Detecting and Detaching Reactive Jammers in Wireless Sensor Network

Pvnm Karthik Kumar, P.Prasanna Murali Krishna

***Abstract:** In recent days, reactive enjoying strike has appeared as an exceptional security risk to wireless sensor network [WSN]. A few schemes are generated to acknowledge the trigger nodes, whose valid transmitting stimulates any reactive jammer. After identifying the trigger node, the node may likely be shut down to deactivate the jammer and its particular routing information is eliminated within the routing table, then the node cannot be employed again within the system. Because the node can't be used again in the community it is among the important downsides. Consequently to overcome the problem, Through this record we suggest a novel strategy, where the accepted trigger nodes are put directly into the checking mode, to ensure that we are able to re-use the trigger nodes, after deactivating the jammer node in the city.*

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

I. INTRODUCTION

Throughout last decade, the security of wireless sensor networks [WSN] has attracted several initiatives, due to the broad applications in various observation procedures and susceptibility towards sophisticated wireless attacks. Among these assaults jamming attack, where a jammer node disrupts the concept shipping of its neighbors sensor nodes with interference signals or packages has become a vital danger for the WSN's. There are many current studies against the recognition of reactive playing and also to decide the trigger nodes that causes jamming inside the device. All these schemes mostly include the procedure for distinguishing cause node and subsequent id, a brand new routing course may be built to prevent initiating of any reactive jammers. Since the battery usage should be successful, but, for the wireless sensor networks building new routing path is becoming overhead. We are aware of the lifespan of said sensor system programs ranges from months to years and, offered small power of sensor nodes, areas high demands in the energy efficiency of the computations. In this document, we only use the jammers to get deactivated with an email exchange scheme in the community. After identification we establish the recognized trigger node within the check mode there the forgery or beacon signals are emitted by them afterwards jammer node believes the node is engaging with within the authentic transmission. This forces the jammer node keep on emitting the playing signal there by tiring the jammer node battery.

Revised Manuscript Received on 30 November 2013.
* Correspondence Author

Pvnm Karthik Kumar, M.Tech in DECS Dept Of ECE, SGIT MARKAPUR, AP, India
Mr. P.Prasanna Murali Krish, Associate Professor Head of Dept, ECE, SGIT MARKAPUR, AP, India

The fundamental opinion of the document will be to first identify the array of victim nodes within the sensor network by examining radio signal strength and accompanying hyperlinks package delivery percentage then these victim nodes are collected into multiple screening teams. When the team testing application is sent to all casualty nodes and created in the base station, as a trigger or low trigger they afterwards locally run the test and determine them. The recognition results might be saved locally for playing localization procedure. Then base station places the identified cause nodes to the scan mode.

The remainder of the documents is structured as follows. Section II provides an overview of associated work, which features the procedure for specifying the trigger nodes. In section III our method model is described by us. Then we describe the system in section IV. We evaluate the information and time difficulty of the recommended strategy by evaluating with yingxuan's plan in section V. Finally we conclude the paper in section

II. RELATED WORK

Within this section we present a number of the methods which already exist to find out the playing within the community as well as the procedure for trigger node identification support for identification of trigger nodes.

All powerful countermeasures against reactive performing attacks contain jamming (signs) detection and jamming mitigation. By such strategies, jamming signals could be uncovered, yet to find the jammer nodes based on these types of signals is really a much more complicated. Secondly, different network diversities are investigated to furnish [9] to mitigation options. Spreading spectrum [4] [10] using Macintosh channels and numerous frequency teams, multiple routing profiting from pre - selected routing paths [6] are two cases of these. But within this technique, the ability of jammers is presumed to be small and helpless to catch the visitors from the camouflage of the diversities. However because of the habits of reactive jammers they will have more ability to destruct these mitigation techniques. A maps support of packed region was provided in [11], which discover the jammed areas and suggest that routing paths avoid these areas. This capabilities for pro-active jamming, since every one of the nodes are experiencing low PDR , therefore incapable for reputable message delay. The reason id service [8] exhibits excellent potentials to be created as reactive jamming protecting techniques. As another instance, without prior understanding of the numbers of jammers, the range of playing signals and unique jamming conduct sorts, it is rather hard to obtain the reactive jammers even the areas are detected.

Trigger Identification Service Within this area we discuss the process for determining the trigger nodes from the pool of casualty nodes in the sensor networks. The procedure of cause node identification involves 3 main steps. This procedure is light weight since all the calculation happens at the base station, as well as the transmission overhead as well as the time complexity is low theoretically guaranteed.

1) Anomaly Detection

Previously we understand that the entire sensor nodes in town occasionally deliver a status report information for the bottom stop. But when the jammers are triggered by information transmission, these statements will not be received by the base station from some sensors. By evaluating the percentage of obtained reviews to pre defined thresholds, the station may so determine whether a playing assault has occurred within the network. The position report information includes the tag subject in the basis of the status. It might be defined in three ways. It reviews it features a casualty and set it for the testing after the base station doesn't get tips with that node for an interval of length. Whether any sensor node won't notice jamming signals and it's able to supply its position statement for the base station subsequently that node is believed to be untouched node. If any node will not receive ack from its neighbors on the following hop of the trail within a period, it attempts for several retransmission. It is quite possible that neighbour is a target node afterwards node updates label tuple as border node in its position record, if no ack are obtained.

2) Jammer Property Estimation

Here we approximation the jamming range and the jammed area as effortless polygons, based on the locations of the limit and victim nodes.

