ISSN No. 0976-5697

Volume 8, No. 3, March – April 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Deactivation of Reactive Jammers in Wireless Sensor Networks

Supreetha Patel T P
Asst. Prof
Department of CSE
KIT, Tiptur
Karnataka, India

Pallavi R and Nandini P
Asst. Prof
Department of CSE
SVCE, Bengaluru
Karnataka, India

***Abstract*:** In latest days, reactive jamming assault has emerged as a first rate security risk to wireless sensor community. Several techniques are evolved to identify the cause nodes, whose valid transmission turns on any reactive jammer. After identifying the trigger node, the node will be close all the way 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 community. Since the node can't be used once more within the network it's far one of the most important disadvantage. Hence to triumph over the trouble, In this paper we propose a unique technique, in which the recognized cause nodes are installed to the scanning mode, in order that we are able to reuse the trigger nodes, after deactivating the jammer node in the network.

***Keywords*:** Reactive Jamming, Jamming detection, Trigger Identification, Scanning mode.

I. INTRODUCTION

During remaining decade, the security of wireless sensor networks has attracted several attentions, because of its huge packages in various tracking structures and vulnerability toward sophisticated wireless assaults. Among these attacks jamming attack, where a jammer node disrupts the message delivery of its neighbor sensor nodes with interference signals or packets has emerge as a crucial risk to the WSN's. However in Reactive jamming attack, wherein jammer nodes live quiet till an ongoing valid transmission (even has a single bit) is sensed over the channel emerged lately and requires stronger protecting gadget to become aware of and extra green detection scheme to deactivate it.

There are many current researches against the detection of reactive jamming and to become aware of the trigger nodes which causes jamming in the network. Several techniques are evolved to discover the trigger nodes [5] [2]. All those strategies specifically contain the manner for figuring out trigger node and after identity, a brand new routing direction would be built to avoid activating of any reactive jammers.

But for the Wi-Fi sensor networks building new routing route has grown to be overhead, since the battery usage ought to be efficient. We understand that the lifespan of such sensor network packages degrees from months to years and, given restrained power deliver of sensor nodes, locations excessive needs on the strength efficiency of the algorithms. In this paper, we in reality use a message alternate scheme to deactivate the jammers within the network.

In this paper, we use an software layer actual time cause-identity provider for reactive jamming in Wi-Fi sensor networks [WSN], which promptly offers the listing of trigger-nodes using a light weight decentralized algorithm, without introducing neither new hardware devices, nor extensive message overhead at every sensor node. After identity we positioned the recognized trigger node in the scanning mode there they emits the fake or beacon signals then jammer node thinks that the node is collaborating within the actual transmission. This forces the jammer node hold on emitting the jamming sign there via laborious the jammer node battery.

The simple concept of this paper is to first perceive the set of victim nodes inside the sensor community with the aid of investigating corresponding links packet delivery ratio and receiver sign strength then those victim nodes are grouped into more than one checking out teams. Once the organization checking out schedule is made at the bottom station and routed to all sufferer nodes, they then regionally conduct the test and identify them as a cause or non-trigger. The identity results can be stored locally for jamming localization manner. Then base station puts the diagnosed trigger nodes to the scanning mode. In this mode the trigger nodes ship beacon sign until the power of jammer node exhausts to deactivate it.

The rest of the paper is organized as follows. Section II offers a top level view of related paintings, which includes the method for identifying the cause nodes. In section III we explain our machine model. Then we explain the proposed machine in phase IV. We analyze the message and time complexity of the proposed method by evaluating with ying xuan's scheme in segment V. Lastly we conclude the paper in segment VI.

II. RELATED WORK

In this segment we present a number of the strategies which already exist to clear up the jamming inside the network and the manner for cause node identification carrier for identification of cause nodes.

All effective countermeasures against reactive jamming assaults include jamming (signals) detection and jamming mitigation. First aspect, detection of interference indicators from jammer nodes is nontrivial due to the discrimination between ordinary noises and adversarial alerts over risky Wi-Fi channels. Numerous tries are made to screen the essential communication associated items, consisting of receiver signal power(RSS), service sensing time (CST), packet transport ratio (PDR) in comparison with particular thresholds, which were hooked up from simple statistical methods and multimodal techniques[2][3]. By such schemes, jamming signals can be discovered, but to

discover the jammer nodes primarily based on these alerts is plenty greater complicated.

