Middle-East Journal of Scientific Research 24 (4): 1335-1340, 2016
ISSN 1990-9233
© IDOSI Publications, 2016
DOI: 10.5829/idosi.mejsr.2016.24.04.23304

Defense Against Primary User Emulation Attack in Cognitive Radio Networks Using Cryptosystem

C. Sahaya Kingsly and J. George Chellin Chandran

Department of Computer Engineering,
Manonmanium Sundaranar University, Tirunelveli, India

Abstract: This paper considers Primary User Emulation Attack in Cognitive Radio (CR) networks. Some unwanted user can use empty channel through attacks and threats. We present a Diffie Hellman (DH) assisted scheme for security. Using this scheme encrypted reference signal is generated and used as synchronization bits of data frames. Shared key is allowed between transmitter and receiver. The reference signal can be regenerated at the receiver to identify the primary user. This paper analyses the performance of primary user and identifies the malicious users. This scheme is useful to identify the authorized user. The Primary User Emulation Attacks are identified and prevented with efficient spectrum sharing.

Key words: Spectrum sharing · PUEA · Dynamic spectrum · Sensing · DH · LC method

INTRODUCTION

The wireless communication has been increased and requirement of high data rate has also been increased. The licensed spectrum space remains idle at most of the times [1] due to inefficient allocation of frequencies and the cellular bands are overloaded. The secondary users can sense the spectrum users and utilize the bands when the spectrum is not undecided the primary user. The most dominant attack in CR network is primary.

Malicious users can try and mimic a primary user's air space, thus leading to a false spectrum sensing. Such an attack is termed as a Primary User Emulation Attack (PUEA). Generally, licensed users are known as primary users (PU) and un-licensed users are secondary users (SU). When information is send through a licensed spectrum band is a PU, only some channel of band is used, others are empty. These empty channels are used by un-licensed user called SU. SUs always watch the activities of PU and detect the empty channel and occupy the channel without disturbing the PU and effects have been investigated [2]. A more challenging problem is to develop effective countermeasures after the attack is identified. Though Public key encryption based PU identification has been proposed, [3] for preventing SUs masquerading as PUs. In [4], public key cryptography mechanism is used between PUs and SUs, such that the SUs can identify the PUs accurately based on their public keys. A possible concern with this scheme is that the public key based approaches generally have high computational complexity. In [5], a two-stage PU authentication method was proposed: (i) first, generate the authentication tag for the PU using a one-way hash chain; (ii) secondly embed the tag in the PU's signal through constellation shift. This tag embedding scheme resembles the digital watermarking. Existing methods for PU detection can be categorized as energy detection and feature detection [6]. In energy detection method, any captured signal whose energy exceeds a threshold is identified as a PU signal. In feature detection methods, SUs attempt to find a specific feature of a captured signal, such as a pilot, a synchronization word and cyclostationarity. If a feature is detected, then the captured signal is identified as a PU signal.

Related Studies: Various Attacks in the protocol stack are studied and listed.

PU Emulation Attack: When the spectrum band is free from use by the PU, a malicious attacker emulates the signal characteristics of the PU and sends a jamming signal.

Corresponding Author: C. Sahaya Kingsly, Department of Computer Engineering,
Manonmanium Sundaranar University, Tirunelveli, India.

Table I: Various Attacks on the Protocol Stack

Protocol Stack	Attacks
Physical Layer	PUEA; OFA; CCDA
Link Layer	SSDF;SCN; Control channel saturation Dos
Network layer	Sink Hole attack; Hello Flood attack
Transport Layer	Lion attack; jellyfish attack
Application Layer	All the above attacks have various harmful effects on this layer

