A SURVEY ON JAMMING ATTACKS, DETECTION AND DEFENDING STRATEGIES IN WIRELESS SENSOR NETWORKS

Mehreen Shaikh[1], Abid. H Syed[2]

[1]*Student of M.Tech, Department of Electronics & Communication Engineering, BLDEA'S CET, Karnataka, India*
[2]*Assistant Professor, Department of Electronics & Communication Engineering, BLDEA'S CET Karnataka, India*

Abstract

Wireless Sensor Network (WSN)s are now a days most widely used and are undergoing many security threats. Of the different types of threats, Jamming attack has been considered a severe security threat. These jamming attacks cause the overutilization of scarce resources like the battery power. Further, high computations require lot of memory. Such problems cause the reduction in the lifetime of the sensor nodes in WSNs. There are four types of jamming attacks in which the most difficult type of attack is the reactive jammer as it is easy to launch by the adversary but very difficult to detect and defend. In this paper we present a brief survey of the types of jamming attacks, methods used to detect and defend the jammers.

Keywords: *Wireless Sensor Networks, Jamming Attacks, Reactive jamming attack, and Trigger node identification.*

----------***----------

1. INTRODUCTION

Wireless Sensor Networks contain a number of sensor nodes that are responsible for routing the data over the wireless networks. WSNs are more widely used and find its applications in data aggregation, data monitoring etc. The major aspect of WSN is to provide security of data in such a way that data is not affected by any intruders or jammers. WSNs are affected by jamming attacks. Jamming attacks are those which try to interfere with the transmission and reception of wireless signals by emitting RF signals. There are different types of jammers that try to intentionally inject false data during the communication between two nodes which affects the data transmission and also the performance of WSN reduces as it causes the overutilization of the scarce resources like battery power, memory etc. There are many methods that have been developed to detect the jammers and also to defend the jamming attacks.

Our work in this paper describes the survey of different methodologies used to detect and defend the jamming attacks. This paper is organized as follows, in Section II we describe the types of jammers, in Section III Overview of the methods used for detecting Jamming Attacks, in Section IV Overview of the methods used for evading Jamming Attacks, in Section V Overview of the methods proposed for locating and defending Reactive Jammers.

2. TYPES OF JAMMERS

Jamming nodes are classified depending on the different characteristics these nodes posses [1]. They are i) Constant Jammer ii) Deceptive Jammer iii) Random Jammer iv) Reactive Jammer.

Constant jammer: It continually emits a radio signal, and can be implemented using either a waveform generator that continuously sends a radio signal or a normal wireless device that continuously sends out random bits to the channel [1].

Deceptive jammer: The deceptive jammer continuously sends regular packets on the channel without any gap between the packets.

Random jammer: A random jammer alternates between sleeping and jamming. During its jamming phase, it behaves like a constant jammer or a deceptive jammer.

Reactive jammer: This type of jammer is quiet until the medium is idle and when it senses transmission on the medium it starts injecting false data which avoids the legitimate user to send data. Among all the above four jammers the reactive jammer is very difficult to detect.

3. OVERVIEW OF THE METHODS USED FOR DETECTING JAMMING ATTACKS.

The various methods employed for the detection of jamming attacks is based on the Basic Strategies and Advanced Strategies. Each of these strategies has drawbacks that we discuss in the paper as follows [1] [2].

3.1 Basic Strategies

a) Signal Strength — As the strength of the signal gets affected by the presence of interference hence in this method the detection of jamming is done by the strength of the received signal. Here we compare the average signal magnitude with the threshold which is calculated by the noise levels.

Drawback: It is very difficult to discriminate between the normal traffic and reactive jammer traffic as the signal strength for both the traffic is similar. Hence reactive jammers are difficult to detect.

b) Carrier Sensing Time — In this method the carrier sensing time is used to detect the presence of jammer. Here we can detect whether the channel is busy or idle by comparing the noise level with fixed threshold.

Drawback: This method is efficient only for the detection of constant jammer. If the jammers are random and reactive this method is inefficient.

c) Packet Delivery Ratio — PDR is defined as the ratio of the total number of packets delivered successfully to destination to the total number of packets transmitted by the source. In this method jamming is detected based on the value of PDR. If the value of the PDR is close to zero then this indicates the presence of jammers. PDR is effective in differentiating jamming and network congestion.

