



Defending Reactive Jammers Attacks in Wireless Sensor Networks by Identifying Trigger Nodes

Karuna Patil*, Abdul Rehman Afrad

Department of Computer Science and Engineering
SIET- Bijapur, Karnataka, India

Abstract: *Much literature is available against reactive jamming attacks like frequency hopping or channel surfing which requires too much computational capabilities on wireless devices which have serious side effects in wireless sensor networks. The jamming attack is one of the most important security issues where a jammer node get in the way with the signal of adjacent sensor nodes disrupting the message delivery of its neighboring nodes. In wireless sensor network which is having a broadcast nature and also limited resources such as battery power, memory, computational capabilities these jammers can create problems to legitimate sensor communication. Reactive jamming attack is a light weight attack performed by the adversary but they are easy to start on and difficult to recognize. To avoid the problems in existing methods, in this project a novel approach proposed against reactive jamming attacks by identifying the trigger nodes, whose transmissions activate any reactive jammers. Hence in this paper various techniques to identify the jamming attack has been discussed and the emphasis is laid on detecting the reactive jammers. A more efficient method has been proposed which identifies and defends the reactive jammers in wireless sensor network using the sensing trigger nodes.*

Key words: *Wireless Sensor Network, Jamming attack, Reactive jammers, Trigger nodes.*

I. INTRODUCTION

Wireless sensor network is widely used now-a-days and has many applications in today's scenario. Ranging from data gathering to monitoring applications, hence security of data over these networks becomes an important aspect so that the data or the network does not get susceptible to any intruder or third party. Security challenges are increasing day by day as the adversary are finding new ways to detect the confidential transmissions hence there is a great need to think differently over the situation. Since the traditional ways of defending the attack is not fulfilling the need of security, hence a new approach towards this problem is needed.

Jamming resembles to denial-of-service attack and thus prevents legitimate users to send its data as the jammers purposefully emits radio frequency signals to corrupt wireless transmissions. The jammers nodes can have different characteristics depending upon which they have been classified as: (i) Constant Jammer, (ii) Deceptive Jammer, (iii) Random Jammer, (iv) Reactive Jammer. Among these jammers the most harder to detect is the reactive jammer since compared to others which are active in nature i.e. they try to block the channel without having any prior information of the traffic pattern on the channel while the reactive jammer stay quiet when the channel is idle, but starts transmitting a radio signal as soon as it senses some activity on the channel. Thus reactive jammers are harder to detect and needs more efficient identification and defending system.

There are various techniques for sensing the jammed areas which has been carried out and studied against the jamming attacks. 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 favored by attackers. Furthermore, in reactive jamming attacks [1], 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.

II. LITERATURE SURVEY

Coping with jamming and interference is usually a topic that is addressed through conventional PHY-layer communication techniques. In these systems, spreading techniques (e.g. frequency hopping) are commonly used to provide resilience to interference [2, 3]. Although such PHY-layer techniques can address the challenges of an RF interferer, they require advanced transceivers. Further, the issue of detecting jammers was briefly studied by Wood et al. [4], and was further studied by Xu et al. [5], where the authors presented several jamming models and explored the need for more advanced detection algorithms to identify jamming. Jamming detection was also studied in the context of sensor networks [6, 7] and in networks involving frequency hopping [8]. Our work focuses on localizing jammers after jamming

attacks have been identified using the proposed jamming detection strategies. Without localizing jammers, Wood et al. [4] has studied how to map the jammed region. The basic idea is to have the jammed nodes bypass their MAC-layer temporarily and announce the fact that they are jammed. With slightly modification, our algorithm can not only localize the jammer but also map the jammed region.

The basic techniques like Received signal Strength (RSS), Carrier Sensing time (CST), Packet Delivery Ratio (PDR), together has a disadvantage that they only can work to identify the interference in the signal. Though there are enough schemes or methods by which the jamming signals can be discovered but to locate the jammer nodes depending on the signals is not solved yet.

On the other hand the advanced techniques make use of multiple frequency bands and MAC channels however; the high computational overhead and excessive wastage of the frequency band badly reduces the efficiency of the resource limited network environment. To take an example of the channel surfing method the frequency hopping take place till it does not find a suitable channel free of any adversary. Since here an environment is considered where resources are tightly bounded i.e. Wireless Sensor Network we cannot ignore these resources to be utilized vaguely. Since in WSNTs the sensors have to scan all the channels to find a free channel even in the middle of communication can cause communication stalls. Thus if this happen frequently then it will result in longer transmission duration and more energy consumption.