Table II: Comparison of Different Defense Techniques

Defense Technique	Contributions	Tests/ Models used	Key Features/ Advantages/ Disadvantage
Fenton's Approximation	S.Anand, Z.Jin and K. P. Subbalakshmi (2008), [7]	Markov's Inequality, WSPRT	Fading wireless networks, rarely violates spectrum evacuation technique
Location Based	(R.Chen and J.M.Park, 2006) [13]	TDoA, RSS	TDoA-high accuracy, sensitive to multipath propagation, RSS-inexpensive, hardware implementation simple, high errors, not suitable for long range
Sybil Attack	(S.Bhattacharjee *et al*, 2013;) [9]	Spider ratio test	Attacker mask multiple identity
PU Authentication	(Meena Thanu, 2012) [10]	Channel Impulse response	Best method to identify PU, Location estimation technique used
Encryption and Displacement method	(X.Zhou *et al*, 2011) [11]	NS-2 Simulation	Solves air interception problem
Cooperative Spectrum Sensing	(C.Chen *et al*, 2011) [2]	Optimal Combining Scheme	Optimize detection probability of PU, set of cooperative sensors used
Variance Detection	(Z.Chen *et al*, 2009)[8]	Naïve Detection	Better performance than mean field approach and max likelihood estimation, different channel parameters used
Hybrid PUEA Defense	(F.Bao *et al*, 2012)[14]	Energy Detection,	Better performance, high probability, low resource consumption
IRIS	(A.W.Min *et al*, 2011) NA Checks [12]	Variance Detection	consistency, high attack tolerance, small communication and computation overheads

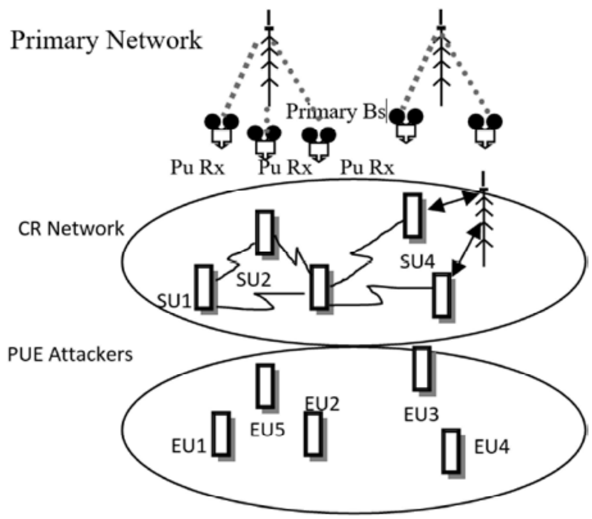


Fig. 1: CR Scenario

We develop a new PU detection method using DH algorithm to distinguish PU signal from attacker signal. Section II gives Random Number Generation. Section III explains security method. Section IV overview of our proposed method. Section V Experimental Evaluation Section VI concludes this paper.

Primary User Emulation Attack (PUEA) and Its Impact on CR: A PUE attack is a new type of attack unique to CR networks, in which the attackers may modify their radio transmission frequency to mimic a primary signal, thereby misguiding the legitimate SUs to erroneously identify the attackers as a PU. Fig. 1 shows a typical scenario of a PUE attack. There are two spectrum bands, licensed band I and band II. Both of the spectrum bands have six channels, indexed by frequencies f1, f2, • • •, f6 and f7, f8, • • •, f12, respectively. In band I, where the primary base station (BS) is transmitting in channels f1, f3 and f4 to the PU receivers. Channels f2, f5 and f6 are idle. By observing this, SU1, SU2 and SU3 are allowed to use these three idle channels for transmissions. However, the appearance of a PUE attacker, say, EU2, may block the SUs from using an idle channel. EU2, for example, mimic the primary signal in channel f2. Once the attack succeeds, SU1 and SU3 are misled to evacuate channel f2 and the link between them is interrupted.

In band II. The primary network is occupying channels f11 and f12, while SU4 and SU5 are using channels f9 and f10, respectively. PUE attackers EU3and EU4 are emulating the primary signals in channels f7 and f8, respectively. In this situation, SU4 and SU5 need to find channels to connect with the cognitive BS. If attackers EU3 and EU4 cannot be correctly identified, SU4 and SU5 will find no vacant channels and hence may not be able to communicate with the cognitive BS. The above two examples describe two different attacking cases. The first example illustrates the case that the PUE attacker attacks the in-service SUs and seizes one of their channels, causing interruption of some of the SU services. The second example illustrates the case that the PUE attack occupy the idle channels and waste the spectrum opportunities of the Sus.