Drawback: PDR cannot differentiate between jamming attack and network dynamics hence it is not as effective in case of network dynamics i.e. if the sender battery fails and sender is not within the communication range of receiver which causes drop in PDR.

3.2 Advanced Strategies

The basic strategies provide the information whether the jammer is present or the network is congested but do not evade the jammers. These advanced strategies are developed by combining the basic strategies [3]. By combining basic strategies such as PDR and signal strength we can find the reason for bit errors within a packet and determine whether the packet was affected by jamming attack or was sent through a weak link.

When there is no interference, high signal strength refers to a high PDR. If the signal strength is low, the PDR will also be low. A low PDR may also be due to a node's neighbors have died by consuming battery or device faults, or jamming of the node.

4. OVERVIEW OF THE METHODS USED FOR EVADING JAMMING ATTACKS.

To defend against the jamming attacks following are the strategies developed [1].

a) Channel Surfing: This strategy is a motivation of frequency hopping modulation. In channel surfing if a node senses interference then to avoid interference it changes its assigned channel to a new channel.

This strategy is well suited for the communication between two nodes. It is not suitable if there are multiple nodes and after sensing interference each node switches to a new channel which causes unreliable coordination and in turn provides challenges like asynchrony, latency and scalability.

If we use coordinated channel switching then the entire network will switch to a new channel. But latency increases as the scale of the network increases which results into an unstable network.

This problem can be overcome by allowing only jammed regions to switch to a new channel.

b) Spatial Retreats: In this strategy the jammed nodes try to move from the jammed regions. This technique is best suited for the mobile sensor networks. If the mobile sensor node finds a jammed area or a jammed node then it must move to a safer location.

The problem associated with this technique is that as the jammers are mobile hence they can cause the entire network to relocate. In order to overcome this problem the spatial retreat must gain robustness to mobile jammers. This can be achieved from two phases they are
1) Escape phase – In this phase the nodes which are located in jammed area escape to "safe" regions and also manage to stay connected with the network.
2) Reconstruction phase – In this phase the mobile nodes achieve uniform coverage and also the network partitioning is prevented.

c) Region Based Signal to Noise Ratio:
In order to determine the level of disturbance the entire network is subdivided into three divisions they are unaffected nodes, jammed nodes and the boundary nodes.

Considering region based and signal to noise ratio based are the two jamming models then the region based model determines the impact of jamming by evaluating received jammed signal strength. But whereas SNR based model determines the SNR at the receiver which determines more accurately the effects of jamming.

Table-1 Methods for detection of jamming attacks in WSNs

Method	Description	Problems
Signal strength	The strength of the signal is affected by the presence of jammers. We compare the average signal magnitude with a threshold which is calculated from the noise levels.	Difficult in discriminating jamming scenarios and normal traffic scenarios.
Carrier Sensing Time	Two important observations are made a)MAC protocol is used to determine the status of the channel b)Jammers must not be reactive or random.	It is used to detect only constant jammer. Cannot be allowed for detection of all jamming scenarios.
Packet Delivery	The number of packets sent and received	Not effective for network parameter

Ratio	successfully by the sender and receiver is determined.	dynamics like 1)sender battery failure 2) sender or receiver out of communication range etc.

Table-2 Methods used for defending jamming attacks in WSNs

Methods	Description	Problem
Channel Surfing	It is the motivation of frequency hopping modulation. If interference is sensed then to avoid interference the assigned channel changes to a new channel	Suitable only for two nodes scenario Channel switching causes unreliable co-ordination of channel frequency
Spatial Retreats	The jammed nodes move from jammed regions. Suitable for mobile sensor network	As jammers are mobile hence they cause the entire network to relocate.
Region based SNR	Network is subdivided in three subdivisions. Impact of jamming is determined by evaluating received jammed signal strength.	Complex as network must be subdivided and time consuming

5. OVERVIEW OF THE METHODS PROPOSED FOR THE LOCATING AND DEFENDING REACTIVE JAMMERS.

In the above methods it is very difficult to identify the reactive jammers. The different techniques used to detect and defend reactive jammers are as follows [3] [4].

a) Non –Adaptive Group Testing: Group Testing was developed and applied to medical testing since WWII. This technique can be associated with the work to identify the trigger nodes from large victim nodes.

