user. The Secondary User detect whether a Primary User's channel is free or occupied at the time using spectrum sensing techniques. It is proved that single Secondary User free channel detection success ratio is comparatively low than cooperative sensing with other secondary user because of noisy wireless channel. The security concern arises when any of the cognitive radio selfish node is transmitting false detection report to fusion center which taken decision would be wrong and result of low free channel utilization. We propose model detect wrong information sent by cognitive radio and misbehaving cognitive radio in cognitive radio network. By using the advanced encryption standard find the authorized primary user.

Keywords: *Cognitive Radio Network, Primary User Emulation Attack, DTV, AES-Encrypted, DSA, CR Networks*

I.INTRODUCTION

Cognitive radio can be described as an intelligent and dynamically reconfigurable radio that can adaptively regulate its internal parameters as a response to the changes in the surrounding environment. Namely, its parameters can be reconfigured in order to accommodate the current needs of either the network operator, spectrum lessor, or the end-user. Although this doesn't necessarily need to be the case, Cognitive Radio (CR) is usually being defined as an upgraded and enhanced Software Defined Radio (SDR). Typically, full Cognitive Radios will have learning mechanisms based on some of the deployed machine learning techniques, and may potentially also be equipped with smart antennas, geolocation capabilities, biometrical identification, etc. However, the newly-introduced cognitive capabilities are exactly what make Cognitive Radios susceptible to a whole new set of possible security issues and breaches. Furthermore, the threats characteristic to Software Defined Radios, as well as those characteristic to "traditional" wireless networks also need to be taken into account. Cognitive Radio Network can be described as a network in which one or more users are Cognitive Radios. With the assumption of the potential attacker, as well as legitimate Secondary Users (SUs) always being CRs, the taxonomy of the threats within CRNs can be done with respect to the type of the Primary Users (PUs) considered.

II. RELATED WORK

It is desired to minimize spectrum sensing error that means sum of false alarm and miss detection probabilities since minimizing spectrum sensing error both reduces collision probability with primary user and enhances usage level of vacant spectrum. To provide reliable spectrum sensing performance (i.e., minimize spectrum sensing error), one of the great challenges is determining threshold levels since spectrum sensing performance depends on the threshold level. When determining threshold level, besides spectrum sensing error, spectrum sensing constraint which requires false alarm and miss detection probabilities to be below target level should also be considered since it guarantees minimum required protection level of primary user and usage level of vacant spectrum.

III. PROPOSED SYSTEM

In the proposed system an Advanced Encryption Standard for DTV is robust and reliable primary and secondary system operations. In the proposed system, At the Sending end primary user generates a pseudo-random number AES-encrypted reference signal that is used as the segment sync bits. The sync bits in the field sync segments remain unchanged for the channel estimation purposes at the receiving end, the reference signal is regenerated for the detection of the primary user and malicious user. It should be emphasized that synchronization is still guaranteed in the proposed scheme since the reference bits are also used for synchronization purposes. For each Slot period check the correlation and the threshold value it will detect the Primary user emulation attack.

