Iran J Sci Technol Trans Electr Eng (2018) 42:291–297
https://doi.org/10.1007/s40998-018-0073-5

RESEARCH PAPER

Trust Establishment in Chaotic Cognitive Environment to Improve Attack Detection Accuracy Under Primary User Emulation

Shriraghavan Madbushi[1] · Rajeshree Raut[2] · M. S. S. Rukmini[1]

Received: 28 August 2017 / Accepted: 12 June 2018 / Published online: 27 June 2018

Abstract
In this paper, we propose a novel algorithm for primary user emulation attack detection and removal in cognitive radio networks, which are driven by chaotic tag-based sequencing for communication. Our proposed approach demonstrates the use of the look-up table-based challenge sequences which are monitored by the cognitive base station and act as the first line of defense against any primary user emulation attacker. This ensures that almost all of the attackers are suppressed, and for the remaining attackers if any, we use a tag-based chaotic communication system, wherein each of the requests from secondary users is sent like a chaotic noise sequence on the channel, and the receiving entity decodes this sequence in order to get the signal communicated by an authorized transmitter. If there is any communication by an attacker, then it is detected immediately, as none of the receiving entities can decode the signals sent by these unwanted attacker nodes. This ensures that our system guarantees greater than 99% detection and identification of attackers in primary user emulation attacks.

Keywords Primary user emulation · Challenge system · Chaotic communication · Tag identification · Primary user · Secondary user

1 Introduction

Cognitive radios are prone to many types of attacks; these can be primary user emulation, selfish channel negotiation, control channel negotiation and many more. These networks are prone to such kind of attacks because they have the inherent entities of primary users, secondary users and channel sensing. Once the network is under attack, the basic properties of cognitive radio network are deteriorated, and the network behaves erratically.

In primary user emulation attack, the attacker emulates the functionality of a primary user and blocks the spectrum so that all the genuine secondary users are denied service (Haghighat and Sadough 2012), because the primary property of a cognitive radio is that it assigns a channel to one secondary user and keeps it assigned until the communication of the secondary user is completed or until the primary user returns back. This ensures high quality of service to the primary users, and the channel bandwidth is assigned to other secondary users once the current primary communication is completed. Owing to this property, the network communication is optimized, and the channel utilization is evenly managed.

Primary user emulation attackers tend to be present in all cognitive radio environments. These can be present in the form of software-defined radios or virtual trans-receivers in cognitively capable devices. These attackers monitor the network traffic and perform primary user emulation attack when the network usage is maximum. The impact of this is huge, and communications, mainly high priority communications, get disrupted due to it.

In our proposed approach, we introduce a trust-based mechanism for detecting and locating the source of primary user emulation attacks. Once the attacker nodes are identified, they are blocked and removed from the network

✉ Shriraghavan Madbushi
m.shriraghavan@gmail.com

[1] Department of ECE, Vignan's Foundation for Science, Technology and Research, Guntur, India

[2] Department of EDT, Shri Ramdeobaba College of Engineering and Management, Nagpur, India

communication process. Genuine secondary nodes have an individual and unique trusted look-up table-based request-challenge mechanism. The main strength of the algorithm is in the fact that each genuine secondary node is pre-configured and has some unique parts when compared with other genuine secondary nodes.

Primary user emulation attackers have a less to no chance of getting through this trust-based system, but in case they do, then we have applied a second layer of attack detection, in which a chaotic communication system is implemented. This chaotic communication system encodes a test sequence from the genuine transmitters; this test sequence appears as noise on the channel; thus, it cannot be detected by any primary emulation attacker node. The testing receivers detect this signal, and if it is received within a proper BER range, then the node is marked to be safe. Otherwise, the node is marked to be unsafe or attacker node and is removed from the network.

This two-layered approach helps us to detect and remove primary user emulation attackers from the network in a very effective and optimized way. Our results demonstrate that the primary user emulation attackers are detected and removed at a rate of 99%, and the network communication is restored with minimum delay. This property allows us to use the two-layered approach in practical real-time scenarios, without compromising the quality of service (QoS) of the network for primary and secondary nodes. Most of the work on mitigating primary user emulation attack has been done over past few years by the research community. We summarize a few selected contributions referred by us in Table 1.

