ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 6, June 2018

Mitigation of ISSDF Attacks by using Mobility and Context Aware Trust Management Algorithm

Headar Tarsh Batool[1], Prof.Dr. R.S.Kawitkar[2]

Dept. of E&TC / Sinhgad College of Engineering[1,2]

Abstract: The dynamic spectrum access in Cognitive Radio Networks (CRNs is found, in which Secondary Users (SUs) can use the licensed spectrum bands which are based on opportunistic non-interference. These networks are based on efficient cooperation between the secondary users (USs) in its operation regarding the spectrum sensing. Many kinds of attacks can affect on performance of CRNs very harmful, one of these types is the Insistent Spectrum Sensing Data Falsification (ISSDF) attack. Many recent studies proposed methods based on trust management to face such attacks, but these methods were not enough to alleviate such attacks especially in the dynamic environment where primary users (PUs) repeatedly transitions between active and inactive state. In this paper we propose a novel technique efficient ISSDF attack alleviation method for the Distributed Cooperative Spectrum Sensing (DCSS) in the Cognitive Radio Ad Hoc Networks (CRAHN). The proposed method is based on mobility aware technique for energy efficient ISSDF attack mitigation along with context aware distributed trust method. The SU nodes analyse the trustworthiness with each other using PU absent and present contexts in which they make observations from each other by considering mobility and energy values of SUs. The utilization of energy values and mobility of SUs helps to extend the network operational lifetime while dealing with ISSDF attacks.

Keywords: Secondary Users, Insistent Spectrum sensing data falsification, Primary User, Cognitive Radio Ad hoc Networks, Context aware, mobility aware

I. INTRODUCTION

Now days, the applications of wireless networking technologies are increasing tremendously. Some new methods, protocols, devices, and applications are consistently acquainted with the clients, making chance for better approaches for communicating and expanded profitability in the expert circle. The numerous wireless devices have been developing exponentially. In excess of 6 billion cell phone participations notwithstanding extraordinary wireless devices, for instance, Wi-Fi devices and it is represented toward the complete of 2011 as showed by the International Media Telecommunication Union (ITU) report - Estimating the Data Society 2012. As indicated by a near report, around 85.7% of the world's masses have their own particular cell phone enrolments [1] [2].

Beginning late, the influencing of the Internet of Things (IoTs) and Cyber Physical Systems (CPS) is offering chance for context-aware mindful offices. With IoTs and CPS, a massive number of devices can be networked to offer new office [1]. These movements, regardless, have other than agreeable new challenges with respect with the administration of spectrum, which isn't an abundant asset.

The administration of radio frequencies in different countries and districts, each with their own specific controllers, is overseen by techniques under the umbrella of the ITU. For example, the Federal Conversation Commission (FCC) and National Telecommunications and Information Administration (NTIA) in the Unified States manage the utilization of range by non-government and government customers, autonomously.

In Europe, the European Meeting of Postal and Telecommunications Organization are in charge of the radio repeat parcel. The range is assigned for different rehash and types of progress by these controllers. The allotted domain is for select use by a particular movement or advantage and these bands are called embraced bands and the rest are unlicensed bands. The customers that are guaranteed to use these frequencies are known as the affirmed customers or major customers [3].

Cognitive Radio (CR) and Cognitive Radio Networks (CRNs) are giving a response for resolve or if nothing else bolster this anomaly [4]. The basic idea of the CR thought, in this recommendation, is to let unlicensed customers (also called right hand customers or SUs have endorsed bands when the PUs isn't utilizing them. The unused affirmed bands in time and rehash areas are called White Spaces (WSs); the SUs endeavour to use WSs without making any hindrance the PUs. As necessities are, the time when a PU shows up, SUs ought to stop using that particular WS immediately. It has enlivened diverse standardization get-togethers, for instance, Ecma, IEEE 802.22, IEEE 802.11af, IEEE 802.16h, IEEE 802.19.1 and IEEE Dynamic Spectrum Access Networks (DySPAN) 1900.6 [5][6].