IV. BLOCK DIAGRAM AND DESCRIPTION OF THE PROPOSED SYSTEM:

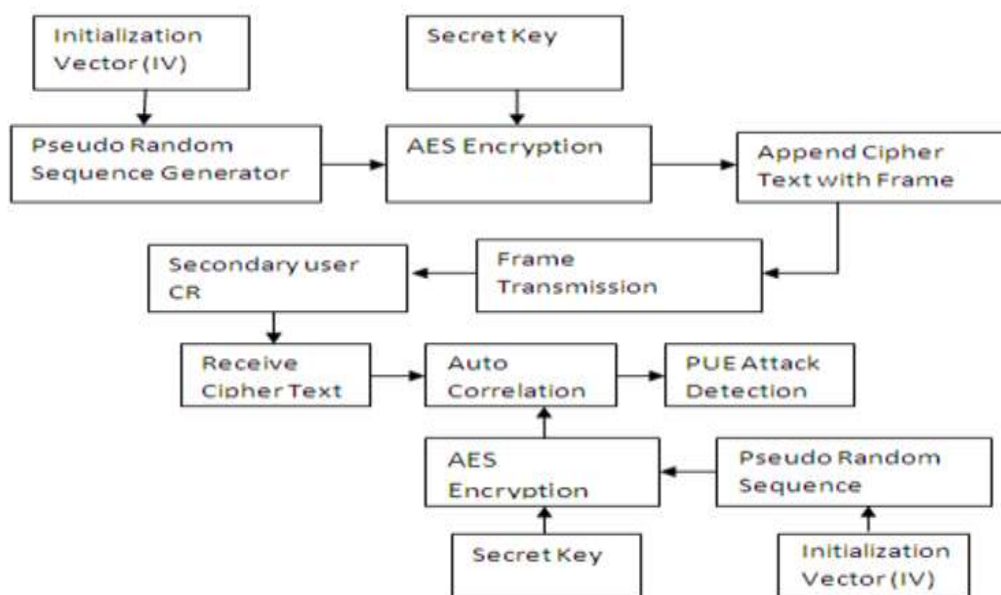
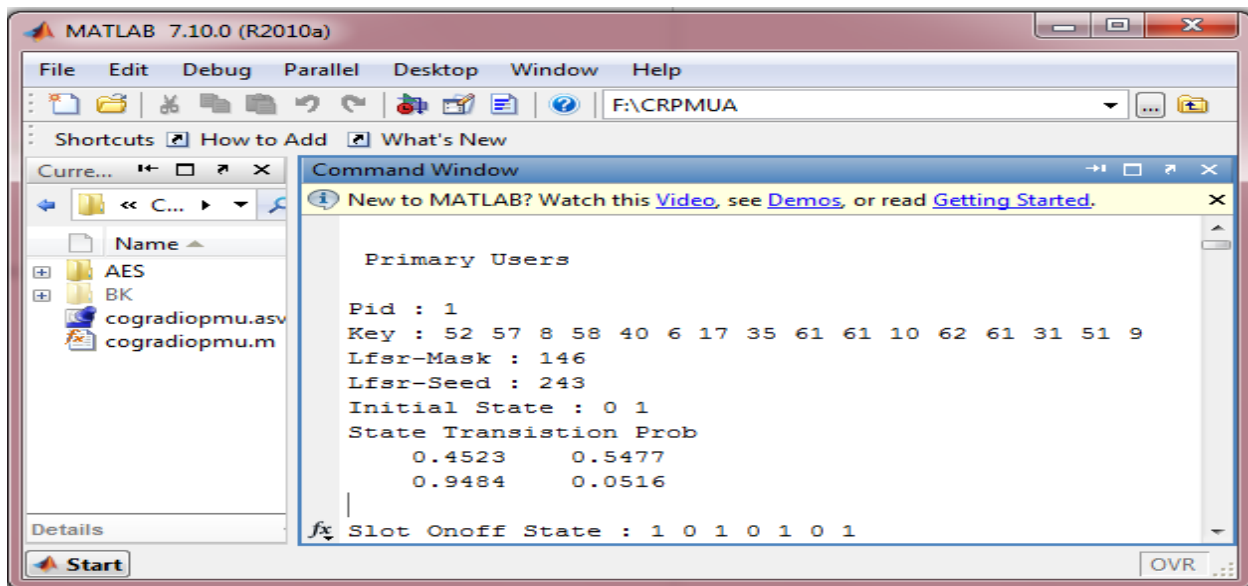


Fig 1 Block diagram cognitive radio using AES

Primary user is detected in its spectrum band immediately vacate that band and switch to a vacant one “vertical spectrum sharing” when another secondary user is detected in its spectrum band. When there are no better spectrum opportunities, it may choose to share the band with the detected secondary user “horizontal spectrum sharing”. CR MAC protocol guarantees fair resource allocation among secondary users. Primary signal transmitter localization is more challenging than the standard localization problem due to two reasons: no modification should be made to primary users to accommodate the DSA of licensed spectrum. This requirement excludes the possibility of using localization Protocol that involves the interaction between a primary user and the localization device. PST localization problem is a non-interactive localization problem when a receiver is localized, one does not need to consider the existence of other receivers. However, the existence of multiple transmitters may add difficulty to transmitter localization.