Another problem in the Spatial retreat is that it has considered that the jammer is stationary hence if the jammer is mobile then its movement may cause the network to become severely unbalanced. All these methods [9] have assumed that that the jammers capabilities are limited and powerless to catch the actual traffic from the camouflage of these diversities. However due to silent behavior of reactive jammers, they have more powers to destruct the other mitigation methods.

Contributions in this project is as follows-

- To introduce the concept of trigger nodes in reactive jamming attacks.
- 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. This is critical and suitable for WSNs since they have only limited resources and energy conservation.

2.1. Problem Statement

Traditional approaches for the detection of jamming in wireless sensor networks use the packet-delivery-ratio (PDR) and the received ambient signal strength as the main decision criteria. Jamming is detected as soon as the (averaged) PDR and/or the ambient signal strength exceeds a pre-defined threshold (see Section VII). Although these approaches are well-suited for the detection of proactive (long-term) jamming, they are not sufficient to protect the considered applications against targeted reactive jamming: Firstly, existing schemes rely only on the CRC of a packet to decide whether it was received correctly and thus can (in general) not distinguish between packet failures due to weak radio links and interference. Secondly, assessing an accurate PDR is not practical in a reactive forwarding scheme as messages are sent very rarely.

Thirdly, jamming does not necessarily cause a steady and high received signal strength (RSS) value as only a small fraction of a packet has to be interfered with in order for the packet to be invalid

III. APPROACHES AND METHOD

3.1 Basic Techniques

The main focus is on the identification of the reactive jammers. This identification can be on the basis of radio interference, or in a scenario where there is poor connectivity involving congestion and device failures thus it becomes very difficult to differentiate between jamming attack or a real time situation of congestion. Thus to have a closer look at the situation many methods [10], [11] have been are there which are as follows:

Signal Strength

One of the methods is to determine the strength of the signal by measuring the signal strength and analyzing the signal strength distribution to have the account of the presence of the attacking jammer. The approaches to identify the jamming signal involve comparing average signal magnitude with that of the threshold calculated from the overall noise level.

With the study on this method it has been found that the reactive jammer can keep the increase in the effective RSS (Received signal Strength) value very low and hence it avoid being detected.

Carrier Sensing Time

A constant Jammer keep the channel constantly busy thus preventing the source to send out packets hence carrier sensing time can be used to know whether the device is jammed or not. Similar to the Signal strength method a channel is idle or not can be determined by comparing the noise level with the fixed threshold. To distinguish between a congestion and jammed scenario carrier sensing time can be used as the sensing time in first will be bounded and in later sensing time will be unbounded.

Packet Delivery Ratio

PDR refers to the ratio of packets that successfully delivers to a destination compared to the number of packets that have been sent out by the sender. But here detecting the reactive jammer is a mere challenge because in this the messages are sent very rarely and typically only when it is triggered by some another signal. However PDR can be used to distinguish between the jamming attack and a congested network scenario.

3.2 Advanced Techniques

The above discuss methods involve some basic statistical method which only can be used get the information regarding whether the there is a congestion in a network or a jammed situation. Identification of jammer nodes cannot be done through the above methods; it requires some advanced detection strategies [12] such as to combine PDR with the Signal strength which can give more efficient results compared to the basic methods.

Since there may be many other techniques to defend the jammers it would not be always possible to detect and defend them using these techniques due to its (Reactive Jammer) vague properties. The adversary may be in continuous efforts to disrupt the network while the security experts would always find ways to defend them.

Channel Surfing

Radio communication operates on the single channel therefore if any third party comes in the range of the communication the communicating device may migrate to another channel which is free. This happens in the physical layer of the network and is called as the frequency hopping. Using this technique jammers can be evaded by continuously switching from one frequency channel to another until it finds the free channel to transmit its signal.

Spatial Retreats

This technique is best suitable in a mobile network where the communicating nodes are mobile. This technique is used when there is a jammed area in a mobile network such as user with cell phones or WLAN if the mobile nodes are disrupted by the jammer nodes then the mobile nodes should simply escape to a safe location.

