A Survey on Jamming Attacks in Wireless Sensor Networks

Ilavarasan S

Assistant Professor/IT, Saveetha Engineering College, Chennai-India, ilavarasan.sargunan@gmail.com

ABSTRACT*-Wireless sensor network refers to a group of spatially dispersed and dedicated sensors for monitoring and recording the physical conditions of the environment and organizing the collected data at a central location. In Wireless Sensor Networks, nodes collectively collaborate to sense the environment and inform the base station. Wireless sensor network consists of large number of low-cost, resource-constrained sensor nodes. These networks are easily prone to security attacks. There are many possible attacks on sensor network such as selective forwarding, jamming, sinkhole, wormhole, Sybil and hello flood attacks. Jamming is one of the severe types of attack which interferes with the radio frequencies used by network nodes. Jamming style Denial-of-Service attacks is the transmission of radio signals that disrupt communications by decreasing the signal to noise ratio. These attacks can easily be launched by jammer through, either bypassing MAC-layer protocols or emitting a radio signal targeted at blocking a particular channel. The jamming attack is one of the most critical security issues in wireless networks, which disseminates out sufficient adversarial signals into the radio frequencies used by normal sensor nodes, without following any legitimate protocols. Since the jammer interferes with radio reception by producing noise, it could decrease the probability of successful broadcasting in the wireless communication. The jammers do not need to explore lots of internal information of the network components, so this light weight attack is easy to launch and favoured by attackers. Furthermore, in reactive jamming attacks the jammers keep idle until being triggered by messages disseminated within their transmission ranges, thereby further reducing the jammers' operation overhead and making it hard to detect, thus this intelligent attack can be utilized by malicious users in more real-world scenarios*

Keywords- Wireless sensor network, Jamming, Denial-of-Service attacks.

INTRODUCTION

Wireless Sensor Networks (WSNs) are used in many applications which often include the monitoring and recording of sensitive information (e.g. battlefield awareness, secure area monitoring and target detection). Recently the high drop in the prices of CMOS cameras and microphones has given rise to the development of a special class of WSNs, that of Wireless Multimedia Sensor Networks (WMSNs).WMSNs allow the retrieval of video and audio streams, still images, and scalar sensor data from deployed nodes. Hence, they can be efficiently used in various security applications such as surveillance systems for monitoring of secure areas, patients, children, etc. In these applications, QoS requirements rise, since in such systems even a temporal disruption of the proper data streaming may lead to disastrous results. It is therefore evident that the critical importance of WSNs raises major security concerns. Jamming is defined as the act of intentionally directing electromagnetic energy towards a communication system to disrupt or prevent signal transmission. In the context of WSNs, jamming is the type of attack which interferes with the radio frequencies used by network nodes . In the event that an attacker uses a rather powerful jamming source, disruptions of WSNs' proper function are likely to occur. As a result, the use of countermeasures against jamming in WSN environments is of immense importance, especially taking into account that WSNs suffer from many constraints, including low computation capability, limited memory and energy resources, susceptibility to physical capture and the use of insecure wireless communication channels. Jamming attacks may be viewed as a special case of Denial of Service (DoS) attacks. Wood and Stankovic define DoS attack as "any event that diminishes or eliminates a network’s capacity to perform its expected function”. Typically, DoS prevents or inhibits the normal use or management of Communications through flooding a network with ‘useless’ information. In a jamming attack the Radio Frequency (RF) signal emitted by the jammer corresponds to the ‘useless’ information received by all sensor nodes. This signal can be white noise or any signal that resembles network traffic. The main objective of this article is to provide a general overview of the critical issue of jamming in WSNs and cover all the relevant work, providing the interested researcher pointers for open research issues in this field.

JAMMING DEFINITION, HISTORY AND TECHNIQUES

Jamming is defined as the emission of radio signals aiming at disturbing the transceivers’ operation . The main difference between jamming and radio frequency interference (RFI) is that the former is intentional and against a specific target while the latter is unintentional, as a result of nearby transmitters that transmit in the same or very close frequencies (for instance, the coexistence of multiple WSNs on the same area using the same frequency channel may result in RFI).

A. Brief History of Jamming

The first occasions of jamming attacks were recorded back in the beginning of the 20th century against military radio telegraphs. Germany and Russia were the first to engage in jamming. The jamming signal most frequently consisted of co-channel characters. The first wartime jamming activities can be traced back to the World War II , when allied ground radio operators attempted to mislead pilots by giving false instructions in their own language (an example of deceptive jamming). These operators were known by the code name ‘Raven’ which soon became ‘Crow’. The crow represents the universal sign of jamming ever since. Also during World War II the first jamming operations against radars (a new invention at that time) have been reported. Jamming of foreign radio broadcast stations has been often used during periods of tense international relations and wartime to prevent the listening of radio broadcasts from enemy countries. This type of jamming could be relative easy addressed by the stations with the change of transmitting frequency, adding of additional frequencies and by increasing transmission power.