2 System Model: Two-Layered Approach for Attack Detection and Removal

Our research is to detect and locate the nodes which take part in primary user emulation attack. The proposed two-layered approach can be depicted using Fig. 1. In the figure, we can observe that the genuine nodes have two layers of security embedded into them: the first layer deals with a trust-based look-up table (LUT) which stores key value or key expression pairs, while the second layer is a chaotic communication layer which ensures a second-level check on primary user emulation nodes.

A sample LUT stored in two of the nodes is shown in Table 2. The same LUT for each of the nodes is present with the router/home node/base station node.

The process of trust-based attack removal is depicted in Fig. 2.

The procedure for identifying the attacker node can be illustrated as follows:

1. The secondary user (SU) node sends a communication request to the router or base station or home node (*R*).
2. The router (*R*) identifies the node number of SU from the request and responds with a random challenge (*C*).
3. The SU gets this challenge and may respond in the following two ways:
   (a) If the SU is genuine, then it will check the LUT and solve the challenge (*C*) to get the solved value (Sv) and then send Sv back to the router.
   (b) If the SU is an attacker, then it will respond with a random solution (Sr) to the router.
4. The router will solve the challenge (*C*) locally by the LUT of the requesting SU node and keep the correction solution (Sc) ready for comparison.
5. If the SU is genuine, then Sv will match Sc, and the communication will proceed.
6. If SU is an attacker, then Sr will not match Sc, and the node will be identified as an attacker node. The router will block all communications from this node, and the attacker will be removed from the cognitive radio environment.

This algorithm can be defeated only under two scenarios:

1. If the attacker knows about the trusted LUT of the node (which is always kept private).
2. If the attacker responds with the correct challenge answer (random distribution).

From the above 2 cases, it is found from our simulations that case 1 is invalid, as the attacker is usually ad hoc and will never have the private LUT information. But, the second case can happen. In our simulations, we found that in 1 out of 1,000,000 times, the attacker can correctly answer the challenge and get access to the communication system. While this issue can be resolved by increasing the complexity of the LUT key values or key expression pairs, but it also adds exponentially to the complexity of the overall system, which adds a delay in subsequent communications.

To tackle this condition, we have designed a second attack detection layer which is a combination of chaotic communication, tag-based system and a BER analyzer. The second layer scans for pre-decided patterns which are stored at the non-attacking secondary user nodes and continuously monitors the channel. These patterns are unique for different secondary users, and they are known to the network router in advance.

In the second layer, the secondary user will send out its test signal pattern; this test signal is encrypted using a 3-level Lorenz's chaotic attractor encoder for security. The

Table 1 Review of the literature on primary user emulation attack

Serial no.	Contributions	Method/model contributions	Key features/description
1.	Chen and Park (2006)	Used two methods, distance difference test and distance ratio test, finds distances from CR to PU and malicious user	Using the distance information, it is determined whether the transmission is from genuine PU or a malicious attacker
2.	Chen et al. (2008)	Location-based method (LocDef), location estimation, RSS, TDOA	Uses both signal characteristics and primary transmitter's location to detect PUEA
3.	Haghighat and Sadough (2014)	Energy detection method-based spectrum sensing	New spectrum sensing method using energy detection is proposed, and the results are compared with an always present attacker
4.	Liu et al. (2010)	Placing helper node close to the primary users and replicate the characteristics of PU, the secondary users can detect PUEA	Confirms the FCC requirement infrastructure is quite expensive as helper nodes are required
5.	Nguyen-Thanh et al. (2015)	Game theory-based approach to combat PUEA and exhibition using Nash equilibrium (NE)	Channel surveillance process is implemented for determining the active user and attacker; an extra sensing process is also proposed for spotting new opportunities to access the channel
6.	Tan et al. (2011)	Cryptography-based method, channel impulse response (link signatures) embedded in modulation or coding	Adding authentication tags, to channel impulse response (link signatures) embedded in modulation and coding, modifies legacy user signal, not recommended by FCC
7.	Anand et al. (2008)	First analytical model to study PUEA, based on Fenton's Approximation Technique and Markov inequality	Various parameters affecting PUEA have been studied in a fading wireless environment; it is shown that as the distance between the primary transmitter and secondary user increases the probability of a successful PUEA also increases
8.	Thanu (2012)	Location estimation technique using Hidden Markov Model	The incumbent signal is authenticated at CR receiver by comparing the received signal by a priori estimates of the link signatures of PU learned from the environment
9.	Alahmadi et al. (2014)	Advanced encryption standard (AES) and secured hash algorithm (SHA)-based approach	No change in hardware, uses a plug-in AES chip, accurate identification of PU, also detects the malicious user in the presence or absence of PU
10.	Chen et al. (2016)	Probability density function (PDF) and belief propagation (BP)-based algorithm is proposed	Based on PDF each CR calculates its belief value and exchanges this information with other users, then compares this value with a threshold for a decision on PUEA, no location information of PU is required; however, hardware cost is increased
11.	Ghaznavi and Jamshidi (2017)	Received power characteristics of cognitive users are used to detect PUEA	Each CR has energy detector and performs spectrum sensing, sends a report to FC, three scenarios: 'Always ON' attack, 'Probabilistic' attack and 'Adverse' attack are studied; a decision metric is compared with a threshold; and FC makes a final decision about ongoing transmission about PUEA
12.	Li et al. (2016)	Doppler spread and variance of received signal power is used for detection	The variance of received signal power is used as a signature of the transmitter so that the detection performance is not affected because of the relative positions of SU and PUE
13.	Liu et al. (2016)	Proposes an expectation maximization-based algorithm, estimates channel parameters	Malicious user estimates the transmission power and channel parameters of PU and learns them and then emulates; the difference in parameters of PU channel and attack channel are then used to detect PUEA
14.	Chakravarthy et al. (2017)	Underlay RF fingerprint in PU signal is introduced, based on cyclostationary feature detection of a signal	A novel solution to mitigate PUEA, however, modifies PU signal, which is not allowed by FCC; a priori knowledge of PU signal required; and uses cyclostationary feature method and hence involves computational complexity
15.	Ghaznavi and Jamshidi (2015)	Cluster-based model is used, makes use of ML algorithm	The FC detects the trusted sensors, instead of searching for malicious sensors; exchange of raw data between Fc and sensors is reduced significantly