Regardless, the open thought of such networks can provoke unmistakable attacks, for instance, Spectrum Sensing Data Falsification (SSDF) and Insistent SSDF (ISSDF) strike. The SSDF is a called strike for pleasant spectrum sensing designs, where malignant SUs bestow bended sensing information to their neighbors so as to cheat them and exchange

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 6, June 2018

off the spectrum sharing in the academic radio framework [7]. The ISSDF assault is more destructive than SSDF in which the assailant distorts its sensing data as well as broadcasts misrepresents an incentive in every cycle of the participation and ceases from refreshing its incentive as indicated by the iterative the protocol [8].
In recent past, number of solutions presented to mitigate the effects SSDF and very few methods for ISSDF attacks. The mitigating the ISSDF attacks in ad hoc CRNs is challenging task due to mobility and dynamic network settings. In this paper, we propose the context aware ISSDF mitigating technique. In section II, the brief study on related works presented. In section III, the algorithm and architecture for proposed method presented. In section IV, the simulation results discussed. Finally, the conclusion and future discussed.

II. RELATED WORKS

This section presents the study of recent works reported on security for CRNs.
In [1], the researcher depicts a CRN in light of IEEE wireless regional area network (WRAN) and portrays a touch of the security risks against it. For the colleague clients in the CRN to quickly see whether they are being trapped, a principal yet handy ID is then showed up. Their proposal uses non-parametric cumulative sum (cusum) as the change oversee unmistakable proof algorithm to locate the sporadic direct in context of assaults. The maker proposed IDS gets a variety from the standard unmistakable proof approach and it profiles the CRN structure parameters through a learning stage. In this manner, their proposal is in like manner orchestrated to see new sorts of strikes.
In [2], the researcher perceive another intolerant attack write in academic radio exceptionally selected networks and propose a clear and proficient narcissistic cognitive radio ambush affirmation methodology, called COOPON, with multichannel resources by pleasant neighbouring cognitive radio focuses.
In [3], the researcher proposed a proficient AES-based DTV plan, where the ebb and flow reference movement used to make the P2 pilot pictures in the DVB-T2 plots is encoded utilizing the AES algorithm to empower exact basic customer and dangerous customer affirmation. With the proposed plot, they can see PUEA conclusively finished all subcarriers or sub-bands where the P2 pictures appear. Second, they consider a productive correspondence plot for the assistant customers (SUs) under PUEA by mishandling the imperativeness gathering systems. Perfect power part is considered for sum rate expansion.
In [4], the channel-tap power is utilized as a radio-frequency fingerprint (RF) to by and large observe fundamental client copying strikes (PUEAs) over multipath Rayleigh clouding channels. To know identities of fundamental customers and PUEAs, the cross-layer impressive getting the hang of limit of an adaptable right hand client (SU) is manhandled to set up exposure databases by strategies for dependably consolidating the shrewd area of physical (PHY) layer with the precision of higher layer affirmation.
In [5], the researcher proposed spread iterative date-book opening dispersing algorithms for SSI sharing on a submitted fundamental control channel in a cognitive radio impromptu network circumstance. The philosophy in light of a crash unmistakable proof and confirmation plan that arrangement empowers the network focus focuses to get getting some answers concerning crashes with respect to their transmitted SSI bundles.
The centre points use that data to revive their working availabilities using a probabilistic approach; each centre point keeps up and invigorates a parameter speaking to the likelihood of trading the planned opening on account of a crash. Both settled and versatile likelihood based plans are proposed.
In [6], researcher presented a technique for revelation and partition of such threatening customers. Likewise, they besides presented how they can utilize the framework on spouting information (sensing reports) and along these lines perceive and disengage aggressors on the fly.
In [7], the researcher concentrated on security issues ascending out of PUE ambushes in CR networks. They demonstrated an aggregate prelude to PUE ambushes, from the striking procedure for considering and its impact on CR networks to certification and insurance approaches. Reviewing an authoritative objective to secure CR networks against PUE strikes, a two-level database-helped disclosure approach needed to perceive such ambushes.
In [8], the spectrum sensing and spectrum sharing are two essential issues in a cognitive radio network (CRN). The spectrum sensing data falsification (SSDF) strike powers insidious effect on the two areas perceiving system and range sharing method. Reviewing an authoritative focus to deal with the SSDF assault and in penny optional clients (SUs) to hold up under on well, a joint spectrum sensing and asset dispersion (JSSRA) plot in a CRN is proposed.
In [9], the researcher gave a short organization of CR systems and the essential research points of view of their change close to their standardization works out, as a result of their examination. It took after by the isolated examination of the end wine based CR network (CRN) and by a point by point association with the get-together of underlay based CRNs. In the ribbon based CRN, sensing of the Primary User's (PU) spectrum by the Secondary Users (SU) has remained a test, because of truth that the sensing messes up shield us from fulfilling the titanic throughput grabs that the probability of Cognitive Radio (CR) ensures.
In [10], protection plot called Attack-Aware CSS (ACSS). This strategy checks attack quality and applies it in k - out-N controls to secure the perfect estimation of k that limits the Bayes shot. The strike quality is depicted as the extent of

