NSEMX_Conf2021_005

A Brief Review of Proposed Models for Jamming Detection in Wireless Sensor Network

Grace AUDU, Michael DAVID and Abraham U. USMAN
grace.audu@st.futminna.edu.ng

ABSTRACT
Wireless sensor network (WSN) consists of a group of sensor nodes usually deployed in a hostile environment used for sensing, processing, transmitting and receiving data from the area. Sensor Nodes are characterized by limited memory, limited power and short transmission range, which exposes them to attacks like jamming. In this paper, we review different jamming attacks in WSN. We also review several proposed methods for detecting jamming. We have provided a comparative conclusion to aid researchers studying this field.

KEYWORDS: *Jamming, Jamming detection, Denial of Service Attacks, Wireless Sensor Network.*

I. INTRODUCTION

Wireless sensor network (WSN) consists of a group of sensor nodes usually deployed in a hostile environment used for sensing, processing, transmitting and receiving data where they are deployed to a base station (Osanaiye et al 2015).

WSNs have different applications. They find application were collecting data remotely is needed. These areas include military, environmental monitoring, health, controlling traffic, agriculture, and industries (Kumari et al, 2015). WSN have constrained power, storage, bandwidth and short communication distance. These constraints in addition to the open and shared wireless transmission medium makes sensor nodes prone to security attacks. Denial of Service (DoS) is one of the common attacks in WSN. These attacks occur in physical, link and network layer. At the physical layer, the most common DoS attack is jamming. Jamming occurs when a rogue node intentionally transmits a high-range signal to disrupt the normal transmission of information between legitimate nodes by reducing the signal to noise ratio. This attack affects the functionality of the network as it truncates the delivery of desired packets to the intended receiver hence impeding network capabilities (Bhushan & Sahoo ,2018). The major goal of jamming is to affect the long-term availability of sensor nodes. The jammer depletes the resources of sensor nodes by transmitting electromagnetic signals at high power towards the communication channel of the sensor nodes thereby prohibiting data from reaching its destination (Upadhyaya et al.2019).

Jamming can be perpetrated by listening passively to the communication channel in order to transmit at the same frequency as the legitimate sensor node. Jammers have high energy efficiency and are not easily detected (Pelechrinis et al., 2011)

Jamming attack may be mitigated by increasing the robustness of the legitimate signal or by implementing frequency hopping. Due to the limited resources of WSN applying those solution is difficult. WSN, hence the need for detecting jamming. In this paper we describe types of jamming attacks, metrics used for detecting jamming and review the different proposed methods to detect jamming.

WIRELESS SENSOR NETWORK ARCHITECTURE

The WSN architecture is made up of five layers (Akyildiz & Vuran, 2010). These includes:

Physical layer: is responsible for transmission, modulation and receiving techniques.

Link layer: ensures bit are transferred without errors and it controls access to the channel.
Network layer: routes the data supplied by the transport layer.
Transport layer: This layer is needed when the network is going to be access by external networks; it helps to maintain the flow of data to prevent congestion.
Application Layer: provides software for numerous applications depending on the sensing task.
Jamming attack occurs at the physical and link layer.

II. JAMMING ATTACKS IN WIRELESS SENSOR NETWORK

Constant Jammer: constant jammer transmits random bits continuously on the channel to disrupt communication on the channel. This could lead to depletion of the legitimate node's energy. The constant jammer does not follow any

Medium Access Control (MAC) layer procedure before continually transmitting series of radio signals to interrupt legitimate signal transmission in the network. This jammer continuously transmits random bits that occupy the transmission path of the network, hence disrupting legitimate data transmissions initiated by nodes (Misra et al., 2010).

Deceptive jammer: A deceptive jammer continuously injects legitimate bit sequences into the communication channel without gaps in between. The sensor nodes believe that a legitimate transmission is going on, hence they remain in the listening state. Detecting deceptive jammers is difficult since they are aware of the network protocol (Misra et al., 2010).

Random Jammer: Random jammers moves from active mode to sleep mode and vice versa to save energy. During the active state, the attacker jams the network for a specific time then it turns off its transmitter and goes to sleep mode. The attacking node begins to transmit the malicious signal again, after a while then goes back to sleep mode; the sequence continues (Misra et al., 2010).

