International Journal of Current Trends in Engineering & Technology
www.ijctet.org, ISSN: 2395-3152
Volume: 07, Issue: 01 (January-February, 2021)

An Ant Colony Optimization Algorithm for DOS Attack Detection and Prevention in CRN

Zamarud Khan, Abdul Samee Khan
Department of Electronic Communication
ASCT, RGPV, Bhopal, India
zamar.khan888@gmail.com

Abstract— the attacker presence in CRN is only due to unlicensed user communication or SU presence in the network. The spectrum availability is for both licensed and unlicensed users in the network. The CRN includes the (PU) system with an authorised spectrum and the (SU) system without an authorised spectrum. When the SUs wants to use the spectrum, they have to find the idle channels not occupied by the PUs. The sensor nodes are not known about the attacker because the attacker forwards the fake reply of the route between sender and receiver after that flooding the junk of packets. We take the attack as Dos attack, which generates the junk message and deviates the network functions such as a change in RSS value, profile etc. In ACO routing in CRN, the attacker is detected by not forward the data packets to the next node or destination node in the network. The IDS procedure is validating the attacker presence and also disables the attacker presence in the network. The proposed security scheme is identified as the attacker presence and block their malicious functioning in the network. ACO is not only designed for security purpose but better routing approach. The ACO provides the reliability of communication between the sender and receiver by contributing their role to identify the attacker. The proposed IDS identify the trust value in the network, and the performance of attacker detection is identified by low trust value. In this research, we present the identification or security scheme to prevent the network from DoS attacker. The attacker information is identified by detecting unlicensed users, and these users are doing misbehaviour in the network. The ACO helps identify it based on malicious flooding information and Work on a security scheme to secure all communication. In cognitive radio, the unlicensed user uses the free spectrum holes and security of these holes at communication time. The proposed trusted ACO optimisation algorithm detects the DoS attack by analysing its behaviour, trust value and blocks the attacker node. The proposed approach is simulated in NS-2 (Network Simulator version 2) software.

Keywords:- CRN, stations, attack, Security, IDS, Routing, PSO.

I. Introduction

A Wireless Sensor Network (WSN) collects mobile nodes working without any fixed communication infrastructures or base stations to provide connectivity [1, 2]. The nodes are also working with base stations, but these nodes are not continuously changing their location. Each node in the WSN acts both as a host and a router. Suppose two nodes are not within the transmission range of each other. In that case, other nodes are needed to serve as intermediate routers for the communication between the two nodes Cognitive radio network [3] is one of the most intensely studied fields in a wireless communication network in recent times. Dynamic Spectrum Access (DSA) [4] is a major application of this type of network. This is due to the limited spectrum availability and underutilisation of the allocated licensed spectrums [5] [6]. In this type of network, two classes of users, such as Primary Users (PU) and Secondary Users (SU), are defined. The PUs is the high prioritised licensed user, whereas the SUs are the opportunistic users. These SUs (or sometimes called cognitive radio users) are allocated with any part of the spectrum. As a result, interference will affect both Primary Users (PUs) and other co-located Secondary Users (SUs).To avoids this situation, a proper resource allocation mechanism needs to be framed. Simultaneously, the unused band of spectrum (white space) is detected through the process called Spectrum Sensing. The descriptions of the old Work are as follows.

