Research Article Impact Factor: 0.621 ISSN: 2319-507X
Mangesh Bundele, IJPRET, 2014; Volume 2 (9): 279-283 IJPRET

INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

A TRIGGER IDENTIFICATION FOR DEFENDING REACTIVE JAMMERS IN WSN

MANGESH G. BUNDELE, N. S. KILLARIKAR

Department of Electronics & Telecommunication Engineering, Terna Engineering College, Nerul, Navi Mumbai, Maharashtra, India.

Accepted Date: 27/02/2014 ; Published Date: 01/05/2014

Abstract: In this project we are going to identify all the trigger nodes of reactive jammers and disable transmissions invoke the jammer nodes. This work as an application layer service. Three kernel techniques are used for proposed protocol. Error-Tolerant Randomized Non adaptive Group Testing, Minimum Disk Cover in a Simple Polygon, Clique-Independent Set. In Error-Tolerant Randomized Non adaptive Group Testing this technique is used to speed up the identification of affected nodes. In Minimum Disk Cover in a Simple Polygon we are going to find variable-radii in variable-radii. In Clique-Independent Set we are going to find to find a set of maximum number of pair wise vertex-disjoint maximal cliques, then we will identify the trigger nodes. And then we will apply solutions on attacks.

Keywords: RF: Data Availability, Problem Definition Methodologies

Corresponding Author: MR. MANGESH G. BUNDELE

Access Online On:

www.ijpret.com

How to Cite This Article:

Mangesh Bundele, IJPRET, 2014; Volume 2 (9): 279-283

PAPER-QR CODE

INTRODUCTION

A wireless sensor network (WSN) consists of spatially Distributed autonomous sensors to Monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. Jamming technologies have existed ever since wireless communications began. One of the most effective jamming technologies is jamming. This is the method of jamming only when the channel is occupied, therefore it is more energy efficient and harder to detect and compensate against. Existing countermeasures against Jamming attacks consist of jamming (signal) detection and jamming mitigation. On the one hand, 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 to this end monitored critical communication related objects, such as Receiver Signal Strength (RSS),

Carrier Sensing Time (CST), Packet Delivery Ratio (PDR), compared the results with specific thresholds, which were established from basic statistical methods and multimodal strategies. By such schemes, jamming signals could be discovered, but to locate the jammer nodes based on these signals is much more complicated and has not been settled.

II. Data Availability (Replica)

Jamming technologies have existed ever since wireless communications began. One of the most effective jamming technologies is jamming. This is the method of jamming only when the channel is occupied, therefore it is more energy efficient and harder to detect and compensate against. There are many commercial and military applications and several methods to implement to technology.

Primarily military in nature, jamming technologies have proved invaluable on the battle ground as well as beneficial to anyone interested in securing wireless transmission by blocking anyone attempting to listen in. Military uses of jamming have recently played a huge role in preventing the detonation of improvised explosive devices (IEDs) in the Middle East. The jammers are able to detect the detonation command and block the transmission before the signal is able to detonate the IED . Currently reactive jamming is not available to most consumers. The technology is usually only utilized in military applications. Traditional and cheaper constant jammers tend to fulfill the needs of consumer and other commercial interests despite the fact they cause unwanted interference and are less spectrally efficient. In order for reactive jamming to be effective, the signal must be processed in real-time and the jammer must be

activated in microseconds. Any longer and a modern day frequency hopping system will be able to successfully communicate through the jamming. Microprocessors and real-time DSP algorithms must work quickly enough to activate the jammer yet still work efficiently enough to determine the difference between a legitimate signal and an unwanted signal.

III. PROBLEM DEFINITION

3.1 EXISTING SYSTEM:

Existing system also consist of jamming detection and jamming mitigation techniques against jammers. Detection of interference signals from jammer nodes is nontrivial due to the discrimination between normal noises. By this technique jamming signals can be discovered but jammer nodes are complicate to locate and due to the silent behavior of reactive Jammers, they have more powers to destruct these mitigation methods.

3.2 PROPOSED_SYSTEM:

Proposed system provides lightweight decentralized algorithm for trigger nodes. It identifies the victim nodes by investigating PDR and RSS. It uses two solutions to stop the attacks. By applying this solution this system overcomes the limitations of existing system.

IV. METHODOLOGIES

4.1 Error-Tolerant Randomized Non adaptive Group Testing:

Error-Tolerant Randomized Non adaptive Group Testing has been developed to test on large populations. The key idea of group testing is to test items in multiple designated groups, instead of individually. Traditional method of grouping items is based on a designated 0-1 matrix.

4.2 Minimum Disk Cover in a Simple Polygon:

Given a simple polygon with a set of vertices inside, the problem of finding a minimum number of variable-radii disks that not only cover all the given vertices, but also are all within the polygon, can be efficiently solved.

4.3 Clique-Independent Set:

Cliques-Independent Set is the problem to find a set of maximum number of pair wise vertex-disjoint maximal cliques, which is referred to as a maximum clique-independent set. Since this

problem serves as the abstracted model of the grouping phase of our identification, its hardness is of great interest in this scope.

4.4 Anomaly Detection

The base station detects potential reactive jamming attacks, each boundary node tries to report their identities to the base station. The base station waits for the status report from each node in each period of length. If no reports have been received from a node v with a maximum delay time, then it will be regarded as victim.

4.5 Jammer Property Estimation:

In this technique the base station calculates the estimated jammed area and jamming range R based on the locations of boundary nodes.

4.6 Trigger Detection:

In this technique base station short encrypted testing message and broadcast it to all boundary nodes. Then boundary nodes broadcast the message to jamming nodes for some period. And after that all the victim nodes executes the testing procedure.

V. CONCLUSION

In this project we have created application which will find out the reactive jammer nodes in wireless sensor network. Application uses decentralized algorithm with several other techniques. The system has been tested under all criteria. In this technique base station short encrypted testing message and broadcast it to all boundary nodes. Then boundary nodes broadcast the message to jamming nodes for some period. And after that all the victim nodes executes