B. Jamming Techniques

The key point in successful jamming attacks is Signal-to-Noise Ratio (SNR), SNR= Psignal/Pnoise, where P is the average power. Noise simply represents the undesirable accidental fluctuation of electromagnetic spectrum, collected by the antenna. Jamming can be considered effective if SNR< 1. Existing jamming methods are described below.

1) Spot Jamming: The most popular jamming method is the spot jamming wherein the attacker directs all its transmitting power on a single frequency that the target uses with the same modulation and enough power to override the original signal. Spot jamming is usually very powerful, but since it jams a single frequency each time it may be easily avoided by changing to another frequency.

2) Sweep Jamming: In sweep jamming a jammer’s full power shifts rapidly from one frequency to another. While this method of jamming has the advantage of being able to jam multiple frequencies in quick succession, it does not affect them all at the same time, and thus limits the effectiveness of this type of jamming. However, in a WSN environment, it is likely to cause considerable packet loss and retransmissions and, thereby, consume valuable energy resources.

3) Barrage Jamming: In barrage jamming a range of frequencies is jammed at the same time. Its main advantage is that it is able to jam multiple frequencies at once with enough power to decrease the SNR of the enemy receivers. However as the range of the jammed frequencies grows bigger the output power of the jamming is reduced proportionally.

4) Deceptive Jamming: Deceptive jamming can be applied in a single frequency or in a set of frequencies and is used when the adversary wishes not to reveal her existence. By flooding the WSN with fake data she can deceive the network’s defensive mechanisms (if any) and complete her task without leaving any traces. Deceptive jamming is a very dangerous type of attack as it cannot be easily detected and has the potential to flood the PE with useless or fake data that will mislead the WSN’ operator and occupy the available bandwidth used by legitimate nodes.

Table 1- Benchmarks table on Jamming Networks

S.no	Journal name	Problem	Technique	Solution	Merits	Demerits
1.	Jammy:a distributed and dynamic solution to selective jamming attacks in tdma wsn's	TDMA is used in wsn for pre-allocationg slots for sensor nodes.An adversary could attack a victim node by simply jamming its slots because each slot is used by the same node for a number of consecutive frames.	JAMMY,a distributed and dynamic solution for selective jamming	JAMMY changes the slot utilization at every super frame thus making it unpredictable for the adversary.	JAMMY allows multiple nodes to join the network in a limited number of superframes.	Jammy causes negligible energy overhead.
2.	Efficient jammed area mapping in wsn	Adversary emits constant high amplitude noises disrupting the communication among nodes.	Jammed area mapping protocol	(i)Solution is collaborativel-y mapping the jammed region and avoiding traffic through the jammed area. (ii)This protocol detects jamming and notifies neighbours.	The network lifetime increases while using the proposed enhanced J.A.M protocol due to reduced number of packet transmissions in mapping jammed area.	This protocol faces a broadcast storm problem inside the jammed area.
3.	Distributed secure estimation over wsn against random multichannel jamming attacks	Sensor's measurements are divided into ny components.The attacker randomly drops the channel if they are sucessfully jammed.	(i)Two level switching attack model (ii)A distributed attack model	Two level switching attack model to capture random attack strategies.Distributed attack model to achieve consensus estimation for target tracking.	One of the most efficient algorithm which reduces computational compexity.	In the presence of a smart attacker, some random or more complicated attack policies may pose major difficulties for remote estimators.

4.	A trigger identification service for defending reactive jammers in wsn	Reactive jamming causes mass destruction to legitimate sensor communication and difficulty to be disclosed and defended. Numerous attempts like receiver signal strength,packet delivery ratio were used to control jamming attack but jammer nodes could not be detected.	An application layer real time trigger identification service	First identify the set of victim nodes by investigationg coressponding links' PDR and RSS,then these victim nodes are grouped into multiple testing teams.Once the group testing schedule is made at base station it is routed to all victim nodes to identify trigger or non-trigger.	This trigger identification procedure is a lightweight service, which is prompt and reliable to various network scenarios.	Cannot be used for high speed jammers. Main issue is jammer mobility.
5.	Mitigating the effect of jamming signals in wireless adhoc and sensor networks	Probability of success and throughput per mobile nodes can be reduced significantly if the network is attacked by jamming signals.	Mpt-multi packet transmission Mpr-multi packet reception	Probability of success in presence of jamming signals can be mitigated using mpt and mpr capabilities. By using mpr,the probability that a packet will be an authorized one is increased. By using mpr,the probability that no other packet will interfere in increased.	The problem of infrastructure environment is solved by using these mpt and mpr capabilities.	The hardware and software implementaion of the combined mpt and mpr is done with high complexity due to the advancements in electronics.
6.	Geomorphic zonalisation of wsn based on prevalent jamming attacks	Divides the geographic extent of wsn under attack of jammer into different zones as per severity.Existing methods are vulnerable to information warfare as they require to communicate even under a jamming attack.	Modified Graham's scan for convex hull construction (MGSCHC), boundary trace algorithm (BTA)	Proposed method follows centralised approach where mapping is done by base station through hull tracing using pre calculated jamming indices.	One of the most energy-efficient and fastest-known mapping systems.The system has no inherent inaccuracies.	Does not map the jammed area this method just zonalises the entire area into desired number of zones.

