Graduate Research in Engineering and Technology (GRET)

Volume 1 | Issue 2 Article 11

October 2013

AN ENERGY EFFICIENT DEACTIVATION TECHNIQUE FOR REACTIVE JAMMERS IN WIRELESS SENSOR NETWORKS

SUPREETHA PATEL T P
Department of Computer Science and Engineering, Siddaganga Institute of Technology, Tumkur, Karnataka, India., spateltp@gmail.com

K. N. SHREENATH
Department of Computer Science and Engineering, Siddaganga Institute of Technology, Tumkur, Karnataka, India., knshreenath@gmail.com

AN ENERGY EFFICIENT DEACTIVATION TECHNIQUE FOR REACTIVE JAMMERS IN WIRELESS SENSOR NETWORKS

SUPREETHA PATEL T P[1], K.N. SHREENATH[2]

[1]M.Tech Student, [2]Associate Professor, Department of Computer Science and Engineering, Siddaganga Institute of Technology, Tumkur, Karnataka, India.

Abstract- In recent days, reactive jamming attack has emerged as a great security threat to wireless sensor network [WSN]. Several strategies are developed to identify the trigger nodes, whose legitimate transmission activates any reactive jammer. After identifying the trigger node, the node will be shut down to deactivate the jammer and its routing information is deleted from the routing table, then the node can't be used again in the network. Since the node can't be used again in the network it is one of the major drawbacks. Hence to overcome the problem, In this paper we propose a novel approach, where the identified trigger nodes are put in to the scanning mode, so that we can reuse the trigger nodes, after deactivating the jammer node in the network.

Keyword- *Reactive Jamming, Jamming detection, Trigger Identification, Jammer node, Jamming, Reactive jammer node, Sleep mode, Report message.*

I. INTRODUCTION

During last decade, the security of wireless sensor networks [WSN] has attracted numerous attentions, due to its wide applications in various monitoring systems and vulnerability towards sophisticated wireless attacks. Among these attacks jamming attack, where a jammer node disrupts the message delivery of its neighbor sensor nodes with interference signals or packets has become a critical threat to the WSN's. However in Reactive jamming attack, where jammer nodes stay quiet until an ongoing legitimate transmission (even has a single bit) is sensed over the channel emerged recently and requires stronger defending system to identify and more efficient detection scheme to deactivate it.

There are many existing studies against the detection of reactive jamming and to identify the trigger nodes which causes jamming in the network. Several strategies are developed to identify the trigger nodes [8] [3]. All these strategies mainly involve the procedure for identifying trigger node and after identification, a new routing path would be constructed to avoid activating of any reactive jammers. But for the wireless sensor networks constructing new routing path has become overhead, since the battery usage must be efficient. We know that the lifespan of such sensor network applications ranges from months to years and, given limited power supply of sensor nodes, places high demands on the energy efficiency of the algorithms. In this paper, we simply use a message exchange scheme to deactivate the jammers in the network.

In this paper, we use an application layer real time trigger-identification service for reactive jamming in wireless sensor networks [WSN], which promptly provides the list of trigger-nodes using a light weight decentralized algorithm, without introducing neither new hardware devices, nor significant message overhead at each sensor node. After identification we put the identified trigger node in the scanning mode there they emits the fake or beacon signals then jammer node thinks that the node is participating in the actual transmission. This forces the jammer node keep on emitting the jamming signal there by exhausting the jammer node battery. The basic idea of this paper is to first identify the set of victim nodes in the sensor network by investigating corresponding links packet delivery ratio and receiver signal strength then these victim nodes are grouped into multiple testing teams. Once the group testing schedule is made at the base station and routed to all victim nodes, they then locally conduct the test and identify them as a trigger or non trigger. The identification results can be stored locally for jamming localization process. Then base station puts the identified trigger nodes to the scanning mode. In this mode the trigger nodes send beacon signal until the energy of jammer node exhausts to deactivate it.

The rest of the paper is organized as follows. Section II provides an overview of related work, which includes the procedure for identifying the trigger nodes. In section III we explain our system model. Then we explain the proposed system in section IV. We analyze the message and time complexity of the proposed method by comparing with ying xuan's scheme in section V. Lastly we conclude the paper in section VI.

II. RELATED WORK

In this section we present some of the techniques which already exist to solve the jamming in the

network and the procedure for trigger node identification service for identification of trigger nodes.

