International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 4 Issue: 4
ISSN: 2454-4248
546 – 549

Jamming Threat To Wireless Sensor Network

Rohini Sharma
Computer science department
A.I.J.H.M. College
Rohtak, India
rohinisharmaohlan@gmail.com

***Abstract*—**Assurance of security in wireless sensor networks is a difficult task as the sensor networks suffers from limited operating and energy resources. There are several types of denial of service attacks in these networks, but jamming attack is the most severe one. It disturbed the normal transmission of information by reducing the signal to noise ratio. With the help of jammer, radio signals are transmitted towards victim node or the channel. In this work, we analyze different types of jamming attacks which affects the sensor networks. A survey on avoiding jamming attack has been conducted by analyzing signal strength, and packet delivery ratio etc.

Keywords*-Wireless Sensor Networks;Secruity Attacks;Jamming*

*****

I. INTRODUCTION

Wireless sensor network (WSN) is a versatile area of research [1]. It is constituted of small node which are scattered all over the area in a dense mode. These nodes collect information and give it to the sink node as shown in figure 1. These are used in many real life applications [2-3] and the data carried by them is very important. But these have some limitations too like lack of energy conservation [2-4] and energy holes [4]. A lot of research has been carried out in these problematic areas [8- 14].

Energy draining is not the sole problem of the WSN; it also undergoes several types of security attack [15]. The WSN can be secured using different cryptographic techniques [16]. The WSN has a broadcast nature in transmission and it makes it more suspects able to the attacks. Jamming attack works at the physical layer by making interference with the radio signals [17]. The jammer is an antagonistic node which tries to abrupt the normal working of the WSN by throwing radio interference attacks. On the other side WSN tries to defend itself against the jamming attack. It is very easy for a node to jam the network just by simple listening to the open wireless medium and transmitting at the same frequency of the WSN. It can be handled at physical layer by using DSSS (Direct Sequence Spread Spectrum) or FHSS (Frequency Hopping Spread Spectrum). Figure 2 shows an example of the jamming attack [18].

II. MODELS OF JAMMING ATTACK

A jammer can adopt a variety of techniques to attack a wireless medium [19]. Figure 3 shows different types of jamming attacks.

A. Active Jammer

It tries to block the channel in any type of condition.

B. Constant Jammer

It regularly releases radio signals and it is generally executed using a waveform generator.

C. Deceptive Jammer

The deceptive jammer continuously inserts regular packets to the medium deprived of any gap between successive packet broadcasts, instead of directing out random bits. As a consequence, a usual communicator will be misled into trusting there is a genuine packet and be fooled to remain in the receive state.

D. Random Jammer

In spite of endlessly transferring out a radio signal, random jammer swings between inactive and jamming. Specially, after jamming for some units of time, it turns off its radio, and enters into a “sleeping” mode. It will restart jamming after being inactive for some time, and this time can be either random or fixed values.

E. Reactive Jammer

The above specified jammers constantly keep the channel in a busy state; therefore they can be easily detected, however, a reactive jammer does not jam a medium, when it is ideal. But while someone is transmitting, it also starts transmitting radio signals.

F. Shot noise-based intelligen Jammer[20]

Shot noise-based intelligent jammers are protocol-sensitive jammers that just use forward error correction scheme operated at physical and MAC layers. Particular continuous pulse intrusive genuine packet can entirely drop it if it is able to use the FEC scheme operated used in the packet.

