Detection of Wormhole attack in IOT based RPL protocol using Deep Learning Approach

V Chandra Sekhar Reddy[1], Dr. K. Ramesh Reddy[2]
[1]Research Scholar, [2]Asst. Professor
[1]Dept. Of Computer Science and Engineering,Rayalasema University, Kurnool-518007, A.P, India,
[2]Dept. Of Computer Science, Vikrama Simhapuri University, Nellore – 524320, A.P, India,

Abstract- Internet of Things faced biggest threats form cyber attacks and attackers who are external or internal. In resource constrained environment network layer attacks cause huge loss of information and disruption in IOT network. Among all those security attacks, routing protocol attacks cause huge information loss and these are hard to defend because of low power lossynature of network. One such attack on RPL protocol is Wormhole attack.In this paper we address differernt modes of wormhole attack which is applicable on RPL and proposed deep learning based wormhole attack detection approach on RPL protocol. The proposed method has been implemented using Contaki Cooja, PCAP, Wireshark and Python. The experimental results shows that proposed work performs well with respect to throughput, PDR and End to End Delay.

Key Words- IOT, RPL, Deep Learning, Wormhole

I. INTRODUCTION

Internet of things [1] is basically " Inteconnection of objects or things able to connet and exchange data". It is usually abbreviated as IOT. In simple manner the things which are connets and collect data and communicated over Internet. To improve quality of our lives, IOT offers various applications in different environments. These applications will generate enormous amount of data. One of the key upshots of this rising field is the creation of an unprecedented amount of data, its storage, ownership, security, expiry and its routing to a desired destination for generating some intelligence out of it that can be further used to build a smart environment. Routing is an important factor influencing interconnection between devices and performance of information exchange. The routing protocol and its quality in implementation improves the performance of the the Low Power and Lossy Network (LLN). The routing [2] issues become more and more challenging for low-power and lossy radio-links, multi-hop mesh topologies, the battery supplied nodes and frequently changed network topologies. To provide routing for Low power Lossy Networks IETF introduced RPL which is termed as Routing Protocol for Low power Lossy Networks. Routing is the basic process of the overall IPv6 network for IoT. The Routing Protocol for Low Power and Lossy Networks (RPL) [3] will make the IoT into reality. RPL offers Routing State Propagation, Spatial diversity and Expressive link and node metrics. But RPL has some security issues and also goes through some of the attacks and the one of them is Wormhole attack. Wormhole attack, is produced by at least two of the malicious nodes communicating directly with each other at different frequency than in the network which they are. When one of the malicious node gets packet, it sends directly to other without transiting it through the normal path. In this paper we are proposing a secure RPL [5] to identify the wormhole nodes of all categories, which are of caused by Protocol deviations, High power transmission, Encapsulation and Packet relay. For that, we use graph based deep learning training algorithm and testing algorithm to find suspected wormhole nodes. After finding suspected wormhole nodes we use analysis algorithm which can able to detect the exact wormhole nodes in the network. The rest of the paper is organized as follows section gives the details of literature, section-3 describes proposed work, section-4 describes the experimental setup and results finally section-5 concludes the work.

II. LITERATURE SURVEY

Prachi Shukla [1] "ML-IDS: A Machine Learning Approach to Detect Wormhole Attacks in Internet of Things" ,machine learning based centralized IDS are proposed for RPL networks in IoT: unsupervised K-means based IDS (KM-IDS), supervised decision tree based IDS (DTIDS) and a two-stage Hybrid-IDS that combines K-means and decision tree approaches. The K-means approach achieves 70-93% detection rate for varying sizes of random IoT networks. Decision tree based IDS achieves 71-80% detection rate and the hybrid approach attains 71-75% detection rate for the same network sizes. Although the hybrid IDS obtains lower detection rate, it is more accurate than the other two approaches. The hybrid approach eliminates the false positives significantly, while the other two IDS suffer from a higher number of false positives.

Felisberto Semedo et.al [2] "Vulnerability Assessment of Objective Function of RPL Protocol for Internet of Things" This paper aims to investigate the vulnerability assessment of RPL protocol. For this, we focus on the rank attack manipulation and two popular Objectve Functions(OF): Objective Function Zero (OF0) and the Minimum Rank with Hysteresis Objective Function (MRHOF) and also revealed that the rank manipulation attack is directly influenced by the efficiency of the selected OF (e.g. OF0 and MRHOF).