All effective countermeasures against reactive jamming attacks consist of jamming (signals) detection and jamming mitigation. First thing, detection of interference signals from jammer nodes is nontrivial due to the discrimination between normal noises and adversarial signals over unstable wireless channels. Numerous attempts are made to monitor the critical communication related objects, such as receiver signal strength(RSS), carrier sensing time (CST), packet delivery ratio (PDR) compared with specific thresholds, which were established from basic statistical methods and multimodal strategies[3][4]. By such schemes, jamming signals could be discovered, but to locate the jammer nodes based on these signals is much more complicated.

Secondly, various network diversities are investigated to provide mitigation solutions [9]. Spreading spectrum [4][10] making use of multiple frequency bands and MAC channels , multiple routing benefiting from multiple pre-selected routing paths[6] are two good examples of them. However in this method, the capability of jammers is assumed to be limited and powerless to catch the legitimate traffic from the camouflage of these diversities. However due to the silent behavior of reactive jammers they have more power to destruct these mitigation methods. A mapping service of jammed area has been presented in [11], which detect the jammed areas and suggest that routing paths evade these areas. This works for proactive jamming, since all the jammed nodes are having low PDR and thus incapable for reliable message delay.

The trigger identification service [8] exhibits great potentials to be developed as reactive jamming defending schemes. As an example, by excluding the set of trigger nodes from the routing paths, the reactive jammers will have to stay idle since transmissions cannot be sensed even though the jammers move around and detect new sensor signals, the list of trigger nodes will be quickly updated, and so are routing tables. As another example, without prior knowledge of the numbers of jammers, the radius of jamming signals and specific jamming behavior types, it is quite hard to locate the reactive jammers even the jammed areas are detected. However, with the trigger nodes localized, we can narrow down the possible locations of reactive jammers.

A. Trigger Identification Service

In this section we discuss the procedure for identifying the trigger nodes from the pool of victim nodes in the sensor networks. The procedure of trigger node identification involves 3 main steps. This procedure is light weight since all the calculation occurs at the base station, and the transmission overhead as well as the time complexity is low theoretically guaranteed.

1) Anomaly Detection

Already we know that all the sensor nodes in the network periodically send a status report message to the base station. However once the jammers are activated by message transmission, the base station will not receive these report from some sensors. By comparing the ratio of received reports to predefined thresholds, the base station can thus decide if a jamming attack has occurred in the network. The status report message contains the label field based on the jamming status. It can be defined in three ways. Consider if any sensor node hears jamming signals it will not try to send the status report to the base station, but it updates its label field as victim node. Once the base station does not get message from that node for a period of length it declares it has a victim and put it for the testing. If any sensor node does not hear jamming signals and it is able to send its status report to the base station then that node is considered as unaffected node. If any node does not receive ack from its neighbor on the next hop of the route within a time out period, it tries for two or more retransmission. If no ack are received, it is quite possible that neighbor is a victim node then node updates label tuple as boundary node in its status report.

2) Jammer Property Estimation

Here we estimate the jamming range and the jammed area as simple polygons, based on the locations of the boundary and victim nodes.

3) Trigger Detection

The procedure to detect the trigger node is as follows: The identified victim nodes are grouped into the interference free testing teams by using clique independent set which is referred to as a maximum clique independent set(MCIS) [2] [12]. Then the grouped testing teams are further divided into testing groups by using randomized disjoint matrix. Then base station sends the encrypted testing schedule message to all the identified victim nodes. Boundary nodes keep broadcasting to all the victim nodes within the estimated jammed area for a period. All the victim nodes locally execute the testing procedure and identify themselves as triggers or non triggers.

III. SYSTEM MODEL

In this section we explain the consideration of the network. It consists of network model, attacker model and sensor model.

A. Network model

The wireless sensor network in our problem consists of N sensor nodes each having the same transmission

range and one base station (larger networks with multiple base station can be split into small ones to satisfy the model). Each sensor node is equipped with a globally synchronized clock, omnidirectional antennas, m radios for in total k channels throughout the network where k>m, for simplicity we modeled the considered network as a connected unit disk graph (UDG) G=(V,E), where V is the set of N nodes and where any node pair i, j is connected if Euclidean distance between two nodes is less than or equal to transmission range. Since each sensor node has same transmission range and only the neighbor nodes within transmission range can receive its message.

