ISSN: 2581-3404 (Online)
International Journal of Innovative Research in Technology and Management (IJIRTM), Volume-3, Issue-3, 2019

Learning for Mitigating Attacks in Wireless Sensor Network: Survey and Discussion

Yamini Bante[1], Prof. Jitendra Mishra[2]

[1]M. Tech Scholar, Department of EC, PCST, Bhopal (India)

[2]Head & Professor, Department of EC, PCST, Bhopal (India)

[1]yaminibante@gmail.com, [2]jitendra.mishra260@gmail.com

ABSTRACT

Due to the open nature of wireless communication medium, wireless networks are susceptible to jamming attacks. Jammers interfere with the legitimate nodes by sending strong jamming signals. Legitimate nodes can successfully transmit only between the gaps of the jamming signals. It is therefore very important to detect a jamming attack as soon as it happens in order to effectively take counter measurements. This survey present the deep learning and other learning methods for the mitigating the various attacks in wireless sensor networks.

Keywords:. Wireless Sensor Network, Denial of Services, Attacks, Mitigating, Quality of Services.

INTRODUCTION

A WSN comprises of sensor devices (nodes) that sense or monitor physical and environmental conditions and send this information to each other or to a remote location through co-ordination and co-operation. WSNs have wide applications in different fields such as military and civil surveillance, e-health care systems and climate monitoring. However, with the expansion of the application requirements and fields, sensor nodes often need to be attached to the moving objects, or deployed in the hostile and remote environment, Due to their small size, hostile environment and unattended operations they are highly vulnerable to different security attacks. Limited power resources and low computational power are major constraints for WSN, so defense against security attacks and energy problem is a major concern and a lot of research has been done to overcome these problems [5].

Due to the broadcast nature of radio propagation, wireless networks are vulnerable to jamming attacks, as jammers purposefully inject replayed or faked signals into wireless media to interrupt the ongoing radio transmissions between legitimate users. With the pervasion of smart and programmable radio devices such as universal software radio peripherals (USRPs), smart jammers choose to launch multiple types of attacks, such as eavesdropping and spoofing attacks, and select the jamming power, frequency, and time against the ongoing wireless transmissions. Smart jammers can even analyze the ongoing anti-jamming transmission policy and induce the mobile devices to use a specific communication mode and then block them accordingly. Jamming attackers aim to degrade the communication efficiency of the ongoing transmission, increase power consumption of the radio nodes, and even lead to denial of services (DoS) attacks.

Traditional anti-jamming wireless communication solutions, spread spectrum techniques, such as frequency hopping and direct-sequence spread spectrum, have been used for decades to address jamming attacks in wireless networks. However, significant challenges have to be addressed in 5G systems, e.g., spread spectrum technique requires both the transmitter and the receiver to share the physical-layer secrets such as the spreading codes or frequency hopping pattern in advance. However, jammers can derive the spreading codes of the transmitter by eavesdropping the public control channels and compromising cognitive radio nodes in large-scale dynamic wireless network [3].

The wireless medium's inherent openness makes it susceptible to adversarial attacks. A wireless system's vulnerabilities can be broadly classified based on an adversary's capabilities; for example, a passive adversary might eavesdrop on the wireless channel and try to infer information, an active adversary might transmit energy to jam reliable data transmission, and a higher layer active adversary might threaten a link's integrity and confidentiality [2].

Due to the broadcast nature of wireless communications, wireless medium is susceptible to adversaries that can learn and jam the ongoing transmissions. There are various ways of launching wireless jamming attacks such as random and sensing-based jamming, and their impact can be detrimental to network performance. Different countermeasures against jamming have been developed using conventional methods such as frequency-hopping and transmit power control. However, the vulnerabilities of cognitive radio systems using machine learning and potential mitigation techniques are not well understood yet. With the increasing use of machine learning in wireless communication systems, it is critical to understand the security implications of machine learning for cognitive radios [1].