Dragos, Kartal et.al [3] "Deep Learning for Detection of Routing Attacks in the Internet of Things" The biggest issue in this area is the lack of datasets and the quality of available data. Our attack datasets are produced by simulation, using real sensor code and RPL protocol implementation of Contiki-

RPL. The IRAD datasets include up to 64.2 million values, which is a realistic scale for a real life IoT system. Additionally, we constructed deep neural network models trained with the IRAD datasets with high accuracy, precision and recall rates. We have obtained performance figures up to 99%, based on the F1-Score and AUC test score."

PericlePerazzo [4] "Implementation of a Wormhole Attack against a RPL Network: Challenges and Effects" The contribution of this paper is two-fold. First, present an implementation of a wormhole capable of attacking an IEEE 802.15.4-based WSAN, and also a technique to increase its impact (proxy acker technique). We test the realized wormhole against a real WSAN, measuring its impact with respect to various parameters. As a second contribution, we discuss the various countermeasures proposed by the literature, and test the feasibility of one of them in practice. We conclude that the most convenient way to counteract a wormhole attack in a WSAN may be to avoid subsequent attacks, i.e., traffic eavesdropping and selective packet dropping.

Ruchi Mehta [5] "Trust based mechanism for Securing IoT Routing Protocol RPL against Wormhole &Grayhole Attacks" As the IoT devices are provided with fewer resources the security mechanism should be less resource hungry and simple so that it will require low computational and memory power. The traditional cryptographic methods are inoperable for defence against various routing attack [6] as they require high computational, memory and battery power. Hence a Lightweight Trust mechanism is proposed for securing RPL against wormhole and grayhole attacks. Simulation graphs and results evaluate the effectiveness of Trust based mechanism in terms of performance metrics throughput and packet loss rate. Thus this mechanism is able to detect as well as separationof the malicious nodes providing an energy friendly security solution for IoT.

Muhammad Saad Ahsan [7]"Wormhole Attack Detection in Routing Protocol for Low Power Lossy Networks" presented a scheme which uses two techniques in combined form to counter the attack in network. Both of these techniques acts as a backup to each other in case if any anomaly hits the network more over the detection rate is also improved if this scheme is applied in mentioned network scenarios. Keeping in consideration of constrained environment in low power lossy networks this system can sustain in such conditions with minimum resource utilization and giving the best outcome in tackling malicious activities throughout the network.

Faraz et.al "Merkle Tree- based [8] [17] wormhole attack avoidance mechanism in low power and lossy network based networks" This paper constructed a wormhole attack that has the potential of devastating the network by forcing the traffic around specialized routes. The paper begins with a general introduction and motivation behind constructing the scenario as a result of increasing LLN application. Then some related work in the area with emphasis on wormhole attack is mentioned with storing mode. A wormhole attack is constructed with a small proposed security scheme providing resilience and robustness against such kind of attacks. In the end, the paper concludes with some of the shortcomings and future directions of adding more features in the algorithm.

Prachi Shukla "ML-IDS: A Machine Learning Approach to DetectWormhole [18][19] Attacks in Internet of Things [20] [21]" discuss about three kinds of centralized machine learning approaches to detect wormhole nodes in IDS.

III. PROPOSED METHOD

Deep Learning for Secure IOT protocols:

We propose an extremely accessible deep-learning based wormhole attack detection method for realistic IoT scenario over RPL routing protocol. We obtained a high degree of training accuracy. In this study, we have focused on specific IoTrouting attacks called wormhole attack. Here we discuss various methods of launching wormhole attack.

Methods to Launch Wormhole Attack:

There are number of ways wormhole attack can be generated [20].

I.) Encapsulation System: [9] In this strategy the genuine node send route ask for RREQ to the network. The malicious node recognizes the RREQ parcels and passages them to another malicious node present inside the network. After the bundle is gotten second malicious node communicate the demand to its neighbours and neighbours distinguish this is most brief way having less bounce count through passage and disregard the RREQ send by genuine node which is multiple jumps. This strategy keeps the nodes to recognize the first way send by authentic node.

II.) Out of Band Channel [10]: This technique is hard to produce since it utilizes specific equipment. In this assault great, low inertness, single jump remote connection is made between nodes having high data transfer capacity by utilizing directional radio wires or utilizing wired medium to make interface. Because of this long out of band channel the pernicious nodes miss controls the nodes as wrong neighbours.