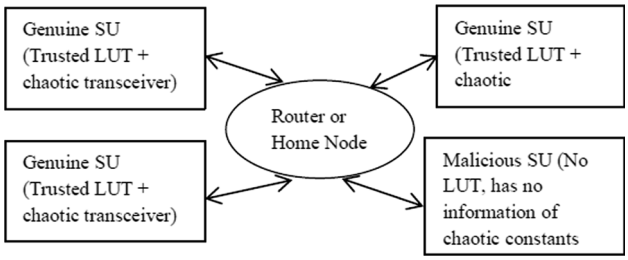

Fig. 1 System model

Table 2 LUT stored at any two of the nodes

Node no.	Input data range (x)	Output value (y)
1	< 10	$x \times 2$
1	< 30	$x/2$
1	< 50	$(x + 2)$
1	< 250	$1/x$
1	< 500	$\sqrt[3]{x}$
1	< 1000	$(x + 1)/(x^2 - x - 1)$
1	≥ 1000	$(x^2 + 1)/(x^3 + x^2 + x + 1)$
2	< 15	$(x + 2)$
2	< 40	$(x - 2)$
2	< 65	$x \times 2$
2	< 125	$(x/2)$
2	< 450	$(x + 5)$
2	< 1200	$(x - 1)/(x^2 - x - 1)$
2	≥ 1200	$(x^2 - x - 1)/(x^3 + x^2 + x + 1)$

Lorenz's chaotic attractor is represented by the following three equations (Kuo et al 2009):

$$\frac{dx}{dt} = \sigma(y - x)$$
$$\frac{dy}{dt} = x(\rho - z) - y$$
$$\frac{dz}{dt} = xy - \beta z$$

here σ, ρ and β are the nonzero constants, and x, y and z are the dynamic states. The encoded test signal pattern behaves like a random noise sequence, is unique and does not interfere with other secondary user patterns as they are orthogonal and have different values for the chaotic constants used in the encryption and decryption process. The non-attacking secondary user transmits a chaotic sequence and is decoded by the receiver/router. As the receiver/router already knows the encryption constants, the sequence is decoded properly, with almost no to minimum errors so that the BER on the receiver side is either 0 or a minimal value. But, if an attacking node transmits any random sequence to gain access over the channel, then improper decoding of the sequence will take place at the receiver/router, and the BER value between the unknown received signal and the known transmitted signal will be very high. In this way, the attacker would be identified. In our simulation process, we have kept the BER threshold at 0.7, which ensures that even if the channel has multiple non-attacking users, then too there are minimal false positives detected by the system. Our proposed results show an accuracy of more than 99% in detection of the primary user emulation attackers and thus are very effective in ad hoc and non-ad hoc cognitive networking environment. A combination of these two layers ensures a detection rate of about 99% which is suited for real-time applications. The delay analysis shows that the system can detect the attacker node in at most two communication sequences, which take less than 1 ms of communication delay per node. Our overall system is very lightweight as there are no complicated, compute-intensive calculations in the system, which will overload the system with preprocessing operations.