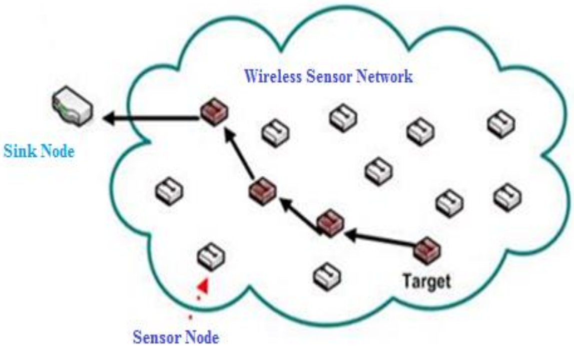

Figure1 Example of WSN

This paper [7] considers routing disruption attacks, which are network layer attacks in CRN. In routing disruption attacks, the malicious nodes attempt to cause packets to be dropped or extra network resources to be consumed. If an attacker is on a certain route, it may drop all of (Primary Users) PUs packets or selectively forward PUs packets. PUs holds licenses for specific spectrum bands in the primary network and can only occupy their assigned portion of the spectrum. SUs does not have any licensed spectrum and opportunistically send their data by utilising idle portions of the primary spectrum. In routing attacks, the malicious SUs may claim that they have the optimum route to the destination. In this way, the honest SUs will forward data packets to the malicious SUs, and all traffic will be routed through it. In the CRN routing context, we define trust as representing the degree that secondary users (SUs) honestly forward data packets to the next hop. In this paper, we will use the statistics of SU forwarding behaviours to construct the trust of neighbouring SU *j* from SU*i* at time t, which is denoted by *T*ij(t). When the data packet of SU *i* needs to be sent to destination SU *j*, a route should be decided between the source and destination pair.

Results Findings:- The first is *Trust values vs simulation time.* This result shows that SU j honestly forwards data packets, and the corresponding trust evaluation of SU j gradually increases, but the presence of attacker trust value decreases.

The second is *End-to-end throughput vs simulation time*. This result shows the trust management model improves the end-to-end throughput in all cases.

The third is *End-to-end delay vs proportion of malicious SUs*. Here end-to-end delay is shown to be improved substantially with the trust management model, especially when the proportion of malicious SUs is high

This paper [8] Credit Risk Value-based algorithm aims to find out the network's selfish nodes. This technique is easy to compute. The CRV technique will sense the attacks of selfish SUs in the network by computing the credit risk value. This technology is being carried out in the fore coming steps. First, it computes the CRV value before transmitting any packet and routes the packet. Again, recalculate the CRV value after routing. The CRV value is constant, which implies the energy consumed for the transmission of packets. In Spectrum Analysis, the spectrum channel network parameters are being analysed for all the spectrum holes. Then, it will be used for the Spectrum Decision process. In Spectrum Decision, the most accurate spectrum hole will be selected by the Cognitive users.

Result findings:- First result is *evaluated the probability of false alarm and probability of detection*. in this result, the attacker detection is confirmed in the network

A second result is the *number of packets sends to nodes and the number of rounds*. These results calculate the number of packets sending in the presence of an attacker.

The third result is based on *energy after routing and the number of rounds*. This result confirms it is the attacker node presence is consuming higher energy in the network.

In this paper [9], CSS has not been discussed with malicious users for all the art's extended state. Meanwhile, to avoid a large interference at the licensed users, a constraint is put on the resulting missed detection probability to keep the interference within the acceptable range. Based on the above mechanisms and motivated by the main existing problems, i.e., the power consumption and poor judgement between honest and malicious users, we propose a trust-based CSS scheme to defence the SSDF attack in CRN. Firstly, we implement a pre-filter among all SUs to select *k* cooperative sensing users based on their SNR. It can save energy and guarantee the valid transmission of data because the nodes under poor sensing circumstance don't need to stop their communication to perform weak sensing. Secondly, there may be some selfish nodes among the selected candidates for sensing. To address this problem and increase access opportunities, we propose a trust-based model to reflect the trustworthy degree of each sensing node's local decision.

Result Findings:- First is the *probability of error detection with varying SNR of SUs.* It means that the presence of malicious users significantly degrades sensing performance.

The second is *Weight comparison for 6 SUs with different attack probability*. It can be seen that a SU in a lower attack. Probability is assigned with a higher weighting coefficient.

The second is the *Global probability of error detection vs the ratio of MUs for different values of the global threshold η*. We also notice that the *Pe* dose does not increase directly with the increasing value of *η*.