 ISSN: 2454-4248
546 – 549

III. IDENTIFICATION OF JAMMING METRICS

The jamming attack takes place either by preventing source node from transmitting the data or by averting the intended receiver from receiving the data. Let M and N are two valid nodes while Z is a jammer node. Following metrics are known as jamming metrics:

A. *Packet Send Ratio (PSR)*

It is the ratio of packets that are effectively sent out by a valid traffic source equated to the amount of packets it intends to send out at the MAC layer. Let, node M has a packet to send for node N. In the MAC protocol utilized by Mica2 node, the medium must be perceived as being in an inactive state for at least certain random period of time before M can transmit a packet. A radio interference attack may affect the channel to be detected as busy, instigating M's transmission to be delayed. If a large number of packets are queued in the MAC layer, the newly entered packets will be plunged. It is also probable that a packet halts in the MAC layer for a extended period of time, ensuing in a timeout and packets being rejected. If, M wants to transmit x number of packets but only y are being sent, then PSR is given by:

$$PSR = y/x \quad (1)$$

B. *Packet Delivery Ratio (PDR)*

The ratio of packets that are effectively conveyed to a destination equated to the number of packets that have transmitted by the M. Even after the packet is transmitted by M, N may not be able to interpret it accurately, owing to the interference introduced by Z. It is known as an unsuccessful delivery. The PDR may be computed at the receiver N by computing the ratio of the number of packets that pass the error correction check with respect to the number of packets received by N. PDR may also be calculated at the sender M by having N send back an acknowledge packet. In either case, if no packets are arriving, the PDR is stated to be 0.

C. *Carrier sensing time*

It is the time a station has to wait for the medium to get inoperative to begin its transmission.

IV. DETECTION OF JAMMING ATTACKS

Many WSN are vulnerable to jamming attacks. To ensure the obtainability of sensor communications, the jamming detection procedures must be established that are easy to scale, spread and have low false positives results. It is a necessary step to construct a secure and robust wireless sensor networks, and it is also inspiring because jammers can employ different jamming attack prototypes. Figure 4 show the process of jamming detection.

Wood et al. [19] have developed a threshold value of jamming signal. This value is called utility metric which help in detecting jamming attack in the WSN. If the value of the metric is below the threshold value, the WSN is under jamming attack otherwise communication can take place. Features that can affect utility metric are

- Recurrent incapability to access wireless medium
- Corrupt framing
- Checksum malfunctions
- Illegitimate values for addresses or other fields
- Protocol violations
- Extreme arriving signal ratio
- Low signal-to-noise ratio
- Repetitive collisions
- Duration of attack.

V. CLASSIFICATION OF JAMMING ATTACKS

There are a few commonly used metrics characterizing the jamming attacks:

- Least recognition likelihood
- Quiet against detectors
- Entirely denial of service like constant jammers
- Protocol alert so that they are less likely to notice
- Authentication of users
- Power against error detecting codes
- Power at physical layer to beat channel coding techniques
- Power saving is to get main jamming efficiency with least energy used

TABLE I. *THE CAPABILITY OF DEALING WITH DIVERSE ATTACK MODELS[17]*

	Signal Strength		**Carrier Sensing Time**	**PDR**
	Average	**High**		
Constant Jammer	X	√	√	√
Deceptive jammer	X	√	√	√
Random jammer	X	X	X	√
Reactive jammer	X	X	X	√

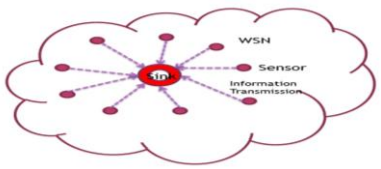

Figure 1. Example of a WSN topology.

VI. CONCLUSION

In this work, a survey on issues related to jamming type Denial-of-Service attack in sensor networks by investigative both the attack and defend sides of the issue. Different jamming attack models have been illustrated that might be expended to disturb sensor networks and metrics that can be exploited as volumes of jamming attacks.

 ISSN: 2454-4248
546 – 549

REFERENCES

[1] S. Hooda, K. Bhatia, and R. Sharma, "Nodes Deployment Strategies for Sensor Networks: An Investigation," IRJET, vol. 03, pp. 2395–0056, April 2016.

[2] Sanju, K. Bhatia and R. Sharma, "An Analytical Survey on Face Recognition Systems", Int. Jour. Ind. Electronic Elec. Engg., in pree.

[3] P. Sharma, R. Sachdeva and R.. Sharma, "Location Based Tracking: The Need of the Hour", International Journal of Engineering and Science Invention, in press.