To check the system performance, we performed tests with a different number of attacker nodes and under varying channel conditions such as the AWGN, Rayleigh, Rician and Nakagami.

3 Results and Analysis

In our experiments, we used the following setup as shown in Table 3.

Table 4 shows the performance regarding delay and accuracy of attacker node detection for our system. The

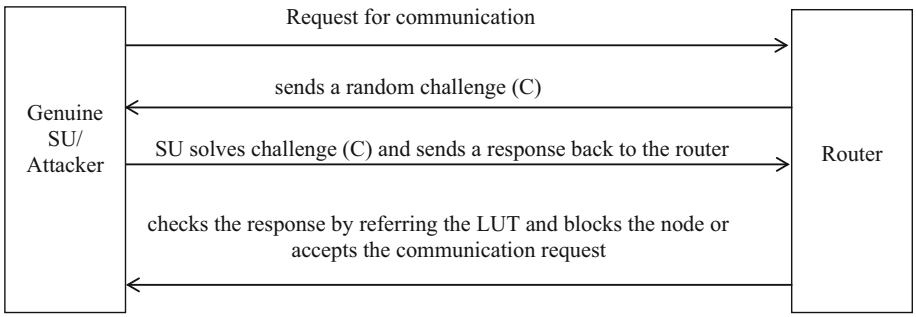

Fig. 2 Trust-based attack removal

Table 3 Parameters and values used in simulation

Parameter	Value
Number of nodes	10–10,000
Number of attackers	10–40%
FFT size	64
Carriers	4
Modulation type	QAM
Chaotic system	3 level
BER threshold	0.7

two-layered approach performs very well under various channel conditions; the detection rate is fairly impressive with the system detecting about 99% of the attacks, with a delay of fewer than 1 ms for each of the AWGN, Rayleigh, Rician and Nakagami channels as shown in Table 4. We used the MATLAB platform to perform all our tests.

The overall system performance can be depicted by the graphs shown in Fig. 3. Figure 3a shows plot of the detection rate versus the number of nodes in AWGN, Rayleigh, Rician and Nakagami channels. Figure 3b shows the plot of delay in detection versus the number of nodes in

Table 4 Detection rate and delay under various channels and attackers

Channel type	Number of nodes	Number of attackers	Detection rate (%)	Mean delay (ms)
AWGN	10	2	99.95	0.1
AWGN	20	6	99.96	0.3
AWGN	30	10	99.96	0.4
AWGN	40	18	99.97	0.45
AWGN	50	22	99.97	0.55
AWGN	100	35	99.97	0.65
AWGN	500	200	99.98	0.75
AWGN	1000	350	99.98	0.88
AWGN	10,000	2500	99.99	0.95
Rayleigh	10	3	99.94	0.15
Rayleigh	20	8	99.95	0.25
Rayleigh	30	12	99.96	0.35
Rayleigh	40	20	99.96	0.5
Rayleigh	50	21	99.97	0.6
Rayleigh	100	30	99.97	0.7
Rayleigh	500	180	99.98	0.76
Rayleigh	1000	320	99.98	0.9
Rayleigh	10,000	2300	99.99	0.94
Rician	10	2	99.92	0.18
Rician	20	6	99.93	0.28
Rician	30	9	99.95	0.37
Rician	40	18	99.95	0.49
Rician	50	22	99.96	0.56
Rician	100	25	99.96	0.67
Rician	500	160	99.97	0.71
Rician	1000	280	99.97	0.82
Rician	10,000	2400	99.98	0.91
Nakagami	10	2	99.91	0.24
Nakagami	20	6	99.92	0.31
Nakagami	30	9	99.92	0.38
Nakagami	40	18	99.92	0.52
Nakagami	50	22	99.93	0.59
Nakagami	100	25	99.93	0.72
Nakagami	500	160	99.93	0.83
Nakagami	1000	280	99.94	0.89
Nakagami	10,000	2400	99.94	0.94