Classification of Attackers

Selfish and Malicious Attackers: A selfish attacker aims at stealing bandwidth from legitimate SUs for its own transmissions. The attacker will monitor the spectrum. Once an unoccupied spectrum band is discovered, it will compete with the legitimate SUs by emulating the primary signal, e.g., SU3 and SU4 in Fig. 1. A selfish attacker is a rational attacker in the sense that, if it is detected by the legitimate SUs and the SUs reclaim the spectrum opportunity by switching back to the band, it has to leave the band. The purpose of a malicious attacker, is to disturb the dynamic spectrum access of legitimate SUs but not to exploit the spectrum for its own transmissions. Malicious attacker may emulate a primary signal in both an unoccupied spectrum band and a band currently used by legitimate SUs, e.g., SU2 in Fig. 1. When an attacker attacks a band being used by a legitimate SU, there exists the possibility that the SU fails to discover the signal and hence, an interference occurs between the attacker and the legitimate SU.

Power-Fixed and Power-Adaptive Attackers: The ability to emulate the power levels of a primary signal is crucial for PUE attackers, because most of the SUs employ an energy detection technique in spectrum sensing. A power fixed attacker uses an invariable predefined power level regardless of the actual transmitting power of the PUs and the surrounding radio environment. Compared to the power fixed attacker, the power-adaptive attacker is smarter in the sense that, it could adjust its transmitting power according to the estimated transmitting power of the primary signal and the channel parameters [3]. Specifically, the attacker employs an estimation technique and a learning method against the detection by the legitimate SUs. It is demonstrated that such an advanced attack can defeat a naive defense approach that focuses only on the received signal power. The location of a signal source is also a key characteristic to verify the identity of an attacker. A static attacker has a fixed location that would not change in all round of attacks. By using positioning techniques such as Time of Arrival (ToA) or dedicated positioning sensors [8], the location of a static attacker could be revealed. A static attacker will be easily recognized due to the difference between its location and that of the PUs. A mobile attacker will constantly change its location so that it is difficult to trace and discover. A viable detection approach that exploits the correlations between RF signals and acoustic information is proposed in [4] to verify the existence of a mobile PUE attacker.

Essential Conditions for Successful PUE Attacks: In a CR network, the successful realization of a PUE attack relies on several essential conditions. To better understand PUE attacks and facilitate the design of the countermeasures. There is no interaction between the primary and the secondary networks. This is a necessary condition for a successful PUE attack. Otherwise, if the legitimate SUs are allowed to exchange information with the PUs, a PU verification procedure could be designed to easily detect a PUE attack. In most cases, this condition holds. It is regulated in the IEEE 802.22 standard and also a general assumption in most existing research work of CR networks.

PU and SU Signals Have Different Characteristics: The primary and secondary networks use wireless signals with different characteristics, i.e., using different modulation modes and different signal statistical features. An SU receiver is inherently designed only for the secondary signal but unable to demodulate and decode the primary signal. The PUE attackers take advantage of this fundamental condition to emulate the primary signal that is unrecognizable for the legitimate Sus.

Primary Signal Learning and Channel Measurement: To emulate the primary signal, the attacker has to track and learn the characteristics of the primary signal. For an advanced attack, the attacker may also estimate the power level as well as the channel conditions to generate more tricky transmitting signals.

Avoiding Interference with the Primary Network: Although this is usually a primary concern for the SUs, it is also an important condition that the PUE attackers have to comply with. The attackers, especially the selfish ones, should carefully monitor the behaviors of PUs and not to cause extra interference with the primary network.

Impact of PUE Attacks on CR Networks

Bandwidth Waste: The ultimate objective of deploying CR networks is to address the spectrum under-utilization that is caused by the current fixed spectrum usage policy. By dynamically accessing the spectrum “holes”, the SUs are able to retrieve these otherwise wasted spectrum resources. However, PUE attackers may steal the spectrum “holes” from the SUs, leading to spectrum bandwidth waste again.