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 6, June 2018

the amount of undermining clients to the aggregate number of clients, which partners to the probability that a specific customer is dangerous.

In [11], the researcher concentrated on security issues rising up out of essential client imitating (PUE) assaults in CR networks. They demonstrate a concentrated prologue to PUE ambushes, from the assault protection and its impact on CR networks, to perceiving proof and check approaches. With a particular authentic objective to secure CR networks against PUE strikes, a two-level database-helped perceiving proof approach is proposed to see such ambushes. Significance unmistakable proof and area check are joined for speedy and demonstrated exposure. An attestation control-based secure approach is proposed to alleviate the execution debasement of a CR network under a PUE trap.

In [12], the researcher proposed a novel security structure to deter SSDF strikes by competently checking unmistakable information with the help of trusted in focus focuses. The proposed plot uses a profitable and quick reputation based algorithm to investigate the lead of every client. As needs be, not exclusively will reliable substantial information be perceived by the central substance, yet what's progressively; pernicious clients can be suitably recognized and removed from the network.

In [13], they symptomatically demonstrated the CGBN-HARQ design with the guide of a Discrete Time Markov Chain (DTMC). Explicitly, an algorithm is passed on for social event all the genuine states and for wiping out the ludicrous states, which causes us in diminishing both the dimensionality of the state change grid and the related computational multifaceted nature. Every single above strategy masterminded assaults other than ISSDF. However there is only a solitary late framework [14] that clearly discussed the ISSDF attack, its impact and the method for mitigations using the context of PUs and SUs. In any case, the watching PUs at each cycle is extra overhead.

III. METHODOLOGY

This examination demonstrates the upgraded context-aware trust management scheme that withdraws the perceptions in observe on the speculated context (PU-Missing or PU-Show). At each sensing round, each SU assesses about the PU activity utilizing the whole bit of the accessible data (from its own particular sensing and its teaming up neighbours' reports) and suppositions the present context. In context of this speculated context, the SU will record the observations from its neighbours in the relating acknowledgment vectors.

Additionally, automatic PU monitoring introduced to reduce the overhead. This can solves the problem in which SU needs to continuously monitoring the PUs context such as absent or present. This unnecessarily leads the communication overhead among all SUs as well as increases the interference with PU. We utilized the SUs position and designed the auto refreshed PUs. In this case, the context of PUs is periodically broadcasting to its neighbour moving SUs. This can help to significantly reduce the communication overhead.

Algorithm 1 presents the proposed context aware observations which are for context-aware trust management.$g_{ij}(t)$denotes the initial value that node i coming from neighbour j in the first consensus iteration of sensing round t, thus, $g_{ij}(t)$ is equivalent to $\upsilon_j(0)$. The final estimate of node i at sensing round t is denoted by $y_i(t)$ which is equivalent to $\upsilon_i(c = \text{final iteration})$. Γ denotes the detection threshold. At sensing round (time) t, node i calculates two trust scores, $\theta_{ij}^{A}(t)$ and $\theta_{ij}^{p}(t)$ based on the absent and present observation vectors, respectively.