Forth is the *Global probability of false alarm vs the ratio of MUs for different fusion rules*. when the proportion of malicious nodes is more than 10% or even higher, global false alarm probability began to decline dramatically

In this paper [10], they propose a distributed trust management solution that does not require a fusion centre, and we show the effectiveness of mitigating belief manipulation attacks. This paper considers belief manipulation attacks and follows a distributed trust management approach to detect and mitigate such attacks. Most of the existing methods to enhance security use authentication and cryptography, aiming at providing data confidentiality, data integrity, and node authentication. However, mitigating against the attacks above cannot be solely done via cryptography and authentication. As a complementary strategy, trust management can further increase CRN's security because it does not assume the statistics are always correct, expire learned beliefs, consider the risk of making decisions, and perform inconsistency checks on parameters statistics.

Result Findings:- First is out *End-to-end throughput when node 2 is malicious, node 5 is a malicious node and node 8 is a malicious node.* The throughput drops the most when the malicious node is located in node 2's position. This is because node 2 is the closest node to node 1 (source node) compared to node 5 and node 8 and has the highest impact on misleading the source node.

The second *is Average throughput vs packet dropping probability*. That shows higher dropping probabilities lead to more throughput degradation for all locations.

The third one is *trust vs time*. In this graph, the thrust value is evaluated in the attack's presence to confirm the attacker presence.

This paper [11] proposes a Trust-based channel-centric approach towards evading selfish collaborative Secondary Spectrum Data Falsification (SSDF) attacks. We discuss two variants of selfish collaboration: static and dynamic. In the static case, the set of attacked channels does not change over time, while in the dynamic case, it does. First, we present a three-step monitoring technique that gathers channel-centric evidence by capturing the advertised occupancy anomalies. First, we estimate the lower and upper bounds on the received power level from a neighbour. The bonds are then compared with some predefined threshold that results in a predicted ternary decision: occupied, not occupied, or cannot be decided. This predicted decision is compared with what a neighbouring node advertised. The comparison yield has three possible outcomes like a match, mismatch, or undecided. The observation data formed by all neighbours' outcomes on a particular channel gives the frequency of matches, mismatches, or undecided matches. More matches indicate agreement on channel occupancy, while more mismatches mean the presence of misleading advertisements.

Result findings:- The first is a Trust-Based Channel Preference. Here, the result shows the channels sorted in a descending manner as calculated by an honest node 12.

The second result is *Channel Preference with more selfish node.* Here, the results show the channels sorted in a descending manner as calculated by the honest node 14. As per most previous works, it is difficult to distinguish dishonest behaviour when the adversary density is higher than fifty per cent.

The third is the *Effect of a fraction of a selfish node.* This result shows the average trust values for the attacked channel set and the non-attacked channel for the increasing number of attackers.

Forth is *Trust variation under dynamic attack.* This result captures the frequent changes in the attacked channel set.

II. Concept of Technology Used in previous Work

The first part of the Work presents the methodology that includes a trilateration technique to get a good estimative location of the PUE based on the RSSI detected between the anchor nodes and the PU/PUE. Then, they apply a Particle Swarm Optimization (PSO) algorithm to minimise the error function based on Trilateration. The second part discusses the results of our simulation. The google localisation technique is obtained through Trilateration under different circumstances. It utilises electronic distance measuring instruments (EDMIs) to calculate the lengths of triangles sides rather than horizontal angles. Besides, it delivers an advantageous cost-benefit ratio compared to other techniques [12]. Through the RSSI technique, it is possible to calculate the exact result between sender and receiver. Attacker detection is possible through RSSI. If the signal strength is weak, then the possibility of data receiving is also affected. The

RSSI has an inconsequential relation between the distance and the environment. Those parameters impact the detection error directly and explicitly on the PUE attack identification. To reduce the deliberate distance's ambiguity, the mobile sensor nodes have to travel toward an optimised position that shows a Low error probability. The attacker detection can be as accurate as possible. The results show the proposed PSO technique provides the accurate position of the attacker in the network. In this position, they detect the attacker by false-positive ration in the network. If the false-positive ratio is more, that means the possibility of attacker detection is more. The results are compared based on Most accurate, Not accurate and Slightly accurate. The result is evaluated between detection error and the number of iterations. The accurate distance is only measured through RSS, and after the anchor node is identified, the attacker presence. Anchor detects the false positive ratio.