B. Attacker model

We consider a basic attacker model in this paper specifically. We provide a solution framework towards the basic attacker model theoretically.

1) Basic attacker model

Conventional reactive jammers [4] are defined as malicious devices, which keep idle until they sense any ongoing legitimate transmission and then emit jamming signals (packets or bits) 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 will be stopped(called jammer sleep period).

a) Jamming range

Jammer node is also equipped with omnidirectional antennas with uniform power strength on each direction. The jamming area can be regarded as a circle centered at the jammer node, where jamming range must be greater than the sensor transmission range, for simulating a powerful and efficient jammer node.

b) Triggering range

On sensing an ongoing transmission, the decision whether or not to launch a jamming signal depends on the power of the sensor signal, arrived signal power at the jammer and power of the background noise.

c) Jammer distance

Any two jammer nodes are assumed not to be too close to each other, i.e. the distance between any two jammers must be greater than their jamming range.

C. Sensor model

Each sensor in the network sends a status report message to the base station, which includes a header and a main message body containing the monitored results battery usage and other related content as shown in the figure 1.

V1 Sourc eID	0950 Times tamp	Victim Label	30 TTL	…….. Main msg body

Fig 1. Sensor periodical status report message

The header of the status report message contains 4 tuples

- sensor_ID: ID of the sensor node (which is unique for all sensor nodes).
- Time_Stamp: the sending out time indicating the sequence number.
- Label: this field refers to the current jamming status of the network.
- TTL: time to live field which is initialized to 2D, where D is the diameter of the network.

According to the jamming status all the sensor nodes in the network are classified into four types:

Trigger nodes (TN), Victim nodes (VN), Boundary nodes (BN) and Unaffected nodes (UN). Trigger nodes refer to the sensor nodes whose signals awake the jammer. Victim nodes are those within a distance R from an activated jammer and distributed by the jamming signals.

IV. PROPOSED SYSTEM

In this section we are trying to deactivate the jammer nodes when we identify the trigger nodes in network. This concept makes use of the already existing trigger identification service [8] to identify the trigger nodes, whose transmission invokes the jammer node. The proposed system for deactivating the jammer node use light weight procedure to deactivate. The procedure makes use of status report message (which have the same fields which we declared in the sensor model) to deactivate jammer. The assumption what we made here is that the base station knows the geographical location of the sensor node in the network. The procedure to deactivate the jammer is explained below.

Once the trigger nodes are identified by the base station, all these nodes (trigger nodes) are then instructed to abstain from participating in the transmission process and go to sleep instead, and to periodically wake up and send out a dummy signal so as to trigger the jammers interference phase. Next the victim nodes are instructed to go to sleep for a configurable length of time, so that no energy is wasted in retransmission requests and also the neighbors of the victim nodes (who are not trigger nodes or not themselves victim nodes) are instructed to use a fallback or alternative routing table that is constructed without using any victim or trigger nodes for the entire length of this time. After some period of time, the jammer node exhausts its energy and die, while the trigger node expends minimal amount of energy. When the trigger node detects that there is no jamming occurs when it sends out the fake signal, then it sends a report to the base station to request that it should be added back as a component node into the routing process of the network.

V. ANALYSIS OF TIME AND MESSAGE COMPLEXITY

In this section we compare the time and message complexity of the proposed system with the Ying Xuan, Yilin Shen system for trigger identification [8].

- Time complexity: Time complexity of our system is also approximately same compared with the trigger identification scheme proposed by Ying Xuan, Yilin Shen.
- Message complexity: Message complexity of our system is same compared with the trigger identification scheme proposed by the Ying Xuan, Yilin Shen, since our system does not uses any other message overhead technique to make reuse of sensor nodes in the network.

VI. RESULTS

In this section we consider the energy constraint of the sensor node against the normal sensor working with jammer and without jammer in an NS2 platform.

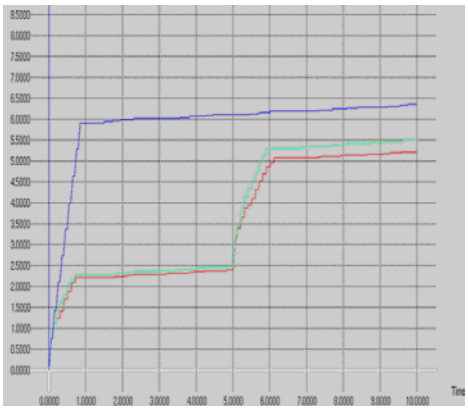

Fig: 6.1. energy utilization graph

From the above graph we can notice the energy utilization of the sensor node in the sensor network.