Secondly, various network diversities are investigated to provide mitigation solutions [6]. Spreading spectrum [3][7] making use of more than one frequency bands and MAC channels , more than one routing benefiting from multiple pre-decided on routing paths[4] are two desirable examples of them. However in this approach, the functionality of jammers is believed to be restricted and powerless to trap the valid visitors from the camouflage of those diversities. However due to the silent behavior of reactive jammers they've more power to destruct these mitigation strategies. A mapping carrier of jammed place has been presented in [8], which detect the jammed areas and advocate that routing paths prevent these regions. This works for proactive jamming, since all the jammed nodes are having low PDR and as a result incapable for dependable message put off.

The cause identity service [5] well-known shows top notch potentials to be advanced as reactive jamming protecting schemes. As an instance, with the aid of except for the set of cause nodes from the routing paths, the reactive jammers will must stay idle because transmissions cannot be sensed despite the fact that the jammers pass around and come across new sensor signals, the list of trigger nodes could be fast up to date, and so are routing tables. As every other instance, without earlier understanding of the numbers of jammers, the radius of jamming indicators and particular jamming behavior kinds, it's miles quite tough to discover the reactive jammers even the jammed areas are detected. However, with the cause nodes localized, we can narrow down the viable places of reactive jammers.

A. Trigger Identification Service

In this section we talk the manner for figuring out the cause nodes from the pool of sufferer nodes in the sensor networks. The technique of trigger node identity involves 3 principal steps. This process is mild weight considering that all of the calculation takes place at the base station, and the transmission overhead in addition to the time complexity is low theoretically guaranteed.

1) Anomaly Detection

Already we understand that each one the sensor nodes within the network periodically ship a standing report message to the bottom station. However once the jammers are activated by message transmission, the base station will now not get hold of those file from some sensors. By evaluating the ratio of received reports to predefined thresholds, the bottom station can for that reason determine if a jamming assault has befell in the community.

The status record message includes the label discipline primarily based on the jamming popularity. It can be described in 3 ways. Consider if any sensor node hears jamming indicators it will not attempt to ship the reputation document to the base station, but it updates its label area as victim node. Once the bottom station does no longer get message from that node for a period of length it declares it has a sufferer and placed it for the checking out. If any sensor node does now not hear jamming alerts and it may send its fame report to the bottom station then that node is taken into consideration as unaffected node. If any node does now not acquire ack from its neighbor on the next hop of the direction within a day out duration, it tries for two or extra retransmission. If no acknowledgements are received, it is quite possible that neighbor is a sufferer node then node updates label tuple as boundary node in its fame file.

2) Jammer Property Estimation

Here we estimate the jamming range and the jammed place as easy polygons, based at the places of the boundary and sufferer nodes.

3) Trigger Detection

The manner to come across the trigger node is as follows: The recognized sufferer nodes are grouped into the interference loose testing groups by way of the use of clique independent set that's called a maximum clique impartial set(MCIS) [1] [9]. Then the grouped checking out teams is in addition divided into testing agencies through using randomized disjoint matrix. Then base station sends the encrypted trying out time table message to all the recognized sufferer nodes. Boundary nodes preserve broadcasting to all of the victim nodes inside the predicted jammed place for a length. All the sufferer nodes regionally execute the trying out process and become aware of themselves as triggers or non-triggers.

SYSTEM MODEL

In this phase we provide an explanation for the consideration of the network. It includes community model, attacker version and sensor model.

A. Network model

The Wi-Fi sensor community in our hassle includes N sensor nodes every having the same transmission range and one base station (larger networks with a couple of base station can be break up into small ones to satisfy the model). Each sensor node is prepared with a globally synchronized clock, omnidirectional antennas, m radios for in general okay channels throughout the network wherein okay>m, for simplicity we modeled the taken into consideration network as a linked unit disk graph (UDG) G= (V,E), in which V is the set of N nodes and in which any node pair i, j is hooked up if Euclidean distance between two nodes is less than or same to transmission variety. Since every sensor node has same transmission range and most effective the neighbor nodes inside transmission range can acquire its message [10].

B. Attacker model

We keep in mind a fundamental attacker model on this paper particularly. We provide a solution framework towards the primary attacker model theoretically.