QoS Degradation: The appearance of a PUE attack may severely degrade the Quality-of-Service (QoS) of the CR network by destroying the continuity of secondary services. For instance, a malicious attacker could disturb the ongoing services and force the SUs to constantly change their operating spectrum bands. Frequent spectrum handoff will induce unsatisfying delay [7] and jitter for the secondary services.

Connection unreliability: If a real time secondary service is attacked by a PUE attacker and finds no available channel when performing spectrum handoff, the service has to be dropped. This real time service is then terminated due to the PUE attack. In principle, the secondary services in CR networks the inherently have no guarantee that they will have stable radio resource because of the nature of dynamic spectrum access. The existence of PUE attacks significantly increases the connection unreliability of CR networks.

Denial of Service: Consider PUE attacks with high attacking frequency; then the attackers may occupy many of the spectrum opportunities. The SUs will have insufficient bandwidth for their transmissions and hence, some of the SU services will be interrupted.

In the worst case, the CR network may even find no channels to set up a common control channel for delivering the control messages. As a consequence, the CR network will be suspended and unable to serve any SU. This is called Denial of Service (DoS) in CR networks.

Interference with the primary network: Although a PUE attacker is motivated to steal the bandwidth from the SUs, there exists the chance that the attacker generates additional interference with the primary network. This happens when the attacker fails to detect the occurrence of a PU. On the other hand, when the SUs are tackling a PUE attack, it is also possible to incorrectly identify the true PU as the attacker and interfere with the primary network. In any case, causing interference with the primary network is strictly forbidden in CR networks.

Random Number Generation

Finding Primitive Roots: If the multiplicative order of a number m modulo n is equal to φ (n) (the order of Zn) then it is a primitive root. In fact the converse is true. If m is a primitive root modulo n, then the multiplicative order of m is φ (n) we can use this to test for primitive roots

First, compute φ(n).Then determine the different prime factors of φ (n), say p_1, ……,$p_{k.}$ now for every element m of Z_n compute

$m^{\varphi(n)/pi}$ mod n for i = 1, ….., k

where number m for which these k results are all different form 1 is a primitive root.

The number of primitive roots modulo n, if there is any, is equal to $\varphi(\varphi(n))$.

Since, in general, a cyclic group with r elements has φ® generators.

If g is a primitive root modulo p, then g is a primitive root modulo all powers pk unless;

$g^{p-1} = 1 \pmod{p^2}$

If g is primitive root modulo p^k the g or g+ p^k (whichever one is odd) is a primitive root modulo $2p^k$

The sequence of random numbers is obtained using the equation:

$R_{n+1} = (a\ R_n + C) \bmod m$

where; m, a, c and Ro are integers, each integer in the range $O \leq R_n < m$, the multiplier and modulus are chosen by transmitter side and for 32 bit arithmetic.

$R_{n+1} = (a\ R_n) \bmod (2^{31} - 1)$

Then the sequence Number is generated. For example:

A = 7, c = 0 , m =32

Sequence is {7, 17, 23, 1 ,7 …...}

Security Method I: The proposed security model is to enable exchange of keys between Distribution center and PU. PU and Distribution center select secret key and generate public keys. Exchange of public keys then authorized PU access the band.

Proposed Method 1:

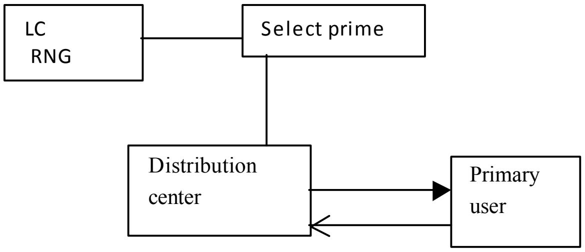


Fig. 2: Security Method 1

Key Exchange Protocols:

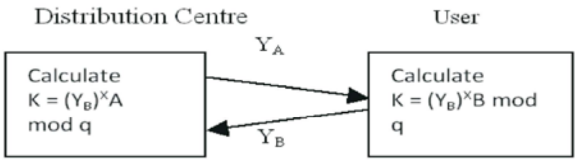

Distribution Centre
User
Y_A
Y_B
Calculate K = $(Y_B)^X$A mod q
Calculate K = $(Y_B)^X$B mod q

Fig. 3: Key Exchange

Proposed Method 2:

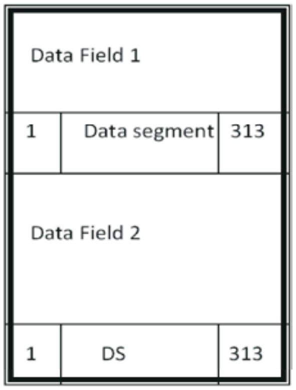
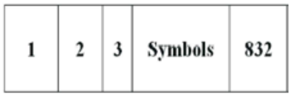


Fig. 4: VSB Signal Frame Structure



1	2	3	Symbols	832

Fig. 5: Segment of Data field

Here we consider eight – level vestigial sideband. (8VSB) modulation in the DTV System Each Frame has two data fields. each data field has 313 segments. Data segments contains 832 symbols. In 832 symbols 4 symbols used for segment synchronization. Each data segment has synchronization symbols. In the proposed system, the PU generates reference signal that can be used in sync. bits. At the receiving end, the reference signal is remunerated for detection of PU and malicious user. Generating Pseudo – random sequence. The pseudo random sequence is generated using linear congruential (LC) method. By selecting primitive roots from the list of primes then secret key is generated and exchanged between PU and distribution center.

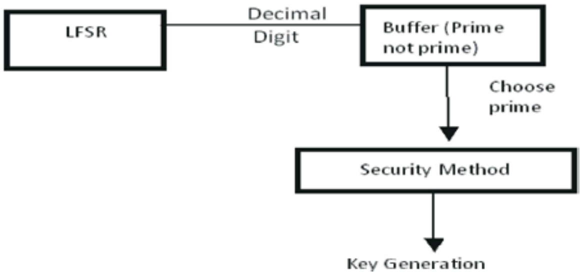


Fig. 6: Security Method 2

Using initialization vector values the Linear Feedback Shift register (LFSR) generates values, equivalent decimal value can be stored in registers. By selecting any prime number and given to the security method and key is generated the exchanged.

Experimental Evaluation: Random numbers are generated using linear congruential method. Select prime for the Random numbers series. Public key is generated by Distribution center and PU.

Consider a = 7 , c = 0, m = 32

$X_{n+1} = (aR_{xn} + C) \bmod m$
$X_{n=1} = x_2 = (7 \text{ x } 1+0) \bmod m$
$= 7 \bmod 32 = 7$
$X_{n=2} = 14 \bmod 32$
$X_{n=3} = 21 \bmod 32$
$X_{n=4} = 28 \bmod 32$

Sequence is {7,14,21,28,3,10}
We take 7 and 3 as a prime
Choose q = 7
$\alpha = \alpha < 9$ and a is α primitive root of q
Take prime Number up to 7
Here ‘3’ is a primitive root of 7
Consider ‘3’ is a primitive root
q is 7, α is 3

Distribution center key generation
$XA < q$
$Y_A = \alpha^{XA} \bmod q$
$Y_A = 2$

PU key generation
$X_B < q$
$Y_B = \alpha^{XB} \bmod q$
$Y_B = 27 \bmod 7$
$Y_B = 6$

The Distribution center and PU generate secret key
$K = (Y_B)^{XA} \bmod q$
$K = (Y_A)^{XB} \bmod q$
$K = 1$