Region Based Signal to Noise Ratio

To now the jamming effects based on the level of disturbance the network can be divided into three categories: unaffected nodes, jammed nodes and boundary nodes. And consider two jamming models region based and signal-to-noise- ratio, here the region based model determines the impact of jamming by examining received jammed signal strength. While the SNR based model determines the SNR at the receiver which can estimate the jamming effects more accurately.

3.3 Proposed Solution

To overcome the disadvantages discussed in above section a method [13] is proposed against reactive jamming attack in Wireless Sensor Network by using trigger nodes. Trigger nodes are named as such due to its properties i.e. the trigger nodes are only the normal nodes taking part in the communication in the network (Fig.5.1) but when the network gets jammed, the victim nodes under that jammed area performs the group testing under is group testing each nodes transmits signal and check for any disruption in the transmission, the node which triggers the activation the reactive jammer node is called as the trigger node.

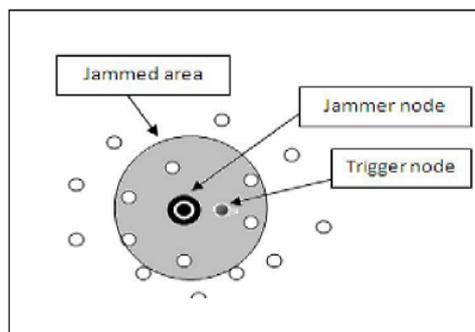


Fig.3.1. Jammed Situation in WSN

The basic idea of proposed solution (Fig.5.2) is that when a packet is routed from source to destination and if the packet does not reach to the delivery point at time it first check whether there is a jamming issue or a congestion problem using PDR and RSS.

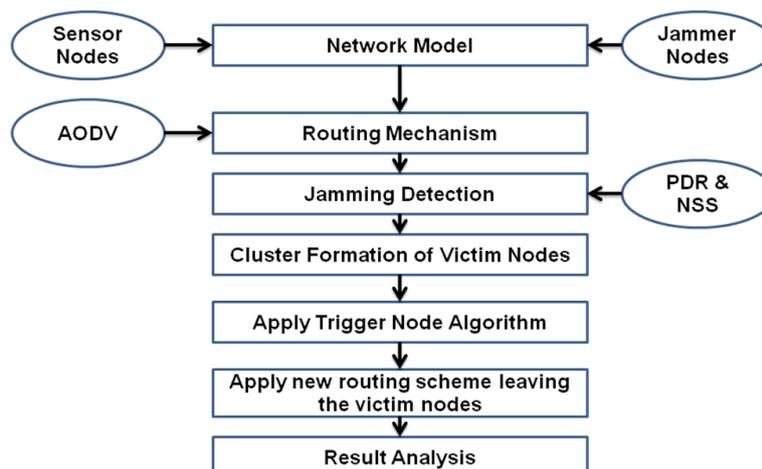


Fig. 3.2: Proposed Methodology.

If jamming is identified then it first identifies the set of victim nodes, then these victim nodes would be clustered into multiple testing teams. Then each cluster or group will perform its testing locally to identify each of them as trigger nodes or non-trigger nodes. Then the results can be stored to deploy a reactive routing mechanism or to send the information to base station. Using this information a new routing mechanism can be devised to route the data packets evading the jammers in the network.

3.3.1 Network Model

For this purpose a basic communication network model is proposed considering following simulation parameters:

Table 3.1. Simulation Parameters

Sl No.	Simulation Parameters	Values
1	The number of nodes in WSN(N) $N \ll 100$	$N \ll 100$
2	The transmission range of the base Station	$r = 250\text{m}$
3	The transmission range of each sensor	250m
4	The number of jammers	$J(1,10)$
5	The noise range of the jammers	$R \gg r$
6	The total testing time	200 Sec
7	Energy of each sensor node	100J

Sensor node:

Sensor node positions cannot be known before-hand and for each simulation it will differ and the sensor nodes as well as jammers would remain static till one round of simulation ends.

- For this consider network as a connected graph $G(V, E)$ where V is a set of N nodes and E representing communication links between nodes.
- Sensors will have omni-directional antennas with uniform strength on each direction.
- Each sensor node would have a Sensor_ID so as to uniquely identify each sensor node in the network.
- Sensor nodes would send a report message periodically to the Base station consisting of Sensor_ID, Status (Victim node/Trigger node/Boundary node/Unaffected node), and Message details.

