IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 1, March, 2013
ISSN: 2320 - 8791
www.ijreat.org

MOBILITY JAMMER IDENTIFICATION IN WSN

THENMOZHI A[1], BASKARAN G[2]

[1]student, Computer Science and Engineering, Srinivasan Engineering College, Perambalur, Tamil Nadu, India

[2] Assistant Prof., Information Technology, Srinivasan Engineering College, Perambalur, Tamil Nadu, India

Abstract

Jammer identification is a serious challenge in wireless sensor network. There are many systems to identify Jammers. Still Jammers attacks sensor networks much faster. So identification of fast mobile jammer is the main threat in WSN. Jammer is a transmitter mainly used for jamming signals. When new nodes enter to the sensor group in WSN, the initial routing process is performed for finding the desired node is jammer or non-jammer. After the identification it is decided for transmission. So here it will not allow any jammers to affect the data transmission in WSN. A new scheme called as debut node decentralization algorithm (DND) is proposed.
Trigger identification service for reactive jamming in wireless sensor networks is presented, which promptly provides the list of trigger nodes, without introducing new hardware devices. It is mainly used in military application.

Keywords: *jammer, trigger node, group testing, routing, non-jammer nodes.*

1. Introduction

The project is about jammer identification in mobility which comes under mobile computing. In wireless sensor network nodes are grouped and are provided with a single base station for each group, where the base station will collect all the information about the nodes that is whether it is jammer or not. It will also detect the jammer range up to which the data cannot be transmitted. When a new node enters to the group then that node can be easily identified by this base station.

Through the activity of those nodes it can be identified that the node can be used for transmission or not. When the nodes are identified it will decide the path to send the message, through this path the message can be transmitted.
Testing of nodes is normally done individually for all the nodes it may consume more time. Instead here nodes are grouped and are tested, so that time delay can also be minimized and it will reach the destination node correctly in time.

2. Problem Statement

The main problem is that the mobility in jammer. When jammer is in fixed location it can be easily identified, but while it is moving it cannot be detected easily.

Resolving the above problem is the proposed system that is the identification of moving jammer in wireless sensor network.

Initially the range of jammer during searching of nodes for identifying the node whether it is jammer or not, it will be difficult while searching each node individually.

So group testing is introduced (shown in figure 1) where some nodes are grouped and is allowed for searching. While it works for proactive jamming, all the jammed nodes are having low PDR and thus incapable for reliable message delay.

However, in the case of reactive jamming, this is not always the case. Only a proportion of these jammed nodes, named trigger nodes, whose transmissions wake up the reactive jammers, are blocked to avoid the jamming effects.

The expected lifespan of sensor network applications ranges from a period of time intervals is given with the limited power supply of sensor nodes, places high demands on the energy efficiency of the running algorithms.

3. WSN group

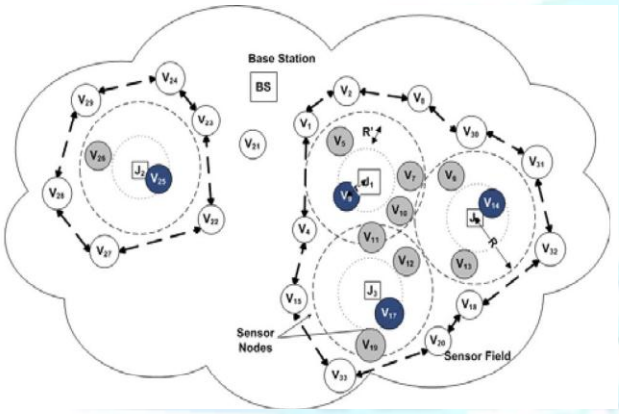

Figure 1 Nodes in grey and blue - victim nodes around jammer nodes, blue nodes are also trigger nodes, which invoke the jammer nodes. Nodes surrounding the jammed nodes are boundary nodes, while the others are unaffected nodes.

4. Existing System

The problem of localizing a jammer in wireless networks by hearing range based localization algorithm is that utilizes the changes of network topology caused by jamming to estimate the jammer's location [1]. The impact of a jammer and have shown the levels of the node's hearing range changes are determined quantitatively by the distance between a node to the jammer. Therefore, it can localize the jammer by estimating the new hearing ranges and solving a least-squares problem.