III.) High Power transmission [11]: This method creates the assault utilizing high power transmission. This assault can likewise be propelled by just parcels with high power when contrasted with different nodes present in the network. At the point when malicious node distinguishes the RREQ parcel it communicates it over the network and different nodes hear the high transmission they rebroadcast back to malicious node. Utilizing along these lines attacker node makes the way between nodes even without the assistance of other attacker nodes.

IV.) Packet Relay: Packet transfer [12] is another sort of strategy utilized by Wormhole to assault the nodes. In this strategy Wormhole makes private connection wired or remote between two inaccessible nodes which are not in scope of each other but rather they are at the scope of malevolent nodes. The assailant nodes show the injured individual nodes as they are neighbours of each other begins replaying packet between them by passage and control traffic between far off nodes through along these lines they can likewise control the traffic between the passage. This assault can be propelled by one to numerous malicious nodes.

V.) Protocol Deviations Wormhole assault can likewise be propelled by utilizing protocol deviation technique. In this strategy to lessen or restrain the MAC layer crash genuine nodes venture back for a snapshot of time before sending the RREQ [13][15] through network yet the malignant node don't back off and reliably communicate the RREQ messages to nodes. By doing as such assailant nodes RREQ will arrive first at the nodes by appearing as their neighbours.

Existing mechanisms are not able to address all modes of wormhole intrusion previously. In our proposed mechanism we are need to address all these kinds of wormholes intrusions in subsequent section.

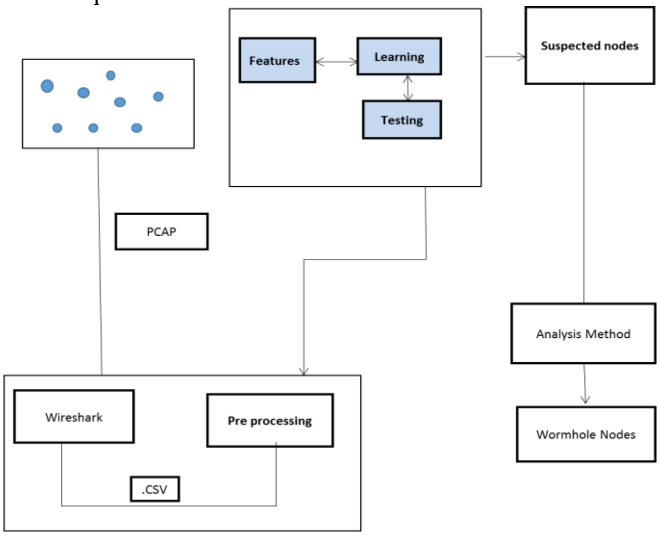

Fig.1: Architecture for wormhole detection

The Deep Learning [14] based wormhole attack detection framework is a centralized methodology, where the frame work uses training records to learn the safe distance between any two neighbouring nodes means ranks of the nodes.

After learning, the frame work can detect the suspected nodes which may be malicious.To identify suspected nodes it creates a decision tree during the learning phase, which is then used to decide if any two nodes can be made neighbours or are victims of attack.

After testing the mechanism it can able to figure out the suspected malicious nodes. These are given as inputs as detection methodology. It can analyse the suspected nodes and able to identify the wormhole nodes.

Training algorithm gets inputs from the network data which was created using Cooja simulator. The data was obtained from Cooja. There it has to be tested by testing algorithm, if the training algorithm shows error greater than a threshold again training will be applied.

Training Algorithm

```
1. Input: n nodes P1,P2, .....,Pn and consistent training data.
2. Create adjacency matrix, M of size nxn
    a. for i = 1 to n do
    b. for j = i to n do
        i. A[i][j].dist = dist(Pi,Pj )
        ii. if(i=j) M[i][j].connected=true
        iii. else M[i][j].connected=false
        iv. M[j][i] = M[i][j]
    c. end for
    d. end for
3. distance = 0
4. for each unique tuple (Pi, Pj, true) in training data do
    a. M[i][j]. connected = true
    b. M[j][i]. connected = true
    c. distance += M[i][j].dist
5. end for
6. threshold = mean (distance)
7. end
```

Testing Algorithm:

```
1. Input: test data of n nodes Q1,Q2,.Qn
2. Create adjacency matrix, U of size nxn
3. Initialize U following Steps 2.a to 2.d from training algorithm
4. suspected node Detected = 0
5. for i = 1 to n do
6. for j= i+1 to n do
    a. if(U[i][j] greater than threshold)
    b. suspect node Detected++
7. end for
8. end for
```

Traffic Threshold: It is measured based on the number of packets transmitted over the network to number of packets travelled via the suspected nodes in a particular period of time. If it is more than 25%, they should be considered as suspected.