The below line which we see in the above graph indicates that the energy utilization of the sensor node in normal packet transmission without any jamming. The mid line in the above graph indicates that the energy utilization of the sensor nodes in packet transmission,by deactivating the jammer node in the network.the above line indicates the energy utilization of the sensor nodes under jamming condition.

VII. CONCLUSION

In this paper, we added a trigger node reuse concept to the trigger node identification service, to overcome the drawback present in the trigger node identification service. Our scheme reuses the identified trigger node in the actual application after deactivating the jammer node in the network. We can say that the proposed scheme efficiently make use of energy to deactivate the jammer node.

REFERENCES

[1] D. Z. Du & F. Hwang, pooling designs: Group testing in molecular biology. Word scientific 2006.

[2] R. Gupta, J. Walrand & O. Goldschmidt, “Maximal clique in unit disk graphs: polynomial approximation,” proceedings international network optimization conference (INOC), 2005.

[3] M. Strasser, B. Daner, & S. Capkun,“Detection of reactive jamming in sensor networks,” ACM transaction, sensor networks, vol 7, pp. 1-29, 2010.

[4] W. Xu, K. Ma, W. Trappe, & Y. Zhang, “Jamming sensor networks: attacks and defense strategies,” IEEE network, vol 20, no 3, pp. 41-47, may/June 2006.

[5] I. Shin, Y.Shen, Y.Xuan, M.T.Thai, & T.Znati, ”Reactive jamming attacks in multi-radio wireless sensor networks: An efficient mitigating measure by identifying trigger nodes.” Proceedings 2nd ACM international workshop foundations of wireless adhoc and sensor networking and computing (FOWANC), in conjunction with mobihoc, 2009.

[6] M.Li, I.Koutsopoulos & R.poovendran, ”Optimal jamming attacks and network defense policies in wireless sensor networks.” Proceedings IEEE INFOCOM, 2007.

[7] M. Cakiroglu & A.T. Ozcerit, “Jamming detection mechanisms for wireless sensor networks.” Proceedings 3rd international conference. Scalable information systems (InfoScale), 2008.

[8] Ying Xuan, Yilin Shen, Nam P. Nguyen and My T Thai, “Trigger identification service for defending reactive jammers in WSN,” Proceedings IEEE International Conference on Mobile Computing, 2012.

[9] P.Tague, S.Nabar, J.A.Ritcey & R.Poovendran, ”Jamming-Aware traffic allocation for multipath routing using portfolio selection.” IEEE/ACM Transaction networking, vol 19, no 1, pp 184-194 Feb 2011.

[10] W.Hang, W.Zanji, & G.Jingbo, ”performance of DSSS against repeater jamming,” Proceedings IEEE 13th International conference Electronics, Circuits and systems (ICECS), 2006.

[11] A.D.Wood, J.Stankovic & S.Son, ”A jammed area mapping service for sensor networks,” proceedings IEEE 24th real-time systems symp (RTSS), 2003.

[12] V.Guruswami & C.P.Rangan, ”Algorithmic aspects of clique traversal and clique independent sets,” discrete applied math, vol. 100, pp 183-202, 2000.

[13] W. Xu, T. Wood, W. Trappe, and Y. Zhang, “Channel Surfing and Spatial Retreats: Defenses against Wireless Denial of Service,” Proc. ACM Workshop Wireless Security, pp. 80-89, 2004.

[14] K. Pelechrinis, I. Koutsopoulos, I. Broustis, and S.V. Krishnamurthy, “Lightweight Jammer Localization in Wireless Networks: System Design and Implementation,” Proc. IEEE 28th Conf. Global Telecomm. (GlobeCom ’09), 2009.

[15] R.A. Poisel, Modern Communications Jamming Principles and Techniques. Artech House, 2004.

[16] Z. Liu, H. Liu, W. Xu, and Y. Chen, "Wireless Jamming Localization by Exploiting Nodes' Hearing Ranges," Proc. Int'l Conf. Distributed Computing in Sensor Systems (DCOSS), 2010.