It does not depend on measuring signal strength inside the jammed area, nor does it require delivering information out of the jammed area. Thus, it works well in the jamming scenarios where network communication is disturbed. But this can be done for jammers which are stable in certain place. In existing algorithms, it cannot perform to locate the triggers in a fault tolerant environment and further identify the jammers by the locations. It also investigate the sufficient conditions for the existence of constructing routing algorithms where triggers as only receivers.

The problem of generating all maximal cliques in a UDG is considered here. General algorithms to find cliques in a graph are exponential, so it relies on a polynomial approximation [5]. Each edge and all maximal cliques with this are found to be the longest edge. Algorithm works by making certain key observations about the geometric structure of these graphs. Demerits of the existing system are reactive jammers can bring up larger damage due to efficient attack and hardness to detect [2].

The expected lifespan of sensor network applications ranges from a period of time intervals is given with the limited power supply of sensor nodes, places high demands on the energy efficiency of the running algorithms. A novel jamming detection scheme is the solution to these problems, but this scheme is able to identify the cause of bit errors for individual packets with high probability by looking at the received signal strength (RSS) during the reception of those bits.

5. Proposed System

A new scheme called as debut node decentralization algorithm (DND) is proposed for finding the new node joining to the sensor group. The identification of fast mobile jammer is the main threat in WSN.

When a new node enters to the sensor group in WSN it can be easily identified by the base station provided for that group. After finding the status of the node that is whether the node is jammer or not, the initial routing process is done. After the identification of path it is decided for transmission.

The application-layer real-time trigger identification service for reactive jamming in wire-less sensor networks, which promptly provides the list of trigger nodes using a lightweight decentralized algorithm, without introducing new hardware devices, nor significant message overhead at each sensor node.

Decentralized trigger-identification procedure is a lightweight in that all the calculations occur at the base station and the transmission overhead as well as the time complexity is low.

It uses error tolerant group testing with that nodes can be grouped and the nodes in that specified group can be easily identified by that base station along with their status like where the nodes are moving from and the status of that node, that is whether the node is jammer or not.
This group testing will detect the jammed area in order to send the data to the destination point without any disturbances and within time.

Thus after defending the jammer area it can choose the path where there is no threat due to mobile jammer.

5.1 DND Algorithm

Initially the nodes are checked, that is every node entering into WSN region.
Once the nodes are investigated the status of each node can be known.
Each node in the group is given with an id when it moves to other group then that node is once again given with a new id.
It will generate key for every node with group id.
Repeat the steps until every node in the network has been grouped.
After the identification of anomaly node alert message is sent to all the nodes about that node.
Certain range is chosen for those anomaly nodes. When a node enters into that area those nodes are said to be as victim nodes.
Those nodes are tested that whether the nodes are affected by the anomaly node or not.
If it is not affected then those nodes are identified to be an non –jammer node with which one can transfer the message through that nodes.

6. Conclusion

Nodes in the group are identified by the base station provided to that group. Base station will receive the status report of all the nodes with this it will find that the node is jammer or not. In order to provide an efficient trigger identification service framework, several optimization problem models and corresponding algorithms to them are provided, which includes the clique independent problem, randomized error tolerant group testing, and minimum disk cover for simple polygon. The proposed scheme debut node decentralization algorithm needs to be analyzed.

7. References

[1] Ying Xuan, Yilin Shen, Nam P. Nguyen, and My T. Thai, Member “A Trigger Identification Service for Defending Reactive Jammers in WSN” VOL. 11, NO. 5MAY 2012
[2] Shin .I, Y. Shen, Y. Xuan, M.T. Thai, and T. Znati, “Reactive Jamming Attacks in Multi-Radio Wireless Sensor Networks: An Efficient Mitigating Measure by Identifying Trigger Nodes,” Proc. Second ACM Int’l Workshop Foundations of Wireless Ad Hoc and Sensor Networking and Computing (FOWANC), in conjunction with MobiHoc, 2009.
[3] Liu .Z, 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.
[4] Liu .H, W. Xu, Y. Chen, and Z. Liu, “Localizing Jammers in Wireless Networks,” Proc. IEEE Int’l Conf. Pervasive Computing and Comm. (PWN), 2009.
[5] Gupta .R, J. Walrand, and O. Goldschmidt, “Maximal Cliques in Unit Disk Graphs: Polynomial Approximation,” Proc. Int’l Network Optimization Conf. (INOC), 2005.