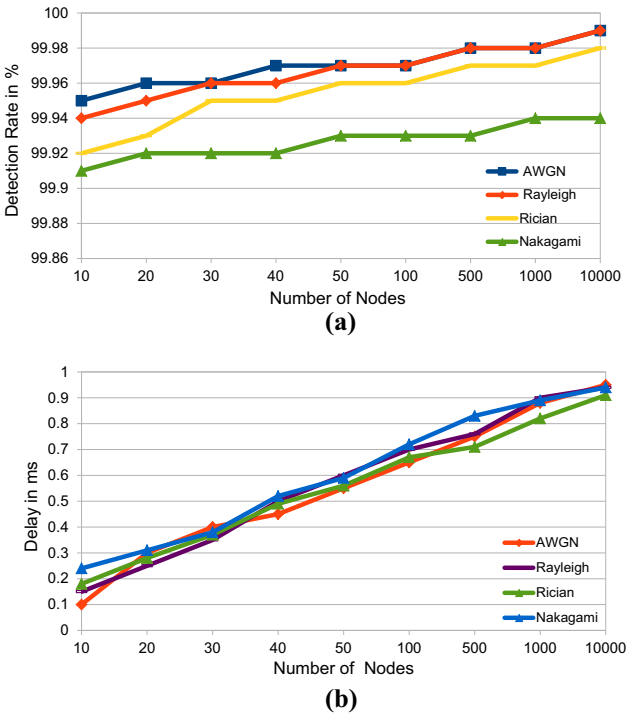

Fig. 3 **a** Detection rate (%) v/s number of nodes. **b** Delay in detection v/s number of nodes

AWGN, Rayleigh, Rician and Nakagami channels, respectively.

The delay performance of the system starts increasing linearly as the number of nodes is increased, but it saturates around 0.85–0.95 ms. The delay for detection is almost independent of the wireless channel, however, there is a marginal change in detection rate because chaotic communication will result in a change in BER whenever there is a change in wireless channel. Detection rate accuracy is found to be in the 99.9% level due to the two-layered communication system, but the system performance under AWGN channel is slightly better than Rayleigh. However, the performance of the system in Rician channel falls behind when compared to AWGN channel performance. This is because signal gets distorted in the Rician channel to a level higher than in the AWGN channel. However, the detection rate under LUT and chaotic communication is in the 99% range bracket which is much higher than the conventional primary emulation attack detection techniques. The newest and most accurate firefly-based technique (Ghanem et al. 2016) gives a detection accuracy of 95%, while physical network coding-based techniques (Xie and Wang 2013) give a maximum accuracy of 90–95% depending on the number of attackers used for simulating the networks. The proposed system's accuracy is about

Table 5 Spectrum sensing techniques (advantages/disadvantages)

Spectrum sensing technique	Advantages/disadvantages
Energy detection method	Sensing time is high
	No prior knowledge of primary user signal is required
	Cannot distinguish between noise and primary user signal
	The most popular method
Matched filter detection	Requires short sensing time
	Requires dedicated sensing receiver for all primary user signal types
	Requires prior knowledge of primary signal
Cyclostationary feature detection	Perhaps the most efficient method
	High computational complexity
	Sensing time is high
	Increase in cost

Table 6 Proposed method's advantages and disadvantages

Technique	Advantages
Proposed test signal method of mitigating PUEA	Use of look-up table (LUT) provides more security
	No prior knowledge of primary user signal is required by SU
	Chaotic test signal provides more security
	No complex computations involved
	Chaotic signals are low-power signals
	Confirms to FCC solution to mitigate PUEA
	Economic approach, no extra cost involved

99% under different channel scenarios and under varying node numbers outperforming the methods proposed in Ghanem et al. (2016) and Xie and Wang (2013).

Moreover, in our proposed method we have not used any traditional spectrum sensing methods and thus wish to state the advantages of our proposed method over traditional spectrum sensing methods. Table 5 below shows the advantages and disadvantages of traditional spectrum sensing methods, and then, we have listed the advantages of our proposed method in Table 6.

4 Conclusion

This research work has demonstrated a very successful detection rate while maintaining a low delay rate for attack detection. More number of attack detection algorithms can be implemented with the proposed two-layered approach. The system architecture is such that almost all of the network primary emulators are detected and removed from the network to ensure a healthy cognitive radio network environment. The overall detection rate of the primary user emulation attack is about 99% under different wirelss channels and varying attacker nodes. In the end, we conclude that as the delay of detection is very less, the proposed method can be used in real-time cognitive radio environment.