3) Trigger Detection

The procedure to find the trigger node is as follows: The determined victim nodes are arranged into the interference free testing groups by using clique independent set that is referred to as a maximum clique independent set(MCIS) [2] [12]. Then grouped testing groups are further broken into testing organizations with randomized disjoint matrix. Then base station sends the protected testing schedule message to every one of the identified casualty nodes. Border nodes keep broadcasting to all of the victim nodes within the approximated packed region for a period of time. Most of the casualty nodes locally run the testing method and determine themselves as sparks or low triggers.

III. SYSTEM MODEL

In this segment we explain the consideration of the network. It consists of network model, assailant model and sensor model.

A. Network model

The wireless sensor network in our problem consists of N sensor nodes each having one base station and the same transmission range (bigger networks with numerous base station might be separated into small ones to fulfill the model). Each sensor node includes 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 just the neighbor nodes within transmission range can receive its message.

B. Attacker model

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

Basic attacker model Conventional reactive jammers [4] are described as malicious devices, which keep idle until they feel any ongoing valid transmission and then emit jamming signals (packets or bits) to interrupt the sensed signal (called jammer aftermath up period), alternatively of the entire channel, which means after the detector transmission finishes, the jamming attack will undoubtedly be stopped(called jammer sleep period).

a) Jamming range

Jammer node is, in addition, furnished with omnidirectional antennas with consistent electricity strength on every direction. The jamming place might be seen as a circle centered at the jammer node, where jamming range has to be greater compared to the sensor transmission range, for simulating a strong and efficient jammer node.

b) Triggering range

On feeling an on-going transmission, the choice whether or perhaps not to launch a jamming signal depends in the ability of the detector signal, arrived signal power in the power and jammer of the back ground noise.

c) Jammer distance

Any two jammer nodes are implicit not to be too close to each other, i.e. the detachment between any two jammers must be superiorto their jamming range.

C. Sensor model

Each sensor in the network sends a position report message to the base station, which consist of a header and a main message body enclosed the monitored results battery usage and other associated content as exposed in the figure 1.

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

Fig 1. Sensor periodical status report message

The header of the status account message contains 4 tuples

- Sensor ID: ID of the sensor node (which is exclusive for all sensor nodes).
- Time_Stamp: the sending out time Indicating the sequence number.
- Label: this field refers to the existing 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 confidential into four types:

Trigger nodes (TN), Victim nodes (VN), Boundary nodes (BN) and unaffected nodes (UN).

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Trigger nodes refer to the sensor nodes whose signals awake the jammer. Victim nodes are those within a detachment R from an activated jammer and disseminated by the jamming signals.

IV. PROPOSED SYSTEM

Within this part we are looking to de activate the jammer nodes when we recognize the trigger nodes in system. This theory uses the already-existing trigger identification assistance [8] to acknowledge the trigger the jammer node is invoked by nodes, whose transmission. Light-weight process can be used by the proposed program for deactivating the jammer node to deactivate. The process makes use of position report information (which have the same areas which we declared within the sensor design) to de activate jammer. The premise whatever we made here's the base station understands the geographic region of the sensor node in the program. The process to deactivate the jammer is explained below. Following the trigger nodes are based on the base station, all of the nodes (trigger nodes) are then advised to prevent participating within the transmitting procedure and get to sleep alternatively, and also to occasionally wake up and spread a dummy signal as a way to trigger the jammers hindrance phase. Then it transmits a report to the bottom station to request that it ought to be used rear for a element node into the routing process of the device, when the trigger node detects that there is no playing happens when it transmits out the tranny.

V. ANALYSIS OF TIME AND MESSAGE COMPLEXITY

Within this part we evaluate the message and time complexity of the proposed system with all the Ying Xuan, YilinShen system for cause identification [8].
Time complexity: Time complexity of our system is also, around same compared with the cause identification scheme proposed by Ying Xuan, YilinShen.
Message complexity:
uses any other message overhead technique to make reuse of sensor nodes within the network.

VI. RESULTS

In this section we consider the energy limitation of the sensor node against the normal sensor working with jammer and exclusive of jammer in an NS2 platform.

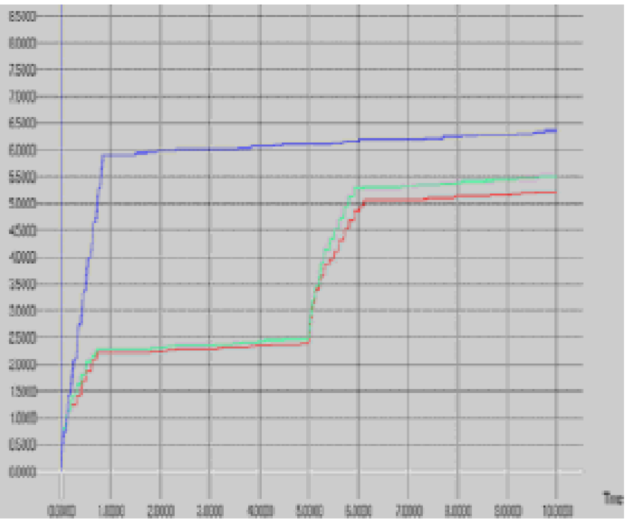

Fig: energy utilization graph

From the preceding graph we can notice the energy use of the sensor node in the sensor network. The below line which we see in the above graph indicates that the energy use of the sensor node in standard packet transmission without any jamming. The mid line within the aforementioned graph indicates the energy utilization of the sensor nodes in packet transmission, by deactivating the jammer node within the system. The preceding line indicates the power usage of the sensor nodes under jamming state.

VII. CONCLUSION

Within this paper, we added a trigger node re-use concept for the trigger node id service, to overcome the downside present within the trigger node identification service. Our program reuses the identified cause node within the program after de-activating the jammer node in the community. We might state the proposed scheme cheaply make use of electricity to de-activate 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, YilinShen, 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 24threaltime 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.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)