Drawbacks of previous Work:-

1) *Attacker nodes quantity is not mentioned.*
2) *The number of packets sends by nodes is not shown.*
3) *The false-positive ratio depends on packet dropping or weak signal strength, but how sure packets are dropped due to attacker presence.*
4) *Why use a location scheme to identified attacker but only weak RSS is satisfactory. Attacker identification is possible if there is a part of routing.*

III. Proposed Approach

The Secondary Users in CR has used the available spectrum holes, and the possibility of attack is more. In future, we will propose a security scheme in CRN to secure the spectrum from the attacker. In this scheme, the ACO (Ant Colony Optimization) technique identifies the attacker existence through pheromones value in the network. In cognitive radio, the unlicensed user uses the free spectrum holes and security of this hole at communication IDS (Intrusion Detection System). It is used to detect and prevent the network from the attacker. The whole communication performing between sensor devices, and these devices are not aware of the attacker. The proposed approach is simulating in NS-2 (Network Simulator version 2) software. In any communication networks, there are two major attacker classifications: on-path versus off-path. An off-path adversary can inject data into a stream or spoof other devices on the network but cannot, in real-time, see the traffic being transmitted. Off-path adversaries can be thwarted by using protocols only to participate if they can see the traffic. Ns-2 extensibility is perhaps what has made it so popular for sensor networks. In addition to the various extensions to the simulation model, the object-oriented design of ns-2 allows for straightforward creation and use of new protocols. The combination of easy protocol development and popularity has ensured that many different protocols are publicly available, despite not being included as part of the simulator's release. Its status as the most used sensor network simulator has also encouraged further popularity, as developers would prefer to compare their Work to results from the same simulator.

Table 1 Simulation parameters will use for simulation

Number of nodes	50
The dimension of the simulated area	800×600
Radio Range (meters)	250
Routing Protocol	AODV
Simulation time (seconds)	100
Transport Layer	TCP, UDP
Traffic type	FTP, CBR
Packet size (bytes)	1000
Number of traffic connections	10
Nodes Speed (m/s)	Random

Ns-2 does not scale well for sensor networks. This is in part due to its object-oriented design. While this is beneficial in terms of extensibility and organisation, it hinders performance in environments with large numbers of nodes. Components within a single cognitive radio, showing reasoning and learning engines that manipulate the SDR's operating state on-path adversaries are by far the most capable. They can both observe and transmit data in real-time. This gives them the ability to observe traffic and spoof, inject, remove, and alter it. Protection against denial-of-service (DoS) attacks is difficult, as the adversary can degrade the link such that communication between valid parties is impossible. To protect against non-DoS attacks, a combination of mutual authentication, data integrity protection, and data encryption can be used. Most security-related protocols design for the worst-case scenario, the on-path adversary. Table 1 represents the following simulation parameters to make the scenario of routing protocols. The NS instructions can define the network's topology structure and the nodes' motion model, configure the service source and the receiver, etc.

IV. Results Analysis

The overall performance of the previous scheme, attacks and proposed IDS is mentioned in table 5.2. The proposed prevention scheme provides better results and also gives better performance in CRN. The number of packets sending, receiving and loss and other metrics like PDF, NRL and throughput attacks are counted up to the end of simulation time. The better data receiving improves utilisation of the available spectrum. The attacker presence in the network also enhances the network's load, affecting the data receiving and affecting the spectrum availability. The result of the proposed scheme is measured through the following performance metrics. The proposed scenario is based on the results of ACO with IDS in CRWSN. The proposed scenario results are compared with the existing scheme and will be finding that the proposed performance is better. There are following different performance metrics have been considered to make the comparative study of protocols through simulation.