RTT Threshold: Round Trip Time is the time taken by a data packet to travel from source to destination vice versa. RTT threshold is the mean time of network RTT. If it is varies more than 20%,they should need to be suspected.

Detection Algorithm:

```
1. Algorithm for Attacker node analysis:
2. {
3. Input: suspected attack nodes
4. Output: wormhole nodes
5. //Verify all suspected node recent RREQ communications
6. If(RTT> Threshold) && (Traffic > Threshold)
7. {
8. Add to wormhole list
9. }
10. Else
11. {
12. Recertify
13. }
```

The detection algorithm spots all the wormhole nodes in the network, by verifying all suspected nodes which are obtained from the Deep learning mechanisms. After detecting all wormhole nodes, the IDs of wormhole nodes are propagate in the network by base node. Those nodes are eliminated from the routing.

IV. EXPERIMENTAL SETUP

In experimental setup we use 16 GB RAM and 1 TB HDD and UBUNTU 16.04 LTE machine. Here we use PCAP packet formats which are capturing packets from network using Wireshark, the data which has been obtained from the network is given back to the Deep Learning using Python and TensorFlow SDK.

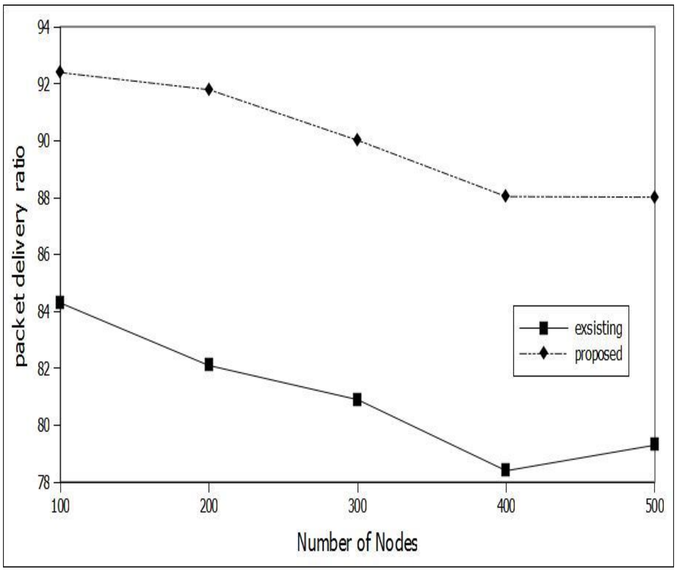

Fig.2: Packet Delivery Ratio

Fig-2 shows the comparative performance of exiting work of ML-RPL and proposed method. Existing work is based on machine learning based approach, generally ML approaches takes more time in training and goes for high error values than compared to DL method. Due to DL based strategy error rate decrease it give chance of improvement in fiddling wormhole nodes in the network. Fig-2 clearly shows that PDR is increased in proposed method than compared to the existing method.