The detection of jamming attacks requires not only to detect the radio interference that caused network performance degradation, but also to distinguish the observed degradation caused by a jammer from those caused by network congestion or weak signals. Many jamming detectors use test statistics derived from network measurements such as packet delivery ratio, packet error rate, and received signal strength, etc. for jamming attack detection, however the detection logic is often simplistic as only summary information is used and the detection threshold is often preset at the initial setup phase. The limitation of existing work is not being able to maintain detection performance when the network dynamics increases as users join and leave the network. Dynamics in the normal operation of a network as well as the evasive techniques employed by the attacker makes fast and reliable jamming detection very challenging. Despite the large body of literature in jamming attacks, there is still unaddressed issues: mainly how to improve detection delay and accuracy [7].

As the lack of security and privacy properties raise concerns in deploying such smart appliances throughout our homes, it is crucial to monitor the events occurring in today's home networks and analyzing them for signs of potential security risks associated with these devices. Once a security attack is identified, it is also necessary to consider a proper defence mechanism to stop the adversary from having a harmful effect. One possible approach for securing the myriad smart devices within the home is to redesign and embed security agent inside them. However, such an approach would not scale, nor would be affordable. This motivates us to propose a framework that will be capable of detecting and mitigating security threats within smart home environments at network-level, whereby it does not require any amendment to their design.

The rest of this paper is organized as follows in the first section we describe an introduction of about the various types of attacks in wireless sensor networks and techniques for the prevention. In section II we discuss about the key jammer capabilities in network, In section III we discuss about the rich literature survey, finally in section IV we conclude the about our paper and discuss the future scope.

II KEY JAMMER CAPABILITIES

Our taxonomy primarily delineates jammers by capabilities that define their fundamental behavior. A jammer can have one or more of the following major capabilities: We chose these four capabilities based on our survey of jammer models that emphasized complex forms of jamming. For example, a learning (or cognitive) jammer might not represent the majority of what's found in current day operations, but it's a topic of interest in recent research and likely to become more prevalent over the next decade. We discuss correlation in the time domain specifically, because it's implicit that, to be successful, a jammer's signal must have some correlation in the frequency domain with the victim's desired signal (that is, the jammer must at least be aware of the spectrum the victim uses to perform jamming).

- Time Correlation,
- Protocol Awareness,
- Ability to Learn
- Signal Spoofing.

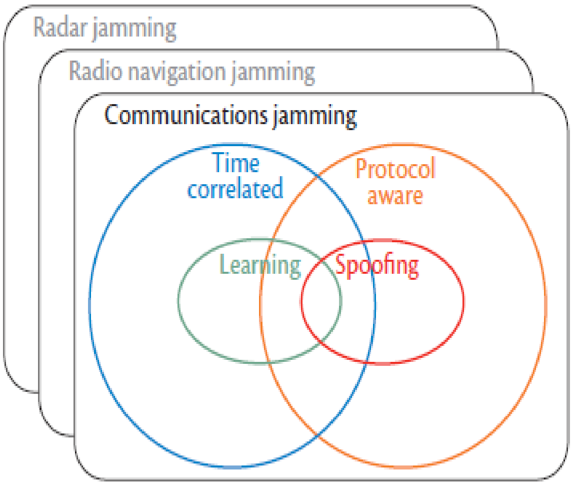

Figure 1: Shows how the jammer capabilities interrelate [2].