1) Basic attacker model

Conventional reactive jammers [3] are described as malicious gadgets, which maintain idle until they sense any ongoing legitimate transmission after which emit jamming alerts (packets or bits) to disrupt the sensed signal (called jammer awaken period), in place of the complete channel, because of this as soon as the sensor transmission finishes,

the jamming assault may be stopped (known as jammer sleep length).

a) Jamming range

Jammer node is likewise ready with omnidirectional antennas with uniform electricity power on each course. The jamming place may be appeared as a circle focused at the jammer node, wherein jamming variety must be extra than the sensor transmission range, for simulating a effective and efficient jammer node.

b) Triggering range

On sensing an ongoing transmission, the decision whether or no longer to release a jamming signal depends on the energy of the sensor sign, arrived sign strength on the jammer and energy of the heritage noise.

c) Jammer distance

Any jammer nodes are assumed now not to be too near every different, i.E. The distance between any two jammers must be greater than their jamming variety.

C. Sensor model

Each sensor in the community sends a standing record message to the bottom station, which incorporates a header and a prime message frame containing the monitored effects battery usage and different associated content material as shown in the fig 1.

V1	0950	Victim	30	……..

SourceID Timestamp Label 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 popularity all of the sensor nodes in the network are labeled into 4 sorts:
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.

III. PROPOSED SYSTEM

In this section we are seeking to deactivate the jammer nodes while we discover the trigger nodes in community. This concept uses the already present trigger identity provider [5] to become aware of the trigger nodes, whose transmission invokes the jammer node. The proposed gadget for deactivating the jammer node use mild weight process to deactivate. The process uses status file message (that have the same fields which we declared within the sensor model) to deactivate jammer. The assumption what we made right here is that the bottom station is aware of the geographical area of the sensor node within the network. The process to deactivate the jammer is explained underneath.

Once the trigger nodes are diagnosed by using the base station, these kinds of nodes (cause nodes) are then advised to abstain from taking part inside the transmission process and go to sleep as an alternative, and to periodically wake up and ship out a dummy sign so one can 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.

IV. ANALYSIS OF TIME AND MESSAGE COMPLEXITY

In this phase we examine the time and message complexity of the proposed gadget with the Ying Xuan, Yilin Shen device for trigger identity [5].

- *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.

V. CONCLUSION

In this paper, we introduced a cause node reuse idea to the cause node identification service, to overcome the disadvantage present in the reason node identification provider. Our scheme reuses the identified cause node inside the actual software after deactivating the jammer node within the network. We can say that the proposed scheme effectively employ strength to deactivate the jammer node.

VI. REFERENCES

[1] R. Gupta, J. Walrand, and O. Goldschmidt, “Maximal Cliques in Unit Disk Graphs: Polynomial Approximation,” Proc. Int’l Network Optimization Conf. (INOC), 2005.

[2] M. Strasser, B. Danev, and S. Capkun, “Detection of Reactive Jamming in Sensor Networks,” ACM Trans. Sensor Networks, vol. 7,pp. 1-29, 2010.

[3] W. Xu, K. Ma, W. Trappe, and Y. Zhang, “Jamming Sensor Networks: Attack and Defense Strategies,” IEEE Network, vol. 20, no. 3, pp. 41-47, May/June 2006.

[4] M. Li, I. Koutsopoulos, and R. Poovendran, "Optimal Jamming Attacks and Network Defense Policies in Wireless Sensor Networks," Proc. IEEE INFOCOM, 2007.

[5] Ying Xuan, Yilin Shen, Nam P. Nguyen and My T Thai, "Trigger identification service for defending reactive jammers in WSN," Proc. IEEE Int'l Conf on Mobile Computing. 2012.

[6] P. Tague, S. Nabar, J.A. Ritcey, and R. Poovendran, "Jamming-Aware Traffic Allocation for Multiple-Path Routing Using Portfolio Selection," IEEE/ACM Trans. Networking, vol. 19, no. 1, pp. 184-194, Feb. 2011.

[7] W. Hang, W. Zanji, and G. Jingbo, "Performance of DSSS Against Repeater Jamming," Proc. IEEE 13th Int'l Conf. Electronics, Circuits and Systems (ICECS), 2006.

[8] A.D. Wood, J. Stankovic, and S. Son, "A Jammed-Area Mapping Service for Sensor Networks," Proc. IEEE 24th Real-Time Systems Symp. (RTSS), 2003.

[9] V. Guruswami and C.P. Rangan, "Algorithmic Aspects of Clique-Transversal and Clique-Independent Sets,"Discrete Applied Math.,vol. 100, pp. 183-202, 2000.

[10] https://www.cise.ufl.edu/~yxuan/papers/ipccc.pdf