[4] A. Rana, K. Bhatia and R. Sharma, "ETM: A survey on Energy, Thermal and Mobility Efficient Routing Protocols for Wireless Body Area Sensor Network", IRJCAS, vol. 7,pp.4–11, May 2017.

[5] A. Rana, K. Bhatia and R. Sharma, "IIEPDR: Improved Information and Energy Proficient Data Relaying Routing Protocol for Wireless Body Area Networks", IRJSET, vol. 8,pp.26–38,june 2017.

[6] R. Sharma and D.K. Lobiyal, "Energy based proficiency analysis of ad-hoc routing protocols in wireless sensor networks", Proc. IEEE ICACEA, March 2015, pp.882-886 , doi:10.1109/ICACEA.2015.7164829.

[7] R. Sharma, "Energy Holes Avoiding Techniques in Sensor Networks: A survey", Int. Jor. of Engg. Trends and Techn., vol. 20, no. 4, pp. 204-208, Feb 2015, arXiv:1510.05363.

[8] R. Sharma and D.K. Lobiyal, "Region Based Energy Balanced Inter-cluster communication Protocol for Sensor networks", proc. NCCCIP , May 2015, pp. 184-195.

[9] R. Sharma and D.K. Lobiyal, "Dual Transmission Power and Ant Colony Optimization Based Lifespan Maximization Protocol for Sensor Networks", Int. Jour. of Business Data Comm. and Net.,vol. 11, Issue1, pp. 1-14, 2015, doi: 10.4018/IJBDCN.2015010101.

[10] S. Hooda, K. Bhatia, and R. Sharma," Enrichment of Life span of Sensor Networks through BCO and Gateway Node" , International Journal of Research in Information Technology, Vol 4, issue 5, pp. 9-20, 2016.

[11] P. chhillar, K Bhatia and Rohini sharma, "Swarm Intelligence Inspired Energy Efficient Routing Protocols for Sensor Networks: An Investigation", Int. Res. Jour of Engg. and Techn., vol. 3 issue 5, pp. 623-630, May 2016.

[12] P. chhillar, K Bhatia and Rohini sharma, "Spiral Based Sink Mobility Method Aiming Lengthening of Lifetime of Sensor Networks", Int. Res. Jour. of Engg and Techn., vol. 3 issue 5, pp. 631-637, May 2016.

[13] R. Sharma and D.K. Lobiyal," Multi-Gateway-Based Energy Holes Avoidance Routing Protocol for WSN", Informatics, vol. 3,iIssue 2, no. 5, pp. 1-26, April 2016, doi:doi.org/10.3390/informatics3020005.

[14] R Sharma and D.K. Lobiyal, Proficiency Analysis of AODV, DSR and TORA Ad-hoc Routing Protocols for Energy Holes Problem in Wireless Sensor Networks, Procedia Compu. Sci., Vol. 57, pp.1057-1066, August 2015, doi: doi.org/10.1016/j.procs.2015.07.380.

[15] R. Sharma, "Security Attacks and Prevention in Wireless Sensor networks," IJETAE, in press.

[16] Sameksha, K. Bhatia and R. Sharma, "Cryptographic Techniques: In new Era", Int. Jour. of Adv. Compu. Engineering and Net., in press.

[17] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks," Proc. ACM MobiHoc, 2005, pp. 46–57.

[18]http://resources.infosecinstitute.com/wireless-attacks-unleashed/#gref

[19] A.D. Wood, J.A. Stankovic and S.H. Son, "JAM: a jammed-area mapping service for sensor networks", Real-Time Systems Symposium, Proc. RTSS 2003. 24th IEEE, Dec 2003, pp. 286-297.

[20] N. Sufyan, N. A. Saqib and M. Zia, "Detection of jamming attacks in 802.11b wireless networks", EURASIP Journ. on Wireless Comm. and Net,vol. 208, 2013.