V RESULT AND DISCUSSION

In this section, we demonstrate the effectiveness of the AES-assisted DTV scheme through simulation. The impact of the noise level on the optimal thresholds we evaluate the false alarm rates and miss detection probabilities for both primary user and malicious user detection. In the simulations, by using the Matlab software we will find the miss detection probability. By using the Mask and Seed Value Primary User generates the Key. The number is generated by use AES Algorithm and the Key are encrypted as a reference Signal. Here consider the number of Primary user will be one. This simulation model is shown in the below fig.



```

MATLAB 7.10.0 (R2010a)
File Edit Debug Parallel Desktop Window Help
F:\CRPMUA
Current Folder: C:\...
Command Window
New to MATLAB? Watch this Video, see Demos, or read Getting Started.

Primary Users
Pid : 1
Key : 52 57 8 58 40 6 17 35 61 61 10 62 61 31 51 9
Lfsr-Mask : 146
Lfsr-Seed : 243
Initial State : 0 1
State Transition Prob
      0.4523      0.5477
      0.9484      0.0516

Slot Onoff State : 1 0 1 0 1 0 1
  
```

Fig 2: Generation of Slot by the Primary User

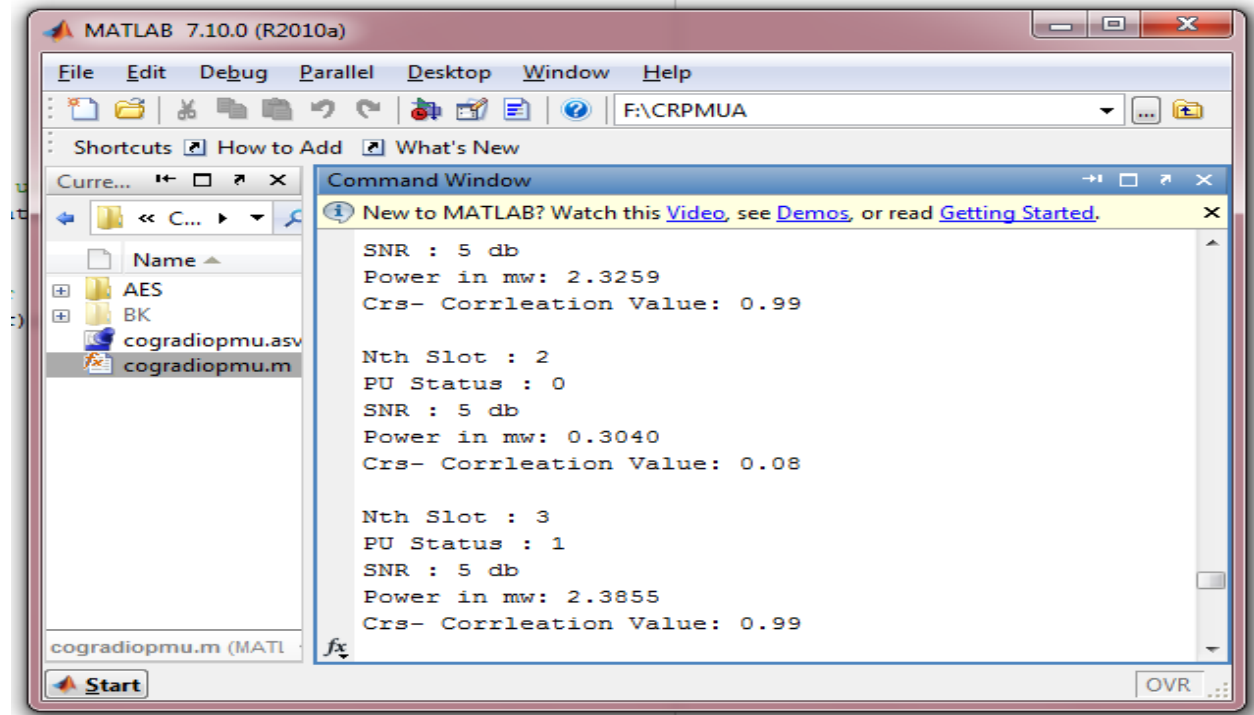


Fig:3 Checking of Correlation and Threshold by each slot

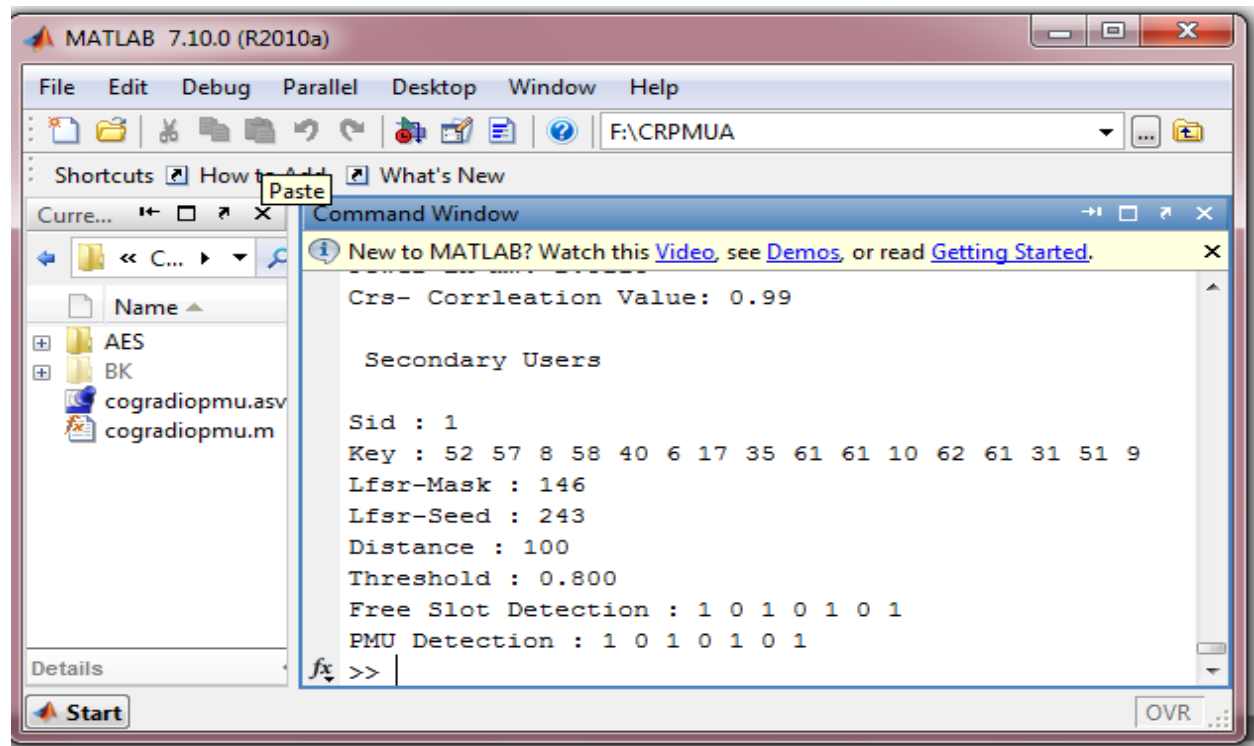


Fig4: Slot generate by the secondary User

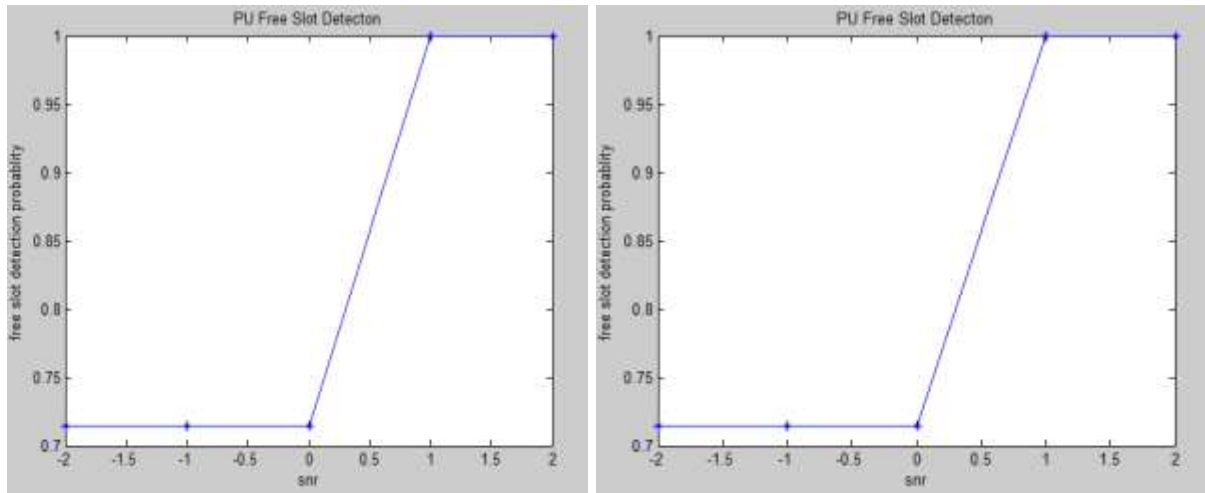


Fig5: Graphs for Different SNR Value

VI. ADVANTAGE AND APPLICATION

- Identification of Primary user and Malicious users are easy.
- If the Primary user and the second user are exchange the key means the data's are more secure
- This system is simple, convenient, time saving and high security..
- Because of the immediate decision making and interface provides an instant diagnosis based on limits.