Reactive Jammer: Reactive jammers constantly sense the channel to listen for when packets are being transmitted. Once they detect a packet transmission on the channel, they begin to transmit malicious signals to disrupt the legitimate signal. This type of jammer reduces the rate of power dissipation and are hard to detect (Misra et al., 2010).

a. PROPOSED METHODS FOR DETECTING JAMMING IN WIRELESS SENSOR NETWORK

Research on jamming detection in WSNs has been ongoing for a while. A lot of proposed methods for detecting jamming involves either the use of dedicated tools or algorithms installed on the sensor nodes. Most of these proposed methods make use of information gathered a priori about some metrics of the node when it is jammed or normal. Some of these metrics include received signal strength(RSS), packet delivery ratio(PDR), packet inter arrival time(PIAT), packet sent ratio, bad packet ratio(BPR) signal to noise ratio(SNR), consumed energy, clear channel assessment.

Osanaiye et al. (2015) proposed an approach for detecting jamming attacks that uses the cluster-based topology. The EMWA algorithm used for detecting jamming is only installed on the cluster head and base station. The base station detects jamming in the member nodes while base stations detect jamming in the cluster head. In order to minimize overhead they used only metric packet IAT to detect jamming. In order to detect changes in traffic flow during situations of both non-jamming and jamming, a trace-driven experiment using EWMA was carried out. Results obtained from their work shows that their proposed model can detect jamming attack efficiently with little or no overhead in WSN from the 20th jammed packet.

Bikalpa et al. (2019) in their work proposed a node-centric approach. To reduce overhead in nodes in this detection method, network information for detecting jamming are passively gathered by anchor nodes placed in the network. Using random forest algorithm, the information gathered a prior about the network is used differentiate when the network is jammed or not. Their work achieved 89.7% and 98.6% accuracy using RSSI from five anchor nodes for real and simulated data respectively.

In their work, Youness et al., (2020) used four metrics BDR, PDR, RSS and clear channel to identify the presence of jamming attack. They generated a large set of data in a real environment simulation and gathered measurements of these parameters when the network was jammed and when it was normal. They then used these data sets to train, validate, and test the machine learning algorithms. The simulation results showed that the proposed detects jamming attacks with an accuracy of 97.5%.

Ganeshkumar et al. (2016) proposed a framework that also uses cluster-based topology for jamming detection. They used statistical tests to compute the detection metrics normal threshold. The cluster head verifies if a packet received is from a legitimate node. The framework validates whether the node is a legitimate node by using the cluster head code. Lastly, the auditing algorithm on the CH estimates the metrics (PDR, RSSI) and makes decision about "jammed situation" or "non-jammed situation. Their proposed framework detects jamming with an accuracy of 99.88%.

A fuzzy logic–based algorithm was proposed by Vijayakumar et al. (2018) for jamming detection in cluster-based wireless sensor networks. The detection metrics is checked by the cluster head to check for jamming. An accuracy of 99.89% was gotten from their simulation. The jamming detection metrics are checked by the cluster head at the lower level and by the base station at the higher level. There by reducing the overhead cost on the member nodes.

Mistra et al., (2010) proposed the use of a fuzzy inference-based system for jamming at the base stations using three metrics. These metrics include received signal strength, total packets received during a period and the number of dropped packets during that period. The power received signal is measured at the base during the jamming attack to find the difference in value between the normal RSS.The total packets received during a specific period and the packet sent over the period is used at the base station to determine the packet drop per terminal (PDPT) and signal-

to-noise ratio (SNR). These metrics are then inputted to obtain the jamming index from the fuzzy inference system. The jamming index varies from 0 to 100. The system's true-detection rate is as high as 99.8%. In a Table 1, we present a summarize Comparison of Proposed Methods for Jamming detection in Wireless Sensor Network.

TABLE 1: Comparison of Proposed Methods for Detecting Jamming in Wireless Sensor Network

REFERENCE	MACHINE LEARNING OR NON-MACHINE LEARNING METHOD	ALGORITHM USED	Metrics	WSN STRUCTURE	ACCURACY
Osanaiye *et al* (2015)	Non-Machine Learning Method	EMWA	IAT	Cluster	100% >20 Jammed packets
Bikalpa *et al.* (2019)	Machine Learning method	Random forest	RSS	Flat	89.7% for real data and 98.6 for simulated data
Youness *et al*., (2020)	Machine Learning method	Random forest	BPR, PDR, RSS	Flat	97.5%.
Ganeshkumar *et al.,* (2016)	Non-Machine Learning Method	Auditing algorithm	PDR and RSSI	Cluster	99.88 %.
Vijayakumar *et al*.,(2018	Non-Machine Learning Method	Fuzzy logic–based jamming detection algorithm	PDR and RSSI	Cluster	99.89 %.
Misra *et al.,* 2010	Non-Machine Learning Method	Fuzzy logic	PDR, RSS	Cluster	99.89 %.