III RELATED WORK

[1] They applied adversarial machine learning to design an intelligent jamming attack on wireless communications and presented a defense scheme against this attack. They considered a wireless communication scenario with one transmitter, one receiver, one jammer, and some background traffic. The transmitter senses the channel and applies a pre-trained machine learning algorithm to detect idle channel instances for transmission. The jammer does not have any knowledge of transmitter's algorithm. Instead, it senses the channel, detects the transmission feedback (if available), applies a deep learning algorithm to predict a successful transmission, and jams such a transmission. In addition, the jammer uses the deep learning classification scores to control its transmit power subject to an average power constraint. [2] As communications systems' sophistication increases, complex jamming will likely become a bigger threat in public safety, military, and other mission-critical domains. Their jammer taxonomy organizes jammer classes by the information they possess and their capacity to act on that information. This new view of jammers emerges naturally from present-day wireless technology's extensive reliance on software-driven behavior. Understanding the key capabilities that distinguish major classes of jamming, as well as the multidimensional parameter space, can aid in the correct application of anti jam and detection strategies. Further research includes the design of radar jamming and radio navigation jamming taxonomies. [4] In this article they analyze the vulnerability of LTE to jamming, spoofing, and sniffing by looking at each of the physical channels and signals of LTE. Using barrage jamming as a baseline, they have shown that more effective jamming methods can be realized by exploiting the specific protocol features of LTE. They derive metrics related to the efficiency and complexity of each method to compare them, and conclude that the PSS, PUCCH, PCFICH, and PBCH are the weakest subsystems and should therefore be addressed first. [5] In this survey they classified DoS attack on Wireless Sensor Network and discussed their countermeasure techniques according to the type of attack. Other surveys related to classification of attacks on WSN are available but they do not include such a number of DoS attacks on WSN along with their countermeasures. Some characteristics of WSN which make them vulnerable to DoS attacks are

also discussed in this paper. Network layer is the most vulnerable layer for DoS attacks due to defenseless routing algorithms. Research based solutions has also been discussed but there is still a need for more work in this domain which can results in novel solution against variety of DoS attacks. [6] They identify a class of Fake VIP attacks as false declarations of a high class to acquire undue service quality, with an awareness that a defense via object signature detection is costly and so invoked reluctantly. They show that, unexpectedly, such attacks can be mitigated by a double blind reputation scheme at the server side. They offer a minimum information framework for Fake VIP attacks and a stochastic analysis of a two-player Stackelberg game to find optimum attack and defense strategies, as well as to identify regions of operation where both the client and the server find the reputation scheme beneficial. [7] In this paper we developed a jamming attack detection method for wireless networks based on time series analysis. The detection algorithm is running over the network performance measurements taken over time, and it reports positive findings in real time. The approach is shown to be effective in terms of detection rate and detection delay. The false alarm rate is bounded by the controllable input parameter ϵ. In future work, they will develop a multiple-stream change point detection algorithm. Another direction for future work is accurate localization of the source of the interferer. Machine learning techniques will be used to build the training data set and predict the location of the jammer based on the received signals. [8] In this paper, they study how Q-learning can be used to learn the jammer strategy in order to proactively avoid jammed channels. The problem with Q-learning is that it needs a long training period to learn the behavior of the jammer. To address the above concern, they take advantage of the wideband spectrum sensing capabilities of the cognitive radio to speed up the learning process and they make advantage of the already learned information to minimize the number of collisions with the jammer during training. The effectiveness of this modified algorithm is evaluated by simulations in the presence of different jamming strategies and the simulation results are compared to the original Q-learning algorithm applied to the same scenarios. [9] In this work, they propose an intrusion detection and mitigation framework, called IoT-IDM, to provide a network-level protection for smart devices deployed in home environments. IoT-IDM monitors the network activities of intended smart devices within the home and investigates whether there is any suspicious or malicious activity. Once an intrusion is detected, it is also capable of blocking the intruder in accessing the victim device on the fly. The modular design of IoT-IDM gives its users the flexibility to employ customized machine learning techniques for detection based on learned signature patterns of known attacks. Software-defined networking technology and its enabling communication protocol, Open Flow, are used to realize this framework. [10] This paper proposes a reinforcement learning based approach to anti-jamming communications with wideband autonomous cognitive radios (WACRs) in a multi-agent environment. Assumed system model allows multiple WACRs to simultaneously operate over the same (wide) spectrum band. Each radio attempts to evade the transmissions of other WACRs as well as avoiding a jammer signal that sweeps across the whole spectrum band of interest. The WACR makes use of its spectrum knowledge acquisition ability to detect and identify the location (in frequency) of this sweeping jammer and the signals of other WACRs. This information and reinforcement learning is used to successfully learn a sub-band selection policy to avoid both the jammer signal as well as interference from other radios.