5 Future Work

To augment further this research work, we can add more attacks to the system for example, Byzantine attack and check the performance of the two-layer model. We can also add attack-removal strategies for various other attacks because our implementation can detect the attackers in a very short span of time. In future we will work towards the FPGA and IoT level implementation of the proposed approach to test the performance in real time scenario.

References

Alahmadi A, Abdelhakim M, Ren J, Li T (2014) Defense against primary user emulation attacks in cognitive radio networks using advanced encryption standard. IEEE Trans Inf Forensics Secur 9(5):772–781

Anand S, Jin Z, Subbalakshmi KP (2008) An analytical model for primary user emulation attacks in cognitive radio networks. In: 2008 3rd IEEE symposium on new frontiers in dynamic spectrum access networks, Chicago, IL, pp 1–6

Chakravarthy R, Huang K, Zhang L, Wu Z (2017) Primary user authentication of cognitive radio network using underlay waveform. In: 2017 Cognitive communications for aerospace applications workshop (CCAA), Cleveland, pp 1–5

Chen R, Park JM (2006) Ensuring trustworthy spectrum sensing in cognitive radio networks. In: IEEE workshop on networking technologies for software defined radio (SDR'06), pp 110–119

Chen R, Park JM, Reed JH (2008) Defense against primary user emulation attacks in cognitive radio networks. IEEE J Sel Areas Commun 26(1):25–37

Chen Y, Yang L, Ma S, Yuan X (2016) Detecting primary user emulation attacks based on PDF-BP algorithm in cognitive radio networks. In: 2016 IEEE international conference on internet of things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (Smart Data), Chengdu, pp 660–666

Ghanem WR, Shokair M, Desouky MI (2016) An improved primary user emulation attack detection in cognitive radio networks based on firefly optimization algorithm. In: 2016 33rd national radio science conference (NRSC), Aswan, pp 178–187

Ghaznavi M, Jamshidi A (2015) A reliable spectrum sensing method in the presence of malicious sensors in distributed cognitive radio network. IEEE Sens J 15(3):1810–1816

Ghaznavi M, Jamshidi A (2017) Defence against primary user emulation attack using statistical properties of the cognitive radio received power. IET Commun 11(9):1535–1542

Haghighat M, Sadough SMS (2012) Cooperative spectrum sensing in cognitive radio networks under primary user emulation attacks. In: 2012 6th international symposium on telecommunications (IST), Tehran, pp 148–151

Haghighat M, Sadough SMS (2014) Cooperative spectrum sensing for cognitive radio networks in the presence of smart malicious users. AEU Int J Electron Commun 68(6):520–527

Kuo HH, Liao TL, Lin JS, Yan JJ (2009) A new structure of chaotic secure communication in wireless AWGN channel. In: 2009. IWCFTA '09. International workshop on chaos-fractals theories and applications, Shenyang, pp 182–185

Li Y, Han C, Wang M, Chen H, Xie L (2016) A primary user emulation attack detection scheme in cognitive radio network with mobile secondary user. In: 2016 2nd IEEE international conference on computer and communications (ICCC), Chengdu, pp 1076–1081

Liu Y, Ning P, Dai H (2010) Authenticating primary users' signals in cognitive radio networks via integrated cryptographic and wireless link signatures. In: 2010 IEEE symposium on security and privacy, Oakland, pp 286–301

Liu L, Zhang Z, Li J (2016) EM-based algorithm for defeating against primary user emulation attacks in cognitive wireless networks. In: 2016 2nd IEEE international conference on computer and communications (ICCC), Chengdu, pp 1450–1455

Nguyen-Thanh N, Ciblat P, Pham AT, Nguyen VT (2015) Surveillance strategies against primary user emulation attack in cognitive radio networks. IEEE Trans Wireless Commun 14(9):4981–4993

Tan X, Borle K, Du W, Chen B (2011) Cryptographic link signatures for spectrum usage authentication in cognitive radio. In: Proceedings of the 4th ACM conference on wireless network security, pp 79–90

Thanu M (2012) Detection of primary user emulation attacks in cognitive radio networks. In: 2012 International conference on collaboration technologies and systems (CTS), Denver, pp 605–608

Xie X, Wang W (2013) Detecting primary user emulation attacks in cognitive radio networks via physical layer network coding. In: 2013 International workshop on communications and sensor networks (ComSense-2013), procedia computer science, vol 21, pp 430–435