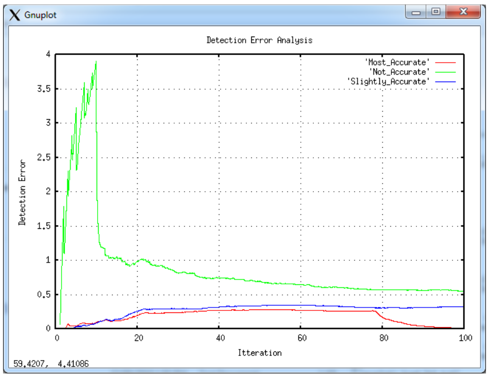

Figure2. Detection Error Analysis

(1) Detection Error Analysis

The Detection error has minimised the possibility of detection of the attacker. The secondary user is also some time attacker. These users are un-licensed, and if the spectrum having a free range of frequencies is allocating by spectrum holes to SUs. The primary users are not creating the problem, but due to SUs. The PUs is not facing the problem of sending data to the receiver through licensed. In this graph, the performance of attacker detection is based on finding the location of the attacker. The performance value of detection error is degraded that showing better performance. The performance of proposed Trust-based communication in CRN is more. The least value of detection accuracy provides a higher probability of attacker detection in CRN.

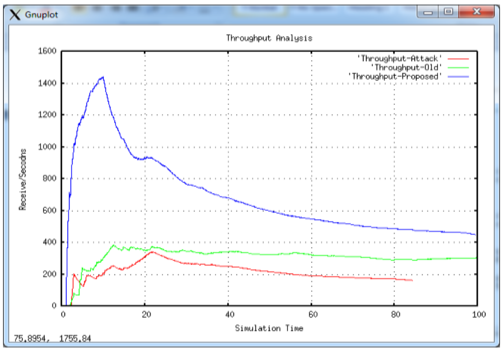

Figure3. Throughput Performance Analysis

(2) Throughput Performance Analysis

The performance of data packets is evaluated through also *throughput* Performance Analysis. The SUs is communicated to the receiver. The primary user's performance is also well collected by you to secure communication between PUs and SUs. The proposed Trust-based scheme's performance reduces the throughput compared to the previous trust scheme in CRN. The performance of the proposed trust provides the 1400pks/sec throughput performance. Compared to the previous scheme, the proposed trust performance provides 50% better performance, only possible by working on frequency bands of spectrum. The low or high rates of frequency are reaches to destination properly in CRN.

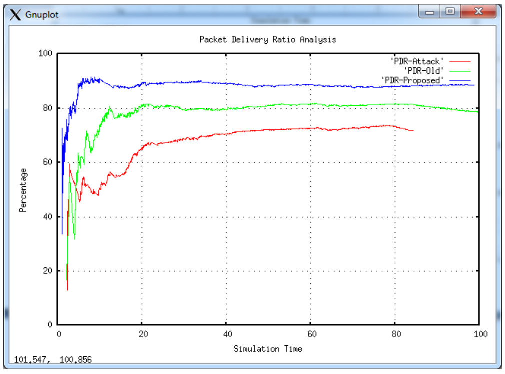

Figure4. PDR Performance Analysis

(3) PDR Performance Analysis

The successful data receiving in any network is showing the possibility of better performance. In this graph, packets receiving percentage is evaluated in the case of packet flooding or DoS attack or without trust, in the presence of an existing trust-based scheme and proposed security scheme. The proposed security scheme's performance shows better data receiving in-network because the packet receiving percentage is also high. The proposed security scheme is very reliable to check the data packets forwarding in each hop value. If the variable's value is not satisfied, then the attacker existence is confirmed in the cognitive ad hoc network, and the performance is degrading. After applying the proposed scheme again, performance is improved in the network.

