ISSN: 2581-3404 (Online)
International Journal of Innovative Research in Technology and Management (IJIRTM), Volume-3, Issue-6, 2019

Performance Analysis for Attacks in Wireless Sensor Network

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)

ABSTRACT

Wireless networks are extremely vulnerable to a plethora of security threats, including eavesdropping, jamming, and spoofing, to name a few. Recently, a number of next-generation cross-layer attacks have been unveiled, which leverage small changes on one network layer to stealthily and significantly compromise another target layer. In this paper we present the comparative experimental study for the various attack in wireless network using the previous method and the proposed method, the efficiency of networks are measured in the terms of throughput and success ratio parameter, our simulated results shows improvements in results than the previous method.

Keywords: Wireless Sensor Network, Attacks, Mitigating, Throughput, Success Ratio, Quality of Services.

INTRODUCTION

Wireless transmissions are exposed to shared media. This is a nice feature that makes them pervasively available but also makes them vulnerable to physical layer attacks. Jamming attack is a type of security attack that uses radio interference to impede normal communications [7]. A jammer does not follow the MAC layer protocol as a normal wireless transmitter does. For instance, if TDMA is used by the normal nodes, a jammer can send signals often at high power to interfere the transmission during normal nodes' allocated time slots; if CSMA is used by normal nodes, a jammer can defeat the CSMA protocol by occupying the channel at arbitrary time making other nodes wait for a long time. Jamming attacks will directly cause packet drops, high packet error rates, reduced throughput, and long delay. To effectively protect wireless networks from jamming attacks, it is important that the jamming attack is timely detected. Normal nodes can then launch the mitigation techniques such as retreating from the jammed area, switching to a different radio channel, or using advanced communication technologies.

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. In this article, we focus on jamming attacks, in which attackers transmit signals interfering with victims' communications, principally those at the physical (PHY) layer, intended to cause a denial of service (DoS) and thus compromise a link's availability [2].

Due to diversity and applicability of wireless sensor network grow in different field such as battle field, medical field and many more application based on dynamic infrastructure and controlled topology. The work processing of wireless sensor network consumed more power for the processing of data and life of sensor consumed more energy. Energy consumed more during path finding and data transmission operations terms as routing. Routing is the most challenging issue and direct concern to energy in WSN comparable with ad hoc and cellular network.

The jamming attack is one of the major threats in CRNs 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. CRNs are characterized by dynamic spectrum access (DSA) and by mainly distributed architectures which make it difficult to implement effective jamming countermeasures. Therefore, some coding techniques have been developed to mitigate the effects of this attack in the transmitted signal. For example, the authors in [5] combine random linear network coding with random channel hopping sequences to overcome the jamming effect on the transmitted control packets. Their proposed algorithm is called jamming evasive network coding neighbor discovery algorithm (JENNA).

Another class of anti-jamming approaches is based on the CR ability of changing its operating frequency while maintaining continuous and proper operation. This ability can be exploited to overcome jamming attacks since the CR can hop to avoid jammed channels. In this context, markov decision process (MDP) has been widely exploited as a stochastic tool to model the CR decision making problem in jamming scenarios with fixed strategy, i.e. assuming that the jammer preserves the same tactic. The CR may use reinforcement learning (RL) algorithms to solve the MDP by learning how to take the best decisions to keep its communication un-jammed.

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 TYPES OF WSNS

Presently many WSNs are deployed on land, underground and underwater. They face different challenges and constraints depending on their environment.

Terrestrial: consists in a large number (hundreds to thousands) of low cost nodes deployed on land in a given area, usually in an ad-hoc manner (e.g., nodes dropped from an airplane). In terrestrial WSNs [2], sensor nodes must be able to effectively communicate data back to the base station in a dense environment. Since battery power is limited and usually non-rechargeable, terrestrial sensor nodes can be equipped with a secondary power source such as solar cells. Energy can be conserved with multi-hop optimal routing, short transmission range, in-network data aggregation, and using low duty-cycle operations. Common applications of terrestrial WSNs are environmental sensing and monitoring, industrial monitoring, and surface explorations.

Underground: consists of a number of sensor nodes deployed in caves or mines or underground to monitor underground conditions. In order to relay information from the underground sensor nodes to the base station, additional sink nodes are located above ground. They are more expensive than terrestrial WSNs as they require appropriate equipments to ensure reliable communication through soil, rocks, and water. Wireless communication is a challenge in such environment due to high attenuation and signal loss. Moreover, it is difficult to recharge or replace the battery of nodes buried underground making it important to design energy efficient communication protocol for prolonged lifetime. Underground WSNs are used in many applications such as agriculture monitoring, landscape management, underground monitoring of soil, water or mineral, and military border monitoring.