7.	Optimal decision rule baesd ex-ante frequency hopping for jamming	A static wireless sensor network is affected by a constant, static jammer. Both the nodes in the network and the jammer are capable of switching frequencies.	Optimal group decision rule	Frequency hopping strategy uses takes into account the individual node decision and finally makes decision for the welfare of overall network.	Provides optimal frequency to get maximum throughput.	The route packet delivery ratio as well as the network packet delivery ratio are affected adversely by a significant extent.
8.	Optimal jamming attack strategies and network defense policies in wsn	The network defends itself by computing the channel access probability to minimize the jamming detection plus notification time.The jammer controls the probability of jamming in order to cause more damage to the network.	Optimal detection test based on the percentage of incurred collisions.	For attack detection this model provides decision based on the incurred collisions with the nominal one.	The method provides valuable insight about the structure of the jamming problem and demonstrate sophisticated strategies for achieving desirable performance.	The detection performance decreases because the mobile attackers move in and out of the range of the observer.
9.	Information Warfare-Worthy Jamming Attack Detection Mechanism for Wireless Sensor Networks Using a Fuzzy Inference System	WSN very suitable for hunting jammers, i.e., detecting, localizing and tracking the jammers is a very costly and difficult task.	Fuzzy Inference System	Jamming detection is done by the base station based on the input values received from the nodes. 1) the number of total packets received during a specified time period 2) the number of packets dropped during the period 3) the received signal strength (RSS).	Decision for jamming detection is taken by the nodes themselves in the existing methods which is considered as not feasible and here it is decided by the base station.	discriminating edge and corner nodes from the rest and allotting various allowances to them for loss of prospective jammed or un-jammed neighbors in our algorithm.

10.	Reactive Jamming Attacks in Multi-Radio Wireless Sensor Networks: An Efficient Mitigating Measure by Identifying Trigger Nodes	To overcome the shortcoming in the existing methods existingi.e. frequency hopping or channel surfing, require excessive computational capabilities on wireless devices which are serious side effects in wireless sensor networks.	group testing (GT) theory routing protocol *TNLT*	By utilizing GT theory, disk cover based grouping and clique based clustering , the proposed protocol can accurately identify the trigger nodes among the victim nodes with low message and computational complexity.	carefully designs a better routing protocol by switching these nodes into only receivers to avoid activating jammers reduces computational overhead present in the previous methods.	Negligible packet loss

CONCLUSION

This article reviewed the main aspects of wireless sensor network security against jamming attacks: vulnerabilities of today’s WSNs, types of jammers and attacks, and effective of jamming attacks. It also classifies the research works that deal with jamming in WSNs based on highlighting their relevant positive aspects and shortcomings. Furthermore it highlights open research issues in the field of jamming in adoption and usage of WSN technologies in military and monitoring applications is expected to bring out the immense importance of this security issue.

REFERENCE

[1] *A. D. Wood and J. A. Stankovic, “Denial of service in sensor networks”, Computer, vol. 35,no. 10, pp.54-62, 2002.*

[2] *Aristides Mpitziopoulos, Damianos Gavalas, Charalampos Konstantopoulos, and Grammati Pantziou, “A Survey on Jamming Attacks and Countermeasures in WSNs”, IEEE communications surveys & tutorials, vol. 11, no. 4, fourth quarter 2009*

[3] *I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “A survey on sensor networks,” IEEE Commun. Mag., vol. 40, no. 8, pp. 102-114, Aug. 2002.*

[4] *A. Proano and L. Lazos. Packet-Hiding Methods for Preventing˜ Selective Jamming Attacks. IEEE Transactions on Dependable and Secure Computing, 9(1):101–114, January/February 2012.*

[5] *L. van Hoesel, Y. Wei Law, J. Doumen, P. Hartel, and P. Havinga, “En- ergy efficient link layer jamming attacks against wireless sensor network MAC protocols,” ACM Trans. Sensor Netw. (TOSN), Feb. 2009.*

[6] *A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, “A survey on jamming attacks and countermeasures in WSNs,” IEEE Commun. Surveys Tutorials, vol. 11, no. 4, Dec. 2009.*

[7] *Misra, S., Singh, R., Mohan, S.V.R.: ‘Information warfare-worthy jamming attack detection mechanism for wireless sensor networks using a fuzzy inference system’, Sensors, 2010, 10, (4), pp. 3444– 3479*

[8] *Xu, W., Trappe, W., Zhang, Y., Wood, T.: ‘The feasibility of launching and detecting jamming attacks in wireless networks’. Proc. Sixth ACM Int. Symp. on Mobile Ad Hoc Networking and Computing, 2005, pp. 46–57*