Algorithm 1: Proposed Algorithm

Sensing round t:
Node i observe node j:

1. PU broadcasts the Boolean value to nearest SUs
   Cont = broadcast (PU)
2. At SU's,
3. if Cont is true,
4. sets context :PU –Absent
5. else
6. sets context :PU –Present
7. **if** $\left(g_{ij}(t) < \gamma\right)$ **then** // i and j in Agreement
8. $o_{ij}(t) = 1$
9. **else** // i and j in Conflict
10. $o_{ij}(t) = 0$
11. **end**
12. Add $O_{ij}(t)$ to O_{ij}^{A}; // Add to Absent Vector
13. **else if** $(y_i(t) < \gamma)$ **then** // i sets context: PU-Present
14. **if** $\left(g_{ij}(t) < \gamma\right)$ **then** // i and j in Agreement
15. $o_{ij}(t) = 1$
16. **else** // i and j in Conflict

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 6, June 2018

17. $o_{ij}(t) = 0$
18. **end**
19. Add $O_{ij}(t)$ to O_{ij}^{P}; // Add to Present Vector
20. **end**

The functionally of proposed method is represented in figure 1.

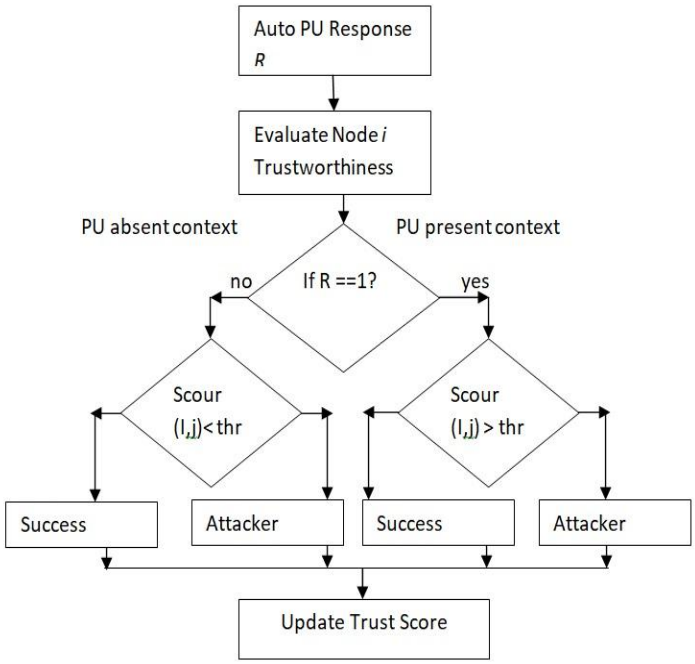

Figure 1: Proposed System Architecture

IV. SIMULATION RESULTS

In this section, we present the current results using the network simulator NS2. We evaluated the methods using the ns-2.34 version on Ubuntu 12.04. The network parameters and techniques represented in table 1. The proposed ACATRT (Automated Context Aware Trust based Routing Technique) method is compared with two state-of-art methods in this section such as CRNRT [19] and CATRT [19].

Table 1: Network Simulation Parameters

Number of Primary Nodes	48
Traffic Patterns	CBR (Constant Bit Rate)
Number of Secondary Users	7
Number of attackers	6
Network Size (X x Y)	1000 x 300
Max Speed	10 m/s
Simulation Time	30 seconds
Packet Interval	0.1-0.3-0.5-0.7-0.9
Pause Time	1.0s
Routing Protocol	CRNRT/CATRT/ACATRT
MAC Protocol	802.22
Threshold (γ)	[-96 , -80] dBm

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 6, June 2018

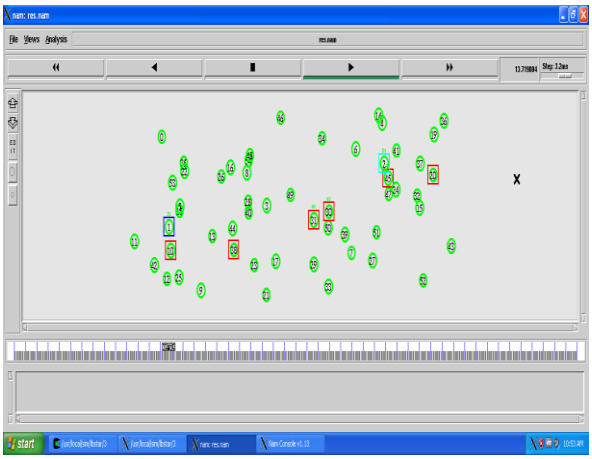

Fig. 2. Detected Nodes and Attacks

In the above figure showing the all available Nodes, the s1 node is Source Node, d1 Node is Destination Node and all other red Nodes are attacks.