Key are validated then PU can access the band

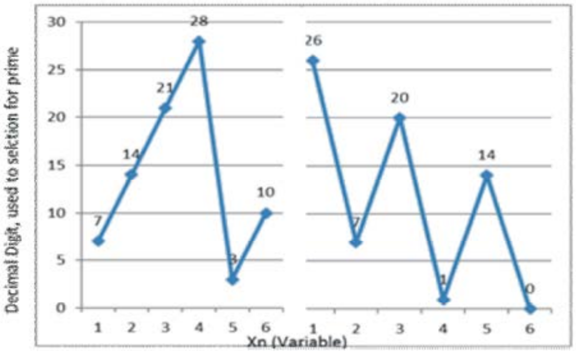


Fig. 7: Selection of Prime Numbers for Finding Primitive Roots

CONCLUSION

In this paper, DH based security model was proposed to prevent PUEA. In the proposed scheme, Signal is generated in the transmitter side using linear congruential method and DH assisted crypto method. Secret key is exchanged between PU and distribution center. The analysis shows the sequence of decimal digit can be generated by variable Xn, by selecting the prime number and finding the primitive roots. In addition DTV scheme was studied and the reference signal can be modified with this security model. These approaches are effective in discovery and defending PUEA attacks in the CR Networks.

REFERENCES

1. Deepa Das and Susmita Das, 2013. Primary User Emulation Attack in Cognitive Radio Networks: A Survey, IRACST, 3(3).
2. Chen, C., H. Cheng and Y.D. Yao, 2011. Cooperative Spectrum Sensing in Cognitive Radio Networks in the presence of Primary User Emulation Attack, IEEE Transactions on Wireless Communications, 10(7): 2135-2141.
3. Mathur, C.N. and K.P. Subbalakshmi, 2007. Digital signatures for centralized DSA networks, in First IEEE Workshop on Cognitive Radio Networks, Las Vegas, Nevada, USA, pp: 1037-1041.
4. Mathur, C. and K.P. Subbalakshmi, 2007. Digital signatures for centralized DSA networks, in Proc. 4th IEEE CCNC, pp: 1037-1041.
5. Borle, K., B. Chen and W. Du, 2013. A physical layer authentication scheme for countering primary user emulation attack, in Proc. IEEE ICASSP, May 2013, pp: 2935-2939.
6. Kim, H. and K.G. Shin, 2008. In-band spectrum sensing in cognitive radio networks: energy detection or feature detection? In MobiCom '08: Proceedings of the 14th ACM international conference on Mobile computing and networking, pp: 14-25, New York, NY, USA, 2008. ACM.
7. Anand, S., Z. Jin and K.P. Subbalakshmi, 2008. An analytical model for primary user emulation attacks in cognitive radio networks, New Frontiers in Dynamic Spectrum Access Networks, 3rd IEEE Symposium, pp: 01-06.
8. Chen, Z., T. Cooklev, C. Chen and C.P. Raez, 2009. Modelling Primary User Emulation Attacks and Defenses in Cognitive Radio Networks, Proc. Performance Computing and Communications Conference, IEEE 28th International, pp: 208-2015.
9. Shameek Bhattacharjee, Shamik Sengupta and Mainak Chatterjee, 2013. Vulnerabilities in cognitive radio networks: A survey, Computer Communications, 36: 1387-1398.
10. Sachin Shetty, Meena Thanu and Ravi Ramachandran, 2012. Cognitive Radio: Primary User Emulation Attacks and Remedies, Recent Patents on Computer Science, 5: 103-108.
11. Wang, Z., D. Liu, X. Zhou, X. Tan, J. Wang and H. Min, 2007. AntiCollision Scheme Analysis of RFID System, Auto-ID Labs White Paper.
12. Min, A.W., K.G. Shin and X. Hu, 2009. Attack-Tolerant Distributed Sensing for Dynamic Spectrum Access Networks, Proc. IEEE 17th Int'l Conf. Network Protocols (ICNP '09), Oct. 2009.R.
13. Chen, R. and J.M. Park, 2006. Ensuring trustworthy spectrum sensing in cognitive radio networks, Proc., IEEE Workshop on Networking Technol. for Software Defined Radio Networks (SDR), pp: 110-119.
14. Bao, F., H. Chen and L. Xie, 2012. Analysis of primary user emulation attack with motional secondary users in cognitive radio networks, Personal Indoor and Mobile Communications, 23rd IEEE International Symposium, pp: 956-961.