A fuzzy inference-based system to detect jamming attacks in the base stations using three metrics measured from each sensor node in the network was proposed by Mistra *et al*., (2010). These metrics are the total packets received during a specific period, the number of dropped packets during that period and the received signal strength (RSS). The base station computes the power received during the jamming attack to find any difference in value between the current RSS and the normal RSS. These values are used by the base station to compute the packet drop per terminal (PDPT) and signal-to-noise ratio (SNR) which is further used as inputs for the fuzzy inference system to obtain the jamming index The jamming index varies from 0 to 100 and is used to determine the intensity of the jamming attack, which can range between a situation of 'no jamming' to absolute jamming'. The system with its high robustness, ability to grade nodes with jamming indices, and its true-detection rate as high as 99.8%, is worthy of consideration for information warfare defense purposes. In a Table 1, we present a summarize Comparison of Proposed Methods for Detecting Jamming in Wireless Sensor Network.

III. CONCLUSION

In this paper, we presented a brief survey about jamming detection in wireless sensor networks. Different jamming attacks occurring in WSNs are described in detail. Different metrics used for detecting jamming was described. The different types of jamming are described, and detection techniques of jamming has been is pointed out. Our future work will focus on improving jamming detection.

ACKNOWLEDGEMENTS

The authors sincerely thank the reviewers for proofreading the article and providing constructive feedback.

REFERENCES

O.A. Osanaiye, S.A. Attahiru, & Gerhard P. Hancke (2018). A Statistical Approach to Detect Jamming Attacks in Wireless Sensor Network. *Sensors*, 1691(18) 1-15

Saru Kumari, Muhammad Khurram Khan, and Mohammed Atiquzzaman. (2015). User authentication schemes for wireless sensor networks. *Ad Hoc Netw*. 27, C (April 2015), 159–194.DOI:https://doi.org/10.1016/j.adhoc.2014.11.018

B. Upadhyaya, S. Sun and B. Sikdar (2019). Machine Learning-based Jamming Detection in Wireless IoT Networks. *2019 IEEE VTS Asia Pacific Wireless Communications Symposium (APWCS),*1-5.

Bhushan, B. & Sahoo, G. (2018). Recent Advances in Attacks, Technical Challenges, Vulnerabilities and Their Countermeasures in Wireless Sensor Networks. *Wireless PersCommun* 98, 2037–2077. https://doi.org/10.1007/s11277-017-4962-0

Y. Arjoune, F. Salahdine, S.Islam, E. Ghribi & N. Kaabouch(2020). A Novel Jamming Attacks Detection Approach Based on Machine Learning for Wireless Communication. *The 34th International Conference on Information Networking (ICOIN 2020)* ffhal02509430f, 1-5.

Ganeshkumar, P. , Vijayakumar, K. , & Anandaraj, M. (2016). A novel jammer detection framework for cluster-based wireless sensor networks. *J Wireless Com Network, 2016 (1*). doi: 10.1186/s13638-016-0528-1

K. P. Vijayakumar,P. Ganeshkumar, M. Anandaraj, K. Selvaraj & P. Sivakumar(2018). Fuzzy logic–based jamming detection algorithm for cluster based wireless sensor network. Int Journal of Communication Systems 31(10), 1-21.

Misra, S., Singh, R. & Mohan, S.V.R (2010). Information Warfare-Worthy Jamming Attack Detection Mechanism for Wireless Sensor Networks Using a Fuzzy Inference System. *Sensors* 2010, *10*, 3444-3479. https://doi.org/10.3390/s100403444

Osanaiye, O., Choo, K.K.R. & Dlodlo, M. (2016). Distributed denial of service (DDoS) resilience in cloud: Review and conceptual cloud DDoS mitigation framework. J. Netw. Comput. Appl. 2016, 67, 147–165. Journal of Network and Computer Applications 67, 147-165 https://doi.org/10.1016/j.jnca.2016.01.001

Pelechrinis, K.; Iliofotou, M.; Krishnamurthy, S.V. (2011). Denial of service attacks in wireless networks: The case of jammers. *IEEE Commun. Surv. Tutor. 2011*, 13, 245–257.

Ian F. Akyildiz & Mehmet Can Vuran(2010). WSN Architecture and Protocol Stack. *Wireless Sensor Networks* 10-15