Underwater: consists of sensors deployed underwater, for example, into the ocean environment. Such nodes being expensive, only a few nodes are deployed and autonomous underwater vehicles are used to explore or gather data from them. Underwater wireless communication uses acoustic waves that presents various challenges such as limited bandwidth, long propagation delay, high latency, and signal fading problems. These nodes must be able to self-configure and adapt to extreme conditions of ocean environment. Nodes are equipped with a limited battery which cannot be replaced or recharged requiring energy efficient underwater communication and networking techniques. Applications of underwater WSNs include pollution monitoring, under-sea surveillance and exploration, disaster prevention and monitoring, seismic monitoring, equipment monitoring, and underwater robotics.

Multi-media WSN: consists of low cost sensor nodes equipped with cameras and microphones, deployed in a pre-planned manner to guarantee coverage. Multi-media sensor devices are capable of storing, processing, and retrieving multimedia data such as video, audio, and images. They must cope with various challenges such as high bandwidth demand, high energy consumption, quality of service (QoS) provisioning, data processing and compressing techniques, and cross-layer design. It is required to develop transmission techniques that support high bandwidth and low energy consumption in order to deliver multi-media content such as a video stream. Though QoS provisioning is difficult in multi-media WSNs due to variable link capacity and delay, a certain level of QoS must be achieved for reliable content delivery. Multi-media WSNs enhance the existing WSN applications such as tracking and monitoring.

Mobile WSN: consists of mobile sensor nodes that can move around and interact with the physical environment [12]. Mobile nodes can re-position and organize themselves in the network in addition to be able to sense, compute, and communicate. A dynamic routing algorithm must, thus, be employed unlike fixed routing in static WSN. Mobile WSNs face various challenges such as deployment, mobility management, localization with mobility, navigation and control of mobile nodes, maintaining adequate sensing coverage, minimizing energy consumption in locomotion, maintaining network connectivity, and data distribution. Primary examples of mobile WSN applications are monitoring (environment, habitat, underwater), military surveillance, target tracking, search and rescue. A higher degree of coverage and connectivity can be achieved with mobile sensor nodes compared to static nodes.

III PROPOSED WORK

To reduce the computational overhead of real-time classification, recent studies apply ML (e.g., decision tree, support vector machine (SVM), and artificial neural network (ANN) to classify a power system’s stability and safety with respect to certain contingencies, based on measured physical conditions of the system. A trained SVM classifies the power system’s stability by using phasor measurement unit data. The SVM must be retrained if the system condition has changed significantly. The ANN model takes the system loading as input to rank the severity of the contingency in question, in terms of a composite performance index.

Detection statistics used in the literature range from packet-level network measurements such as Packet Delivery Ratio and Bad Packet Ratio (BPR), throughput, success ratio, to network wide statistics such as Energy Consumption Amount (ECA) and channel utilization, physical layer statistics such as signal collision ratio, received signal strength (RSS) have also been used for jamming detection. An anti-jamming scheme is developed to protect the reactive alarm systems. It monitors the received signal strength during the reception of bits in sensor networks, and is able to differentiate packet errors due to jamming attacks from errors caused by weak signals.

In this paper we present the comparative experimental study for the attack in wireless sensor network using some standard performance parameters such as the success ratio and throughput. Here we calculate the channel efficiency using some attack types and compare their efficiency for the existing and proposed work.

Name of Attack	METHOD	Throughput	Success Ratio
Relay Attack	DNN	0.646	32.38
	Proposed	0.703	39.20

Table 1: Show that the Comparative values of throughput and success ratio for relay attack using DNN and Proposed Method.

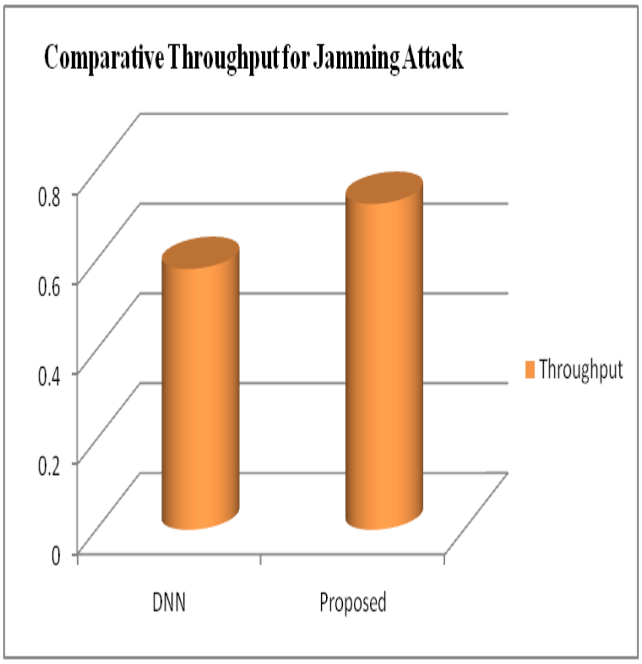

Fig 1: Comparative performance for the throghuput in the jamming attack using the existing and proposed method.