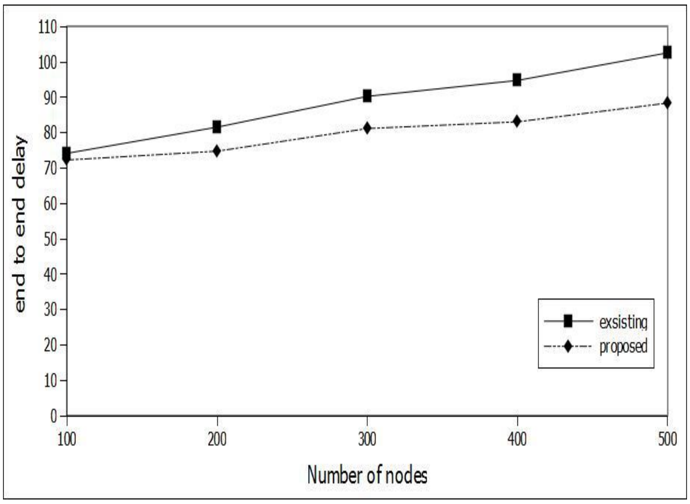

Fig.3: End to End Delay

Fig-3 shows the comparative performance end to end delay happened in exiting work of ML-RPL and proposed method. Existing work is based on machine learning based approach, generally ML approaches takes more time in training and goes for high error values than compared to DL method. Due to DL based strategy error rate decrease it give chance of improvement in trivial wormhole nodes in the network. Fig-2 clearly shows that delay isdecreased in proposed method than compared to the existing method.

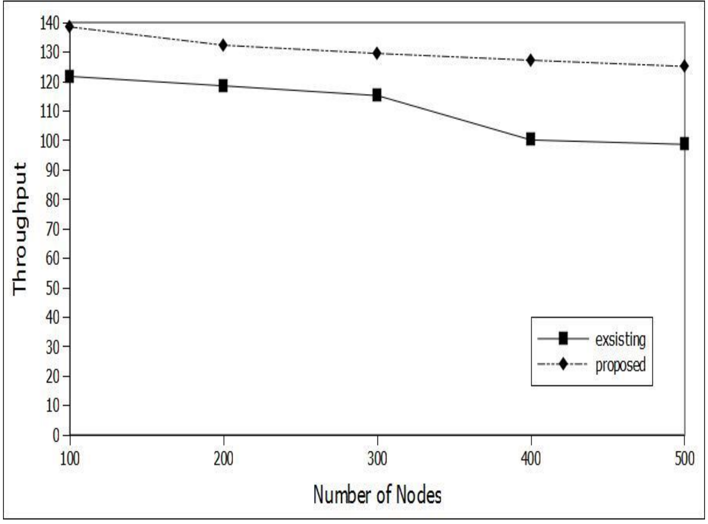

Fig.4: Throughput

Fig-4 shows the comparative performance of throughput in exiting work of ML-RPL and proposed method. Existing work is based on machine learning based approach, generally ML approaches takes more time in training and goes for high error values than compared to DL method. Due to DL based strategy, error rate decreases and it give chance of improvement in finding wormhole nodes in the network. Fig-4 clearly shows that Throughput is increased in proposed method than compared to the existing method.

V. CONCLUSION

In this paper, we addressed differernt modes of wormhole attack which is applicable on RPLand proposed Deep Learning based wormhole attack detection approach on RPL protocol.Proposed approach successfully addresses all kinds of wormhole nodes in LLN. It initially gets training from the deep learning training algorithm which gets inputs from the network file(.CSV). Afterwords it test with the inputs and we made comparision with the existing method of ML-IDS. Existing method using ML algorithm but ML alorithms have more error rate but fast adoptable, finally it is used for worm holes detection. The detected wormhole nodes are analysed for conformation of wormholes and then these nodes are removed from the network. Deep Learning based approach is slow to adaptable but highly accurate. The proposed method has been implemented using Contaki Cooja, PCAP, Wireshark and Python. The experimental results shows that better Throughput, PDR and End to End Delay when compared to the existing method.

VI. REFERENCES

[1]. Shukla, Prachi. "ML-IDS: A machine learning approach to detect wormhole attacks in Internet of Things." Intelligent Systems Conference (IntelliSys),2017. IEEE, 2017.

[2]. X. Li, R. Lu, X. Liang, and X. Shen, “Smart community: An Internet of Things application,” IEEE Commun.Magazine, vol. 49, no. 11, pp. 68–75, Nov. 2011.

[3]. Z. Sheng, S. Yang, Y. Yu, and A. Vasilakos, “A survey on the IETF protocol suite for the Internet of Things:Standards, challenges, and opportunities,” IEEE Wireless Commun., vol. 20, no. 6, pp. 91–98, Dec. 2013.

[4]. X. Liu, M. Zhao, S. Li, F. Zhang, and W. Trappe, “A security framework for the Internet of Things in the futureInternet architecture,” Future Internet, vol. 9, no. 3, pp. 1–28, Jun. 2017.

[5]. I. Andrea, C. Chrysostomou, and G. Hadjichristofi, “Internet of Things: Security vulnerabilities and challenges,”in Proc. IEEE Symposium on Computers and Commun, pp. 180–187, Larnaca, Cyprus, Feb. 2015.