- The focus of this project is to develop a system effective and robust, easy operation and mainly low cost which permits to manage the network security and improve quality.
- The protection and efficiency of the whole system is increased dramatically.
- These are mainly used where the security is most important.

VII. CONCLUSION AND FUTUREWORK

AES-assisted DTV scheme was proposed for robust primary and secondary system operations under primary user emulation attacks. An AES-encrypted reference signal is generated at the TV transmitter and used as the sync bits of the DTV data frames. By allowing a shared secret between the transmitter and the receiver, the reference signal can be regenerated at the receiver and be used to achieve accurate identification of authorized primary users. Moreover, when combined with the analysis on the auto-correlation of the received signal, the presence of the malicious user can be detected accurately no matter the primary user is present or not. This approach is practically feasible in the sense that it can effectively conflict PUEA with no change in hardware or system structure except of a plug-in AES

chip. Potentially, it can be applied directly to today's HDTV systems for more robust spectrum sharing. It would be interesting to explore Primary User Emulation Attack detection over each sub-band in multi-carrier DTV systems. In defense against primary user emulation attack in cognitive radio using advanced encryption standard technique the secret key is shared among Secondary users. No need of 3rd party reliable system. Because time consumption is high when the third party maintain the secret key. To avoid this future work secondary user maintains the secret key instead of third party.