There are four performance metrics evaluated in this paper such as:

- Network Throughput vs. Packet Rate
- Packet Delivery Ratio (PDR) vs. Packet Rate
- Energy Consumption vs. Packet Rate
- Number of packet drops vs. Packet Rate

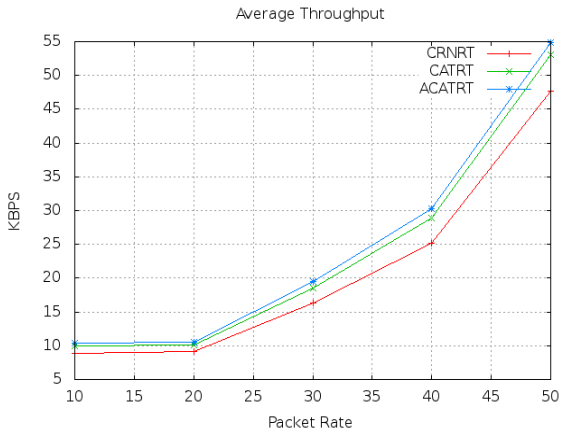

Figure 3: Average throughput performance evaluation

Figure 4: PDR performance evaluation

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 6, June 2018

As showing in the performance of throughput and PDR, the proposed ACATRT technique improves the performance due to the effective strategies designed for the optimum opportunistic routing under the presence of ISSDF attackers. The throughput and PDR performances are increasing with increased number of WBANs.

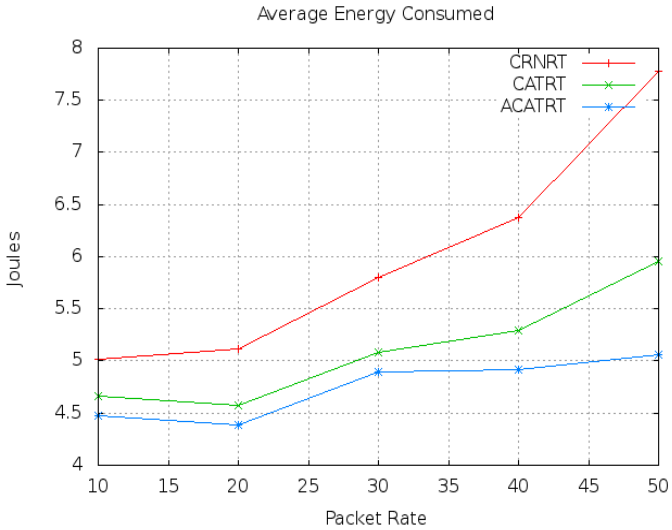

Figure 5: Average energy consumption performance evaluation

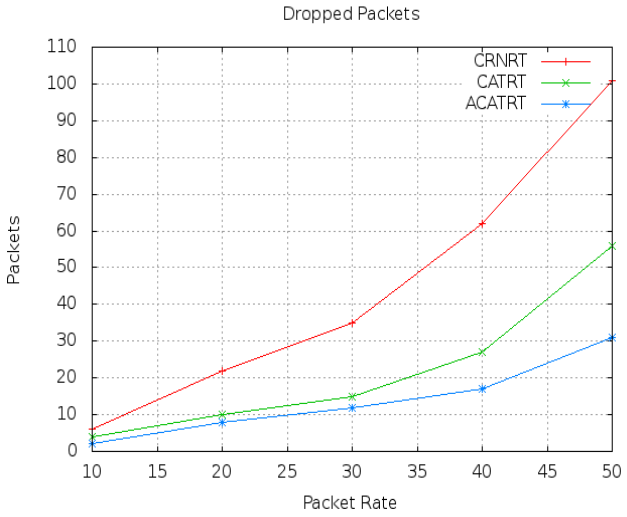

Figure 6: Number of packets drop performance evaluation

Similarly, the average energy consumption performance is optimized using the proposed solution for the varying WBANs. The results of packet drops denotes that there is severe impact of ISSDF attacks on existing methods CRNRT and CATRT which is minimized by proposed method.