By the help of group testing we can find out all the trigger nodes within very short period of time.

b) Minimum Disk Cover in a Polygon: Consider a simple polygon having a set of vertices in it, and we have to find out the minimum number of variable-radii disks that are within the polygon and also cover all given vertices. This technique can be used to estimate the jamming range.

c) Clique-Independent Set: This technique finds a set of optimum number of pair wise vertex maximal cliques, called as maximum clique-independent set.

The reactive jammers are defended by trigger node identification service [3] [5].

This method is lightweight and all the computations are done at the base station which provides low transmission overhead and less time complexity and theoretically guaranteed as well. The three main steps of the procedure are

1) Anomaly Detection - Each sensor sends the status report message to the base station periodically. The base station detects reactive jamming attacks as each boundary node reports their identities to base station.

2) Jammer Property Estimation – the report received by the boundary nodes helps to determine the location of boundary nodes and the base station calculates the jammed area and jamming range.

3) Trigger Identification – Here we consider encryption technique in which base station creates an encrypted message and broadcasts to all boundary nodes in the network.

The boundary nodes continue to broadcast the message to all victim nodes within the jammed area for a certain period of time.

Now all the victim nodes start executing the procedure of testing based on the broadcast massage which helps them to identify themselves as trigger nodes or non-trigger nodes.

6. CONCLUSION

The basic strategies such as signal strength, carrier sensing time and PDR are effective in the detection of jamming attacks with a limitation of defending them. The advanced strategies help in finding out reason for the presence of errors in the packets but do not defend the jammers. The methods channel surfing, spatial retreats and region based signal to noise ratio evade the jammers but have drawback of asynchrony, latency and scalability. All the above methods have a common drawback that they are not effective in detecting and defending reactive jammers. Techniques such as non – adaptive group testing, minimum disk cover in a polygon, clique independent set are effective in detection and defending reactive jammers but with increase in latency. Hence a trigger identification method has been proposed in order to detect the reactive jammer in WSN by providing the advantage of low transmission overhead and less time complexity and also theoretically guaranteed.

REFERENCES

[1]. Wenyuan Xu, Ke Ma, Wade Trappe, and Yanyong Zhang, Rutgers University, “Jamming Sensor Networks:Attack and Defense Strategies”, IEEE Network , May/June 2006.

[2]. Wenyuan Xu, Wade Trappe, Yanyong Zhang and Timothy Wood, “ The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks”, ACM, MobiHoc’05, May 25-27, 2005, Urbana-Champaign, Illinois, USA.

[3]. Ying Xuan, Yilin Shen, Nam P. Nguyen, My T. Thai, “A Trigger Identification Service for Defending Reactive Jammers in WSN”, IEEE Transaction on Mobile Computing, Vol.11, No.5, May 2012.

[4]. Incheol Shin, Yilin Shen, Ying Xuan, and My T. Thai, Taieb Znati, "Reactive Jamming Attacks in Multi-Radio Wireless Sensor Networks: An Efficient Mitigating Measure by Identifying Trigger Nodes",ACM FOWANC'09, May 18, 2009.

[5].Vinothkumar.G, Ramya.G, Rengarajan.A, " Lightweight Decentralized Algorithm for Localizing Reactive Jammers in Wireless Sensor Network",31st International Conference on Distributed Computing Systems,2011.

BIOGRAPHIES

Mehreen R Shaikh received her bachelor's degree from Visveswaraya Technological University and is pursuing master's degree in Digital Communication and Networking from Visveswaraya Technological University Belgaum. Her interests include sensor networks

Syed Abidhusain received his bachelor's degree in Electronics and Communication from Visveswaraya Technological University and master's degree in Digital Communication from BEC Bagalkot. Pursuing Ph D in networking from Visveswaraya Technological University Belgaum. His interests include sensor networks, and networking.