REFERENCES

- [1].Chen and J.-M. Park, "Ensuring trustworthy spectrum sensing in cognitive radio networks," in *Proc. IEEE Workshop Netw. Technol. Softw. Defined Radio Netw.*, Sep. 2006
- [2]. Chen, J.-M. Park, and J. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 1, pp. 25–37, Jan. 2008
- [3].FCC, "Unlicensed operation in the TV broadcast bands and additional spectrum for unlicensed devices below 900 MHz and in the 3 GHz band," Federal Commun. Commission, Columbia, SC, USA, Tech. Rep. ET Docket No. 04-186 and 02-380, Sep. 2010
- [4].Z. Jin, S. Anand, and K. P. Subbalakshmi, "Mitigating primary user emulation attacks in dynamic spectrum access networks using hypothesis testing," *SIGMOBILE Mobile Comput. Commun. Rev.*, vol. 13, no. 2, pp. 74–85, 2009
- [5]. K. Borle, B. Chen, and W. Du, "A physical layer authentication scheme for countering primary user emulation attack," in *Proc. IEEE ICASSP*, May 2013
- [6]. L. Zhang, J. Ren, and T. Li, "Time-varying jamming modeling and classification," *IEEE Trans. Signal Process.*, vol. 60, no. 7, pp. 3902–3907, Jul. 2012
- [7]. N. Singhal and J. Raina, "Comparative analysis of AES and RC4 algorithms for better utilization," *Int. J. Comput. Trends Technol.*, pp. 177–181, Aug. 2011.
- [8].Mathur and K. P. Subbalakshmi, "Digital signatures for centralized DSA networks," in *Proc. 4th IEEE CCNC*, Jan. 2007.
- [9].L. Zhang, H. Wang, and T. Li, "Anti-jamming message-driven frequency hopping—Part I: System design," *IEEE Trans. Wireless Commun.*, vol. 12, no. 1, pp. 70–79, Jan. 2013
- [10]. L. Zhang, J. Ren, and T. Li, "Time-varying jamming modeling and classification," *IEEE Trans. Signal Process.*, vol. 60, no. 7, pp. 3902–3907, Jul. 2012.