CONCLUSION AND FUTURE WORK

This examination introduces the novel versatile context-aware trust management scheme which is teamed up into the passed on helpful spectrum sensing so as to altogether upgrade the strength of the interest collaboration to relentless spectrum sensing data falsification (ISSDF) assaults. When contrasted with condition of-craftsmanship strategies, the proposed strategy, the proposed technique empowers the auxiliary clients to perform more educated trust assessments of their associates based of the particular situation (paying little mind to whether the essential client is missing or display.).To mitigate the issue of keeps checking of PUs by SUs; we utilized the intermittent refresh method from PUs with help of SUs area. The exploratory outcomes check the productivity of proposed strategy over the current strategies. For future work, it wills enthusiasm to research the varieties in other imperative parameters of, for example, portability speed, parcel rate and so forth.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 6, June 2018

REFERENCES

[1] Zubair Md. Fadlullah, Hiroki Nishiyama, and Nei Kato, "Intrusion Detection System (IDS) for Combating Attacks Against Cognitive Radio Networks", IEEE Network • May/June 2013 0890-8044.

[2] Minho Jo, Longzhe Han, Dohoon Kim, and Hoh Peter In ,"Selfish Attacks and Detection in Cognitive Radio Ad-Hoc Networks", IEEE Network • May/June 2013.

[3] Ahmed Alahmadi, Zhaoxi Fang, Tianlong Song, and Tongtong Li,"Sub-band PUEA Detection and Mitigation in OFDM-based Cognitive Radio Networks" IEEE Transactions on Information Forensics and Security, 2015.

[4] Trong Nghia Le, Wen-Long Chin and Wei-Che Kao," Cross-Layer Design for Primary User Emulation Attacks Detection in Mobile Cognitive Radio Networks", IEEE COMMUNICATIONS LETTERS, VOL. XX, NO. XX, FEBRUARY 2015.

[5] Jarmo Lundén, Mehul Motani, and H. Vincent Poor," Distributed Algorithms for Sharing Spectrum Sensing Information in Cognitive Radio Networks" IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 14, NO. 8, AUGUST 2015.

[6] Shikhamoni Nath, Ningrinla Marchang and Amar Taggu ," Mitigating SSDF Attack using K-Medoids Clustering in Cognitive Radio Networks",2015 Eight International workshop on selected topics in mobile and wireless computing.

[7] Rong Yu, Yan Zhang, Yi Liu, Stein Gjessing, and Mohsen Guizani,"Securing Cognitive Radio Networks against Primary User Emulation Attacks", IEEE Network July/August 2015.

[8] Huifang Chen, Ming Zhou, Lei Xie, Kuang Wang and Jie Li," Joint Spectrum Sensing and Resource Allocation Scheme in Cognitive Radio Networks with Spectrum Sensing Data Falsification Attack" IEEE Transactions on Vehicular Technology 2016.

[9] Aaqib Patel, Md. Zafar Ali Khan, S. N. Merchant, U. B. Desai and Lajos Hanzo ,"The Achievable Rate of Interweave Cognitive Radio in the Face of Sensing Errors", IEEE Access 2016.

[10] Abbas Ali Sharifi and Mir Javad Musevi Niya ,"Defense against SSDF Attack in Cognitive Radio Networks: Attack-Aware Collaborative Spectrum Sensing Approach", IEEE Communications Letters 2016.

[11] Rong Yu, Yan Zhang, Yi Liu, Stein Gjessing, and Mohsen Guizani," Securing Cognitive Radio Networks against Primary User Emulation Attacks", IEEE Network • November/December 2016.

[12] Yasir Al-Mathehaji, Said Boussakta, Martin Johnston, and Harith Fakhrey," Defeating SSDF Attacks with Trusted Nodes Assistance in Cognitive Radio Networks", 2017 IEEE.

[13] Ateeq Ur Rehman, Lie-Liang Yang,and Lajos Hanzo,"Delay and Throughput Analysis of CognitiveGo-Back-N HARQ in the Face of Imperfect Sensing", 2017 IEEE access.

[14] Aida Vosoughi, Joseph R. Cavallaro, and Alan Marshall, "A Context-aware Trust Framework for Resilient Distributed Cooperative Spectrum Sensing in Dynamic Settings", IEEE Transactions on Vehicular Technology, 2017.