IV CONCLUSION AND FUTURE SCOPE

The jamming attack is one of the major threats in wireless sensor networks ,cognitive radio networks and other networks because it can lead to network degradation and even denial of service (DoS). Furthermore, the jammer doesn’t need to be a member of the network or to collect information about it to launch such attack. In this paper we discuss various techniques for the attacks in wireless sensor networks, in future we plan to implement secure mechanism from the various attacks and improve the performance of overall networks.

REFERENCES:-

[1] Tugba Erpek, Yalin E. Sagduyu , Yi Shi, "Deep Learning for Launching and Mitigating Wireless Jamming Attacks", IEEE TRANSACTIONS ON COGNITIVE COMMUNICATIONS AND NETWORKING, VOL. 5, NO. 1, MARCH 2019, pp 2-13.

[2] Marc Lichtman, Jaffrey D. Poston, SaiDhiraj Amuru, Chowdhury Shahriar, T. Charles Clancy, R. Michael Buehrer, Jeffrey H. Reed, "A Communications Jamming Taxonomy", Copublished by the IEEE Computer and Reliability Societies, IEEE 2016, pp 47-54.

[3] Xuemin (Sherman) Shen, Xiaodong Lin, Kuan Zhang, "Reinforcement Learning-Based Wireless Communications Against Jamming and Interference", Springer International Publishing AG, part of Springer Nature 2018, pp 1-6.

[4] Marc Lichtman, Roger Piqueras Jover, Mina Labib, Raghunandan Rao, Vuk Marojevic, and Jeffrey H. Reed, "LTE/LTE-A Jamming, Spoofing, and Sniffing: Threat Assessment and Mitigation", IEEE Communications Magazine, 2016, pp 54-61.

[5] Jahanzeb Shahid, Shahzad Saleem, Muhammad Nauman Qureshi, "DOS Attacks on WSN and Their Classifications With Countermeasures - A Survey", NUST Journal of Engineering Sciences, 2016, pp 50-59.

[6] Jerzy Konorski, "Fake VIP Attacks and Their Mitigation via Double-Blind Reputation", 2016, pp 1-8.

[7] Maggie Cheng, Yi Ling, Wei Biao Wu, "Time Series Analysis for Jamming Attack Detection in Wireless Networks", 2017, pp 1-8.

[8] Feten Slimeni, Bart Scheers, Zied Chtourou, Vincent Le Nir, "Jamming mitigation in cognitive radio networks using a modified Q-learning algorithm", 2015, pp 1-8.

[9] Mehdi Nobakht, Vijay Sivaraman, Roksana Boreli, "A Host-based Intrusion Detection and Mitigation
Framework for Smart Home IoT using OpenFlow", 2016, pp 1-11.

[10] Mohamed A. Aref, Sudharman K. Jayaweera, Stephen Machuzak, "Multi-agent Reinforcement Learning Based Cognitive Anti-jamming", 2015, pp 1-6.

[11] Ronnie Johansson, Peter Hammar, Patrik Thoren, "On Simulation-Based Adaptive UAS Behavior During Jamming", 2016, pp 1-6.

[12] Mohsen Riahi Manesh, Naima Kaabouch, "Security Threats and Countermeasures of MAC Layer in Cognitive Radio Networks", 2-17, pp 1-40.

Yamini Bante received her Bachelor`s degree in Electronics Comunication Engineering from SIMS, Indore, M.P., in 2015. Currently she is pursuing Master of Technology Degree in Electronics & Comunication (Digital communication) from PCST, (RGPV), Bhopal, Madhya Pradesh India. Her research area include Ad-hoc Network, Wireless Sensor Network.

Mr. Jitendra Kumar Mishra he is Associate Professor and Head of the Department of Electronics and communication in PCST, Bhopal (RGPV). His received Master of Technology and Bachelor's of engineering respectively in Digital communication from BUIT, Bhopal and from RGPV, Bhopal. He has more than 11 years of teaching experience and publish 35+ papers in International journals, conferences etc. His area of Interests is Antenna & Wave Propagation, Digital Signal Processing, Ad-hoc network, Wireless Communication, Vehicular Ad-hoc network, Image Processing etc.