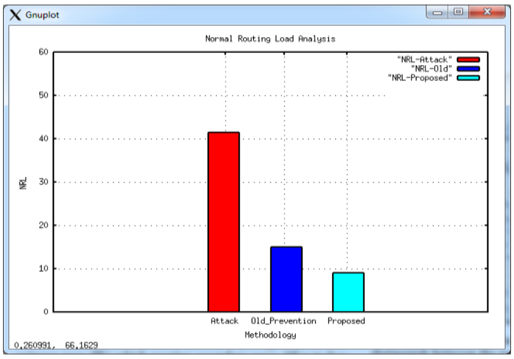

Figure5. Routing Overhead Analysis

(4) Routing Overhead Analysis

The Normal Routing Load (NRL) is a load of forwarding the connection establishment packets in the network. The fraction of these routing packets is evaluated from the number of data packets received at the destination. In this graph, the overhead quantity of packets in the presence of without-trust or packet flooding DoS attack is more. Still, after applying a Trust-based scheme, the performance is again improved, and routing packets are minimised. The proposed security scheme's overhead performance is almost equivalent, but its routing performance is better. The packets receiving percentage is more, and also the trust values of successful receiving is higher in the proposed security scheme.

V. Conclusion

The information exchange through the available spectrum in between different nodes is possible through multihop CRN. In CRN, the available spectrum's communication and control in different nodes and other devices are possible. For communication between the devices, the proper spectrum availability is necessary, and this spectrum availability. Security is the major concern in any network, and this factor is also very necessary for secure communication. The number of unlicensed used uses the spectrum because CRN security is affected, and the attacker has used the information of licensed users. The proposed ACO routing with trust-based IDS is improving the data receiving that enhances the throughput performance. The numbers of sensor nodes are also sending and receiving data in the network. This dissertation proposed the security scheme with Ant Colony Optimization (ACO) against DoS attack to secure licensed and unlicensed users communication. All devices are exchange information, and this information is also possible to consume by Packet dropping attacker. The reliability of the network is checked through ACO and identified malicious functioning. The overhead in the network is controlled, and the increases the detection accuracy. This attacker is very active and harmful to network data.

The proposed IDS scheme with IDS is proving the secure routing in between sender to destination. The proposed IDS checks the reliability of data receiving in each hop count. According to the rule, if data received is affected, and the hop count value is not incremented according to function, the nodes are expected to be the attacker. The IDS is checked the reliability by detected the attacker with the amount of packet loss in CRN. The existing Trust-based scheme's performance also provides security, and the proposed IDS performance may be better than the existing scheme. The attacker presence in-network is always harmful for communication between sender and receiver. The spectrum allocation is not a though task for providing the bandwidth for licensed users in the network. The spectrum allocation is first for primary users, and then if the spectrum is available, allocate to secondary users. In future, we work on the spectrum allocation technique to reduce the spectrum holes in the network. If the number of the hole are created more, then change the allocation technique.

References

[1] Jennifer Yick, Biswanath Mukherjee, Dipak Ghosal, "Wireless sensor network survey", Computer Networks, Elsevier, pp. 2292–2330, 2008.

[2] A. Vincy, V.Uma Devi, "Maximizing Lifetime of Nodes in Wireless Ad Hoc Sensor Network by Preventing Vampire Attack", International Journal of Innovative Research in Science, Engineering and Technology, Volume 3, Special Issue 3, March 2014.

[3] S. Haykin; "Cognitive Radio: Brain – empowered wireless communications," *IEEE Journals on Selected Areas of Communications*, Vol.23, No.2, pp.201-220, February 2005.

[4] I.F.Akyildiz, W.Y.Lee, M. C. Vuran, S.Mohanty, "Next generation/dynamic spectrum access/cognitive radio wireless networks: A Survey," Computer Networks, 50, pp.2127-2159, 2006.

[5] Federal Commissions Commission, "Spectrum Policy Task Force," ET Docket No.02-135, November 2002.