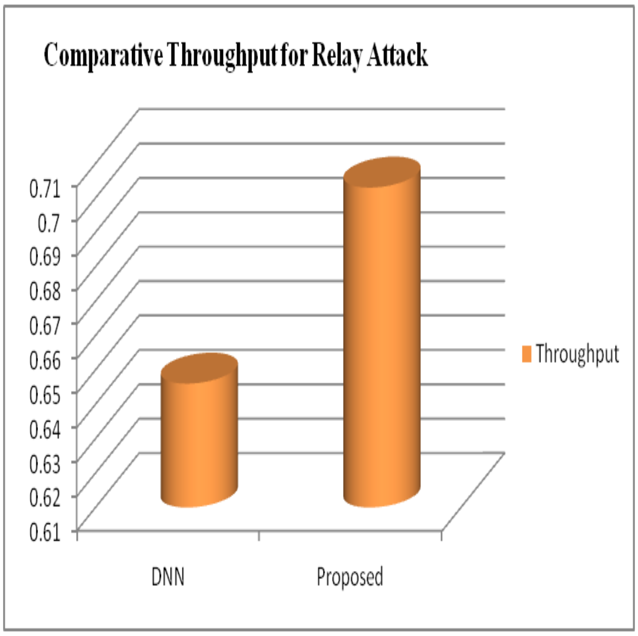

Fig 2: Comparative performance for the throghuput in the relay attack using the existing and proposed method.

IV CONCLUSION AND FUTURE SCOPE

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. In this paper we applied classification approach to design an intelligent jamming attack on wireless communications and presented a defense scheme against this attack. 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. The developed solution can be extended for multiple transmitters and receivers, while interference from non-intended transmitters is sensed as the additional interference term by receivers.

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.

[13] G. Ateniese et al., “Hacking smart machines with smarter ones: How to extract meaningful data from machine learning classifiers,” Int. J. Security Netw., vol. 10, no. 3, pp. 137–150, 2015.

[14] F. Tramer, F. Zhang, A. Juels, M. Reiter, and T. Ristenpart, “Stealing machine learning models

via prediction APIs," in Proc. USENIX Security, 2016, pp. 601–618.

[15] M. Fredrikson, S. Jha, and T. Ristenpart, "Model inversion attacks that exploit confidence information and basic countermeasures," in Proc. ACM SIGSAC Conf. Comput. Commun. Security, 2015, pp. 1–12.

[16] Y. Shi, Y. E. Sagduyu, and A. Grushin, "How to steal a machine learning classifier with deep learning," in Proc. IEEE Symp. Technol. Homeland Security (HST), May 2017, pp. 1–5.

[17] Y. Shi and Y. E. Sagduyu, "Evasion and causative attacks with adversarial deep learning," in Proc. IEEE Mil. Commun. Conf. (MILCOM), 2017, pp. 243–248.

[18] I. Goodfellow et al., "Generative adversarial nets," in Proc. Adv. Neural Inf. Process. Syst., 2014, pp. 1–9.

[19] B. Biggio et al., "Evasion attacks against machine learning at test time," in Proc. ECML PKDD, 2013, pp. 387–402.

[20] A. Kurakin, I. Goodfellow, and S. Bengio, "Adversarial examples in the physical world," arXiv preprint arXiv:1607.02533, 2016.

[21] N. Papernot et al., "The limitations of deep learning in adversarial settings," in Proc. IEEE Eur. Symp. Security Privacy, 2016, pp. 1–16.

[22] L. Pi, Z. Lu, Y. Sagduyu, and S. Chen, "Defending active learning against adversarial inputs in automated document classification," in Proc. IEEE Glob. Conf. Signal Inf. Process. (GlobalSIP), 2016, pp. 257–261.

[23] Y. Shi, Y. E. Sagduyu, K. Davaslioglu, and J. Li, "Active deep learning attacks under strict rate limitations for online API calls," in Proc. IEEE Symp. Technol. Homeland Security (HST), 2018, pp. 1–6.

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 12 years of teaching experience and publish 45+ 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.