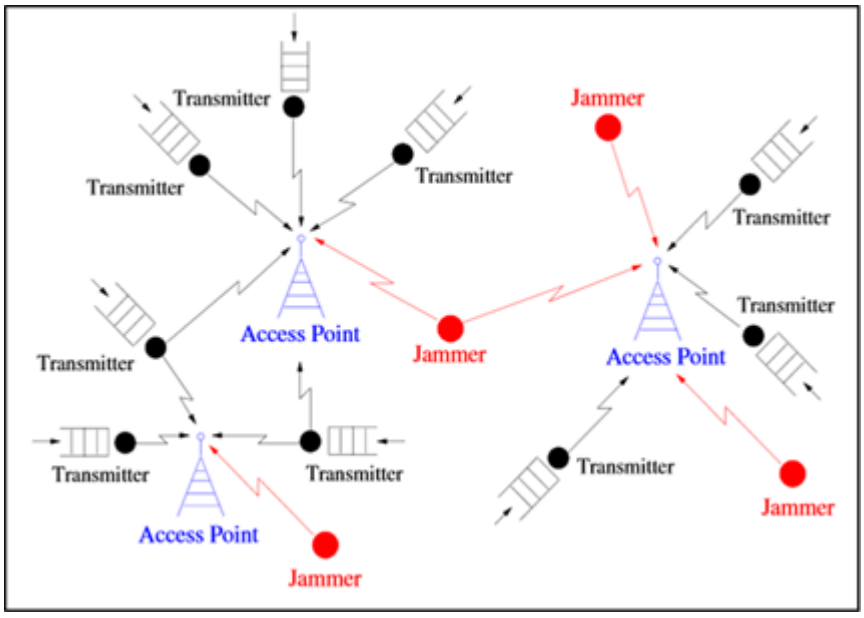

Figure 2. Example of a Jammer.

ISSN: 2454-4248
546 – 549

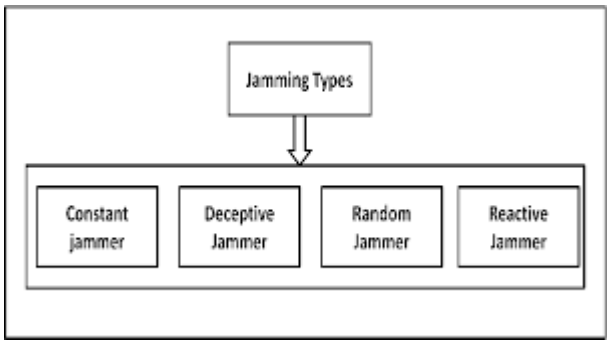

Figure 3. Types of Jamming attacks

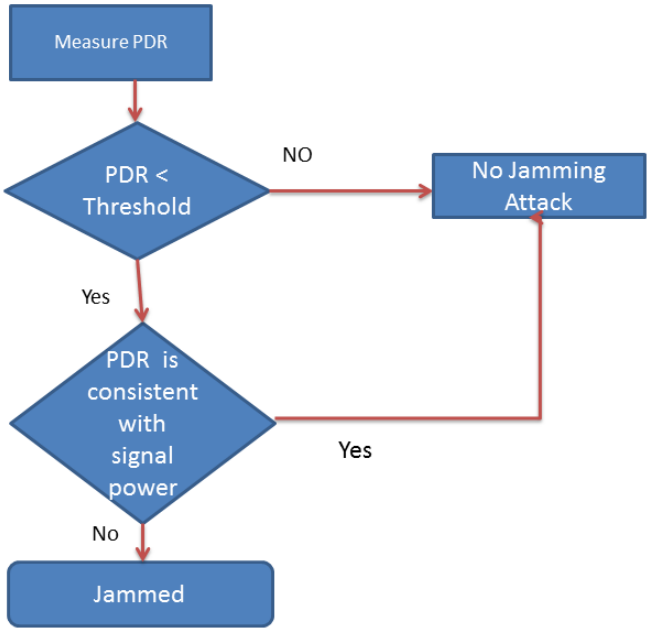

Figure 4. Jamming detection process