Jammer nodes:

Reactive jammers keep idle until they sense any ongoing legitimate transmissions and then emit jamming signals (packet or bit) to disrupt the sensed signal (called jammer wake-up period), instead of the whole channel, which means once the sensor transmission finishes, the jamming attack s will be stopped (called jammer sleep period).

- Jammers would also have omni-directional antennas. The jammed area can be regarded as a circle centered at the jammer node, with a radius R . All the sensors within this range will be jammed during the jammer wake-up period.
- Any two jammer nodes are assumed not to be too close to each other, i.e., the distance between jammer J_1 and J_2 is $d(J_1, J_2) > R$.
 - 1) No large overlapping between jammed areas of different jammers should be there as it lowers down the attack efficiency.
 - 2) The $d(J_1, J_2)$ should be greater than R , since the transmission signals from one jammer should not interfere the signal reception at the other jammer.

IV. CONCLUSION

The Basic and Advanced techniques which has been discussed has not solved the problem i.e. how to locate the jammers and also used traditional ways of security methods of defending only and due to which in the scenario where the resources are limited such as Wireless /sensor Network it would not be efficient to use these technique. Hence a new approach is proposed to efficiently tackle the reactive jammers in wireless sensor network using the trigger nodes which involves the new scheme of evading technique and will help enhance the security and performance of such networks with more efficient routing scheme. Thus giving a new dimension as to how the security issues can be handled i.e. not only by defending them but how to sense them instead and how to evade them thus saving energy, time and computational complexities involved earlier.

REFERENCES

- [1] Y. Z. Wenyan Xu, Wade Trappe and T. Wood. The feasibility of launching and detecting jamming attacks in wireless networks. International Symposium on Mobile Ad Hoc Networking and Computing, pages- 6–57, April 2005.
- [2] Proakis, J. G. (2000). Digital communications (4th ed.). Singapore: McGraw-Hill.
- [3] Schleher, C. (1999). Electronic warfare in the information age. Norwood: MArttech House.
- [4] Wood, A., Stankovic, J., & Son, S. (2003). JAM: A jammed-area mapping service for sensor networks. In 24th IEEE real-time systems Symposium. pp. 286–297.
- [5] Xu, W., Trappe, W., Zhang, Y., & Wood, T. (2005). The feasibility of launching and detecting jamming attacks in wireless networks. In MobiHoc '05: Proceedings of the 6th ACM international Symposium on mobile ad hoc networking and computing. pp. 46–57.

- [6] C. Akirog̃lu, M., & Õzcerit, A. T. (2008). Jamming detection mechanisms for wireless sensor networks. In *InfoScale '08: Proceedings of the 3rd international conference on scalable information systems*. ICST, Brussels, Belgium, Belgium: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), pp. 1–8.
- [7] Mraleedharan, R., & Osadciw, L. A. (2006). Jamming attack detection and countermeasures in wireless sensor network using ant system," in *Proceedings of the SPIE in wireless sensing and processing*, (Vol. 6248). p. 62480G.
- [8] Chiang, J. T., & Hu, Y.-C. (2007). Cross-layer jamming detection and mitigation in wireless broadcast networks. In *MobiCom '07: Proceedings of the 13th annual ACM international conference on mobile computing and networking*. New York, NY, USA: ACM, pp. 346–349.
- [9] Incheol Shin, Yilin Shen, Ying Xuan, and My T. Thai, Taieb Znat, Reactive Jamming Attacks in Multi-Radio Wireless Sensor Networks: An Efficient Mitigating Measure by Identifying Trigger Nodes", *ACM FOWANCF09*, May 18, 2009.
- [10] Wenyuan Xu, Ke Ma, Wade Trappe, and Yanyong Zhang, Rutgers University, Jamming Sensor Networks: Attack and Defense Strategies", *IEEE Network*, May/June 2006.
- [11] 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.
- [12] Mario Strasser, Boris Danev, Detection of Reactive Jamming in Sensor Network ", *ACM Transactions on Sensor Networks*, Vol. 7, No. 2, Article 16, Publication date: August 2010.
- [13] Wenyuan Xu, Timothy Wood, Wade Trappe, Yanyong Zhang, Channel Surfing and Spatial Retreats: Defenses against Wireless Denial of Service", *ACM, WiSe'04*, Philadelphia, Pennsylvania, USA, October 1, 2004.