[6]. R. Roman, J. Zhou, and J. Lopez, “On the features and challenges of security and privacy in distributed Internetof Things,” Computer Networks, vol. 57, no. 10, pp. 2266–2279, Jul. 2013.

[7]. S. Chen, H. Xu, D. Liu, and B. Hu, “A vision of IoT: Applications, challenges, and opportunities with chinaperspective,” IEEE Internet of Things Journal, vol. 1, no. 4, pp. 349–359, Jul. 2014.

[8]. J. Zhou, Z. Cao, X. Dong, and A. V. Vasilakos, “Security and privacy for cloud-based IoT: Challenges,” IEEECommun. Magazine, vol. 55, no. 1, pp. 26–33, Jan. 2017.

[9]. L. Xiao, Y. Li, G. Han, G. Liu, and W. Zhuang, “PHY-layer spoofing detection with reinforcement learning inwireless networks,” IEEE Trans. Vehicular Technology, vol. 65, no. 12, pp. 10037–10047, Dec. 2016.

[10]. M. Abu Alsheikh, S. Lin, D. Niyato, and H. P. Tan, “Machine learning in wireless sensor networks: Algorithms,strategies, and applications,” IEEE Commun. Surveys and Tutorials, vol. 16, no. 4, pp. 1996–2018, Apr. 2014.

[11]. L. Xiao, C. Xie, T. Chen, and H. Dai, “A mobile offloading game against smart attacks,” IEEE Access, vol. 4,pp. 2281–2291, May 2016.

[12]. L. Xiao, Y. Li, X. Huang, and X. J. Du, “Cloud-based malware detection game for mobile devices with offloading,”IEEE Trans. Mobile Computing, vol. 16, no. 10, pp. 2742–2750, Oct. 2017.

[13]. M. Ozay, I. Esnaola, F. T. YarmanVural, S. R. Kulkarni, and H. V. Poor, “Machine learning methods for attackdetection in the smart grid,” IEEE Trans. Neural Networks and Learning Systems, vol. 27, no. 8, pp. 1773–1786,Mar. 2015.

[14]. J. W. Branch, C. Giannella, B. Szymanski, R. Wolff, and H. Kargupta, “In-network outlier detection in wirelesssensor networks,” Knowledge and Information Systems, vol. 34, no. 1, pp. 23–54, Jan. 2013.

[15]. F. A. Narudin, A. Feizollah, N. B. Anuar, and A. Gani, “Evaluation of machine learning classifiers for mobilemalware detection,” Soft Computing, vol. 20, no. 1, pp. 343–357, Jan. 2016.

[16]. A. L. Buczak and E. Guven, “A survey of data mining and machine learning methods for cyber security intrusiondetection,” IEEE Commun. Surveys and Tutorials, vol. 18, no. 2, pp. 1153–1176, Oct. 2015.

[17]. R. V. Kulkarni and G. K. Venayagamoorthy, “Neural network based secure media access control protocol forwireless sensor networks,” in Proc. Int’l Joint Conf. Neural Networks, pp. 3437–3444, Atlanta, GA, Jun. 2009.

[18]. Z. Tan, A. Jamdagni, X. He, P. Nanda, and R. P. Liu, “A system for Denial-of-Service attack detection basedon multivariate correlation analysis,” IEEE Trans. Parallel and Distributed Systems, vol. 25, no. 2, pp. 447–456,May 2013.

[19]. L. Xiao, Q. Yan, W. Lou, G. Chen, and Y. T. Hou, “Proximity-based security techniques for mobile users inwireless networks,” IEEE Trans. Information Forensics and Security, vol. 8, no. 12, pp. 2089–2100, Oct. 2013.

[20]. Y. Gwon, S. Dastangoo, C. Fossa, and H. Kung, “Competing mobile network game: Embracing anti-jamming andjamming strategies with reinforcement learning,” in Proc. IEEE Conf. Communication and Network Security (CNS),pp. 28–36, National Harbor, MD, Oct. 2013.

[21]. M. A. Aref, S. K. Jayaweera, and S. Machuzak, “Multi-agent reinforcement learning based cognitive antijamming,” in Proc. IEEE Wireless Communication and Networking Conf (WCNC), pp. 1–6, San Francisco, CA, Mar.2017