[6] Vo Nguyen Quoc Bao & et al. "Vietnam Spectrum Occupancy Measurements and Analysis for Cognitive Radio Applications"; in Proc. IEEE International conf. On Advanced Technologies for Communications(ATC), PP.135-143, August 2011.

[7] [28] Ling Hou, Angus K. Y. Wong, Alan K. H. Yeung, Steven S. O. Choy "Using Trust Management to Defend against Routing Disruption Attacks for Cognitive Radio Networks" IEEE International Conference on Consumer Electronics-China (ICCE-China), 2016.

[8] R.Ahila Priyadharshini, K.Uma Haimavathi, "Detection of Attacks and Countermeasures in Cognitive Radio Network", this full-text paper was peer-reviewed and accepted to be presented at the IEEE WiSPNET conference, 2016.

[9] Fanzi Zeng, Jie Li, Jisheng Xu, Jing Zhong, "A Trust-based Cooperative Spectrum Sensing Scheme Against SSDF Attack in CRNs", IEEE TrustCom/BigDataSE/ISPA, 2016.

[10] Lei Ding, Onur Savas, Gahng-Seop Ahn, Hongmei Deng, "Securing Cognitive Radio Networks with Distributed Trust Management against Belief Manipulation Attacks", IEEE Globecom Workshops (GC Wkshps), 2015

[11] Shameek Bhattacharjee and Mainak Chatterjee, "Trust-based channel preference in Cognitive Radio Networks under Collaborative Selfish Attacks", IEEE 25th International Symposium on Personal, Indoor and Mobile Radio Communications, 2014.

[12] R. Ahila Priyadharshini, K.Uma Haimavathi, "Detection of Attacks and Countermeasures in Cognitive Radio Network", this full-text paper was peer-reviewed and accepted be presented at the IEEE WiSPNET conference, 2016.

[13] Fanzi Zeng, Jie Li, Jisheng Xu, Jing Zhong, "A Trust-based Cooperative Spectrum Sensing Scheme Against SSDF Attack in CRNs", IEEE TrustCom/BigDataSE/ISPA, 2016.

[14] Lei Ding, Onur Savas, Gahng-Seop Ahn, Hongmei Deng, "Securing Cognitive Radio Networks with Distributed Trust Management against Belief Manipulation Attacks", IEEE Globecom Workshops (GC Wkshps), 2015

[15] Shameek Bhattacharjee and Mainak Chatterjee, "Trust-based Channel Preference in Cognitive Radio Networks under Collaborative Selfish Attacks", IEEE 25th International Symposium on Personal, Indoor and Mobile Radio Communications, 2014.

[16] Ahmed Alahmadi, Mai Abdelhakim, Jian Ren, and Tongtong 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, May 2014.

[17] Linyuan Zhang, Guoru Ding Qihui Wu, Fei Song, "Defending against Byzantine Attack in Cooperative Spectrum Sensing: Defense Reference and Performance Analysis", Received June 9, 2016, accepted July 15, 2016, date of publication August 8, 2016, date of current version August 26, 2016.

[18] Wassim Fassi Fihri, Youness Arjoune, Hassan El Ghazi, Naima Kaabouch, Badr Abou El Majd "A Particle Swarm Optimization Based Algorithm for Primary User Emulation attack detection" 978-1-5386-4649-6/18/$31.00 ©2018 IEEE.

[19] Kefan Xiao, Student Member, IEEE, Shiwen Mao, Senior Member, IEEE, and Jitendra K. Tugnait "MAQ: A Multiple Model Predictive Congestion Control Scheme for Cognitive Radio Networks" IEEE Transactions on Wireless Communications TWC.2017.2669322, IEEE.

[20] Jingbo Zhang, Jianyu Yang, Yiying Zhang and Shufang Zhang "A Dynamic Spectrum Allocation Algorithm for a Maritime Cognitive Radio Communication System Based on a Queuing Model" MDPI Information 2017, 8, 119; doi:10.3390/info8040119.