Cognitive Radio Networks: Defense Against Primary User Emulation Attack (P.U.E.A.)

Naif Almalki

ABSTRACT — The paper discussed about PUEA (primary user emulation attacks) within a cognitive radio network functioning in the white spaces of DTV (digital TV) band. We recommend a consistent digital TV structure assisted by AES that involves an encrypted source signal by AES, produced at the transmitting end of TV and utilized as the sync bits of the data frames for digital TV. By permitting a shared hidden key between the transmitting and receiving end, the source signal could be reproduced at the receiving end and utilized to accomplish correct recognition of the licensed prime operators. Furthermore, while joint with the evaluation on the auto correspondence of the obtained signal, the existence of the harmful invader could be identified correctly with no obligation of presence or absence of the prime operator. We evaluate the efficiency of the recommended method via theoretical assessment as well as simulation illustrations. It is demonstrated that along with the digital TV structure assisted by AES, the prime operator along with the harmful invader could be identified with the extreme precision under PUEA (primary user emulation attacks). It must be highlighted that the recommended structure demands no alteration in equipment or system organization with an exception to a plug-in AES chip. Possibly, it could be implemented straight to modern digital TV system under PUEA (primary user emulation attacks) for further productive sharing of the spectrum.

Keywords / Index Terms— Digital TV, Receivers, Security Synchronization, Transmitters, Emulation, Random variables.

1. INTRODUCTION

Two types of users could utilize a cognitive radio network, the primary user that holds the license and the secondary user that does not holds the license [1]. The secondary user is capable to sense when primary user stops transmitting and therefore utilizes the free spectrum for transmission. On the other hand, when secondary user recognizes that prime operator is utilizing the spectrum, it usually withholds from transmitting [5]. This has been identified as cognitive radio network where the secondary user is allowed to utilize the valuable spectrum without causing any interference in the communication of primary user. The major reason behind the prevalence of the cognitive network is the fact that their assigned users are not utilizing many bands of the valuable spectrum to their maximum potential. This eventually leads towards granting a permission to secondary user to access the unutilized spectrum in order to provide an opportunity to

utilize these bandwidths to their full potential and offering more spectrum to the users [7]. A spectrum goes unutilized most of the time in a situation when a part of its bandwidth is dedicated for an application that has been under development. The duration required for these applications to emerge into the market could be long or in many cases might just not happen and in such circumstances, valuable spectrum might simply go unutilized for a significantly longer duration providing no benefit.

A cognitive network is such kind of a radio network in which each frequency bandwidth is utilized by two kinds of users:

- The Prime User
- The Non-Primary User

The prime operator creates main network and similarly the non-primary user creates the inferior network. The prime user enjoys holding the precedence over the secondary user, which means that the performance of the primary network would have the protection against the transmission of the secondary network. The term protection in this setting means

that any request from the secondary network must not cause any hindrance in the performance of the primary network [2]. Along with that, in case of increase in the load of traffic of the primary network, the possession and throughput of the secondary network must be revoked. Precisely, the secondary users are only permitted to utilize the bandwidth between the intervals when primary user left the space empty. The problem, which arises, is that the protocol utilized by the primary user, in other words also identified as the primary protocol usually emerges following a regulation procedure that overlooks the non-primary users. The implication is the nature of the non-primary protocol is often more tough and further expensive in comparison to the nature of the primary protocol due to the fact that the secondary protocol must have to be submerge with the properties of fundamental protocol to intelligently offer preference to the main operator [1]-[8].

The term spectrum sensing refers to the capability of the cognitive radio technology, which assists users to identify the part of the spectrum that is vacant and sense the existence of the primary user when it operates in a licensed bandwidth. Spectrum management denotes to the proficiency of the cognitive radio technology, which selects the best channel vacant. Spectrum sharing denotes to the competency of the cognitive radio technology, which manages the accessibility of the vacant channel with secondary users and spectrum mobility denotes to the competence of the cognitive radio technology, which evacuates the channel utilized by a secondary user as soon as the licensed user is identified within the range of the bandwidth [6].

The following four phases defines the functionality of the cognitive radio network:

- Spectrum Sensing:

Spectrum Sensing denotes to identify the unutilized bandwidth and share it with secondary user while assuring no damaging interference. Spectrum Sensing is a significant necessity for a cognitive radio network to detect idle frequency bands. Sensing primary user is the most proficient manner to sense the idle frequency bands [9]-[14].

Spectrum Management:

Spectrum management refers to the task of apprehending the best possible vacant bandwidth in the spectrum to address every need of the Quality of Service (QoS) throughout the entire spectrum frequency therefore the functions of spectrum management are needed for cognitive radios. There has been two spectrum management functions, which are classified as:

Bandwidth Decision

Bandwidth Analysis

Spectrum Mobility:

Spectrum mobility is termed as the procedure in which a cognitive radio user swaps the bandwidth of its operation. Utilizing the bandwidth in a profitable way by authorizing the broadcasting stations to function in the most suitable and vacant bandwidth of the spectrum along with sustaining hassle free transmission needs over the course of transition towards more appropriate bandwidth is the aim of a cognitive radio network [13]-[17].

Spectrum Sharing:

Spectrum sharing is one of the main challenges associated with the usage of an open spectrum. Spectrum sharing refers to administration of legitimate procedure of spectrum scheduling.

AES-ASSISTED DTV SYSTEM

In an "AES-assisted DTV structure", an AES-encrypted source signal (pseudo-random) is initiated by the primary user. It is utilized as the sync bits within the field and sync segments are kept the same because of the channel assessment. At the point of reception, the source signal is redeveloped for the recognition of the authorized operator and the unauthorized operator causing damage [16].

2.1. DTV transmitter

The "DTV transmitter" receives the source signal through the following process:

At first, it creates a "pseudo-random" (PN) sequence. Then it utilizes the "AES algorithm" to encrypt the PN sequence. It must be acknowledged here that a pseudo-random (PN) sequence is created with the use of a "Linear Feedback Shift Register (LSFR)" accompanied by a protected "initialization vector (IV)". After the PN sequence is created, it is utilized as an input to the AES encryption algorithm. Along with that, a 256-bit hidden key is utilized for AES encryption in order to achieve the best possible security [3]. The PN sequence is represented by "x", then the output of the AES algorithm is utilized as the source signal that could be demonstrated as:

$$"s = E(\mathrm{k}, \mathrm{x}) \ldots (1)"$$

In this equation, "k" stands for the key and "E(· , ·)" represents the AES encryption process. After that, the transmitter puts the source signal s in the sync bits of the DTV fragments of information.

Apart from the DTV and the CR operator, the hidden key could be developed and issued to the DTV receiver and transmitter through a reliable third party. The third party could manage the issuance of key as well as serving as the validation point for both CR user and the primary user. The key must have a time variance in order to block invasion through impersonation.

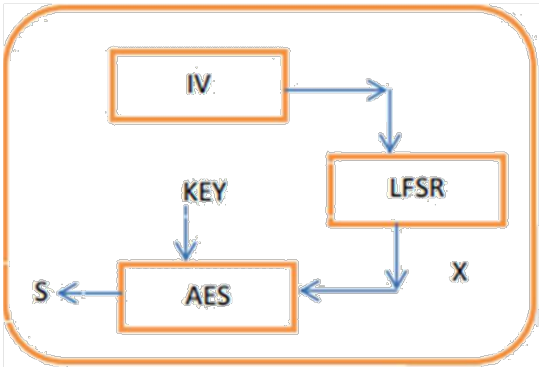

Figure 1: DTV Transmitter

2.2. DTV receiver

The receiver recreates the encrypted source signal with the assistance of the hidden key and initialization vector (IV), which are distributed among the receiver and the transmitter (3). A sensor is deployed to detect the correspondence, where the receiver calculates the cross relationship among the obtained signal "r" and the recreated source signal "s" for the primary operator. Additionally the receiver calculates the auto correspondence of the obtained signal "r" for the recognition of invading harmful user.

The cross relationship between the two random variables "x" and "y" is described as:

$$"Rxy =< x, y >= E\ xy\ *\ \ldots"$$

PUEA, the obtained signal could be demonstrated as:

$$"r = \alpha s\ + \beta m + n \ldots"$$

In the above equation, "s" is the source signal, "m" is the harmful signal, and "n is the noise, α" is the binary measure for the existence of the primary user and "β" for the harmful user. More precisely, α = 0 signifies the nonexistence of the main operator where as its equivalence to 1 signifies the existence of the prime operator. Similarly, value of β = 0 means absence of harmful user and its equivalence to 1 represents the presence of the invader.

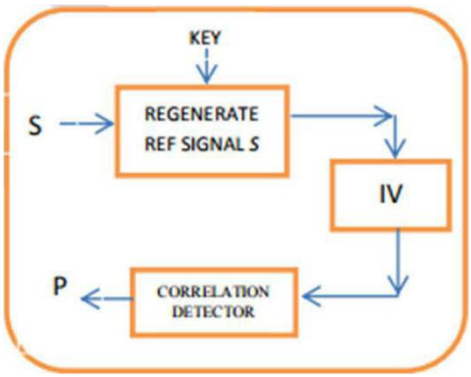

Figure 2: DTV Receiver

2.2.1. recognition of the prime operator:

To identify the existence of the main operator, the receiver calculates the cross relationship among the obtained signal "r" and the source signal "s"

$$"Rrs =< r,s >= \alpha < s,s > +\beta < m,s > +< n,s >= \alpha\sigma 2s \ldots"$$

In the above equation, "σ2s" represents the strength of signal of primary user and 'S", "m", and "n" are supposed to be autonomous towards each other and are of "0" mean. Based on the value of "α" in the receiver confirms the existence or absence of the main operator.

2.2.2. recognition of the malevolent invader:

To identify the existence of malevolent user, the receiver additionally calculates the auto correspondence of the obtained signal "r"

$$"Rrr =< r,r >= \alpha 2 < s,s > +\beta 2 < m,m > +< n,n > = \alpha 2\sigma 2s + \beta 2\sigma 2m + \sigma 2n \ldots"$$

In the above equation, "σ2m" and "σ2n" represent the strength of signal of invader and the strength of noise.

PRIMARY USER EMULATION ATTACK (PUEA):

Among the main technological concerns associated with the identification of bandwidth is the difficulty in appropriately identifying signals of main operator from the transmission of non-primary operator. Within a cognitive radio network, prime operator enjoys the preference of right to access the bandwidth. On the other hand non-primary operator should hand over the accessibility of the bandwidth to the primary operator every single time and guarantee that no intervention would be attempted [12]. As a result, when a main operator initiates to communicate over a bandwidth being consumed by the non-primary user, that secondary operator is obligatory to abandon that particular frequency in real time [18]. On the other hand, when there is no evidence of existence of the prime user in a range of a bandwidth, every non-primary operator hold as equal prospect to utilize the vacant bandwidth [4]. On the basis of this regulation, an opportunity prevails for the malevolent non-primary operator to imitate the basic features of the prime operator with an intention to avail the preferred accessibility to the spectrum being utilized by other non-primary operators. The situation is represented in the literature as the "PUE, Primary User Emulation" [10].

3.1. how DSA networks are affected by PUE:

There have been a number of consequences that could be induced due to PUE strike over a "DSA, Dynamic Spectrum Access" networks:

Unstable Networks

Spectrum Under-utilization

Denial of Service

Intervention with Primary Users

3.2. how PUE strikes affect CR networks:

The existence of PUE strikes sources several hurdles for CR networks. The list of prospective penalties of PUE strikes are:

Waste of Bandwidth

Deprivation of QoS

Connection unreliability

Denial of Service

Interference with the prime network

DEFENSE AGAINST PUE STRIKE:

In a trustworthy "AES-encrypted DTV" system, an "AES-encrypted" source signal is generated. It is utilized as the sync bytes of every statistical structure of DTV [11]. This provides assistance to share a hidden key among the receiver and the transmitter and the source signal could be recreated at the receiver's end. Further, it could be utilized to obtain detailed exposure of licensed prime users (PUs) [19]. This arrangement does not requires any alteration in the equipment or the structure of the systems with the exception of a plug-in "AES Chip". This could be implemented on the recent DTV structure in order to reduce "PUEA" and accomplish proficient sharing of the frequency channels [17]-[20].

Within the DTV structure, the developed AES encrypted source signal is further utilized for the accomplishment of synchronization at the authenticated receivers [15]. The projected demonstration reduces the possibility of "PUEA" along with empowering strong structure of action and assures profitable sharing of the bandwidth frequency. The effectiveness of the projected method is substantiated with the assistance of mathematical sources. The development of a pseudo-random source signal encrypted via AES by the prime user (PU) highlights that synchronization is certain in the projected model.

CONCLUSION

A valid DTV structure has been proposed through assistance of AES for strong primary and non-primary organization functions under "Primary User Emulation Attacks, (PUEA)". In the projected arrangement, a source signal is produced, which is encrypted via AES at the TV transmitter and utilized as the sync bits of the statistical structures of the DTV. By permitting a hidden shared key between the receiver and transmitter, the source signal could be reproduced at the receiver and utilized to accomplish correct recognition of licensed prime operators. Further, when

attached with the examination on the auto correspondence of the obtained signal, the existence of an invader could be identified perfectly without the condition of presence or absence of main operator. This arrangement is practically reasonable for the reason that it could proficiently oppose primary user emulation strikes while requiring no modification in the equipment or organization of the system apart from a plug-in AES chip. This could be possibly applicable to the modern day's HDTV structures for further productive sharing of the frequency bandwidth. It would be further exciting to further investigate "PUEA" occurrence into each sub-band in multicarrier DTV structures.

REFERENCES

A. Alahmadi, M. Abdelhakim, J. Ren, T. Li. Defense against primary user emulation attacks in cognitive radio networks using advanced encryption standard, IEEE transactions on information forensics and security, Vol. 9, No. 5, pp. 772-781, 2014.

D. Das, S. Das. Primary user emulation attack in cognitive radio networks: A survey, IRACST-International Journal of Computer Networks and Wireless Communications, Vol. 3, No. 3, pp. 312-318, 2013.

M. S. Jain, M. A. Dhawan, C. K. Jha. Emulation Attack in Cognitive Radio Networks: A Study, International Journal of Computer Networks and Wireless Communications (IJCNWC), Vol. 4, No. 2, pp. 169-172, 2014.

I. F. Akyildiz, W. Y. Lee, M. C. Vuran, S. Mohanty. NeXt generation/dynamic spectrum access/cognitive radio wireless networks: A survey, Computer networks, Vol. 50, No. 13, pp. 2127-2159, 2006.

S. Haykin. Cognitive radio: Brain empowered wireless communications, IEEE Jl. on Sel. Areas in Commun., Vol. 23, No. 2, pp. 201–220, 2005.

IEEE Standards for information technology-Telecommunications and information exchange between

systems- Wireless Regional Area Networks-Specific Requirements- Part 22-Cognitive wireless RAN medium access control (MAC) and physical layer (PHY) specifications: Policies and procedures for operation in the TV bands, 2006.

C. Cordeiro, K. Challapali, D. Birru, S. Shankar. IEEE 802.22: the first worldwide wireless standard based on cognitive radios. New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005. 2005 First IEEE International Symposium, pp. 328-337, 2005.

E. Visotsky, S. Kuffner, R. Peterson. On collaborative detection of TV transmissions in support of dynamic spectrum sharing. New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005. 2005 First IEEE International Symposium pp. 338-345, 2005.

A. Harrington, C. Hong, T. Piazza. Software defined radio: The revolution of wireless communication, White paper, Ball State University. [Online]. Available: http://www.bsu.edu/cics/alumni/whitepapers/

I. F. Akyildiz, W. Lee, M. C. Vuran, M. C., S. Mohanty. Next generation/dynamic spectrum access/cognitive radio: A survey, Elsevier Journal on Computer Networks, vol. 50, pp. 2127–2158, 2006.

X. Liu, Z. Ding. ESCAPE: a channel evacuation protocol for spectrum-agile networks, IEEE Symposium of New Frontiers in Dynamic Spectrum Access Networks (DySPAN) 2007, pp. 292–302, 2007.

R. Chen, J. M. Park. Ensuring trustworthy spectrum sensing in cognitive radio networks, IEEE Workshop on Networking Technol. for Software Defined Radio Networks (SDR) 2006, pp. 110– 119, 2006.

R. Chen, J. M. Park, J. H. Reed. Defense against primary user emulation attacks in cognitive radio networks," IEEE Jl. on Sel. Areas in Commun.: Spl. Issue on Cognitive Radio Theory and Applications, Vol. 26, No. 1, pp. 25–37, 2008.

R. Chen, J., M. Park, K. Bian. Robust distributed spectrum sensing in cognitive radio networks, IEEE Conference on Computer Communications (INFOCOM) 2008 mini-conference, 2008.

L. F. Fenton. The sum of log-normal probability distributions in scatter transmission systems, IRE Trans. on Commun. Systems, No. CS-8, pp. 57–67, 1960.

S. Ross. Probability Models. Academic Press, 2003.

M. Vu, N. Devroye, V. Tarokh. Primary exclusive region in cognitive networks, IEEE Consumer Communcations and Networking Conference (CCNC'2008), 2008.

M. Vu, N. Devroye, M. Sharif, V. Tarokh, Scaling laws of cognitive networks, IEEE Journal on Selected Topics in Signal Processing.

S. Anand, R. Chandramouli. On the secrecy capacity of fading cognitive wireless networks, IEEE Cognitive Radio Oriented Wireless Networks and Communications (CROWNCOM'2008), 2008.

T. S. Rappaport, Wireless Communications: Principles and Practice. Prentice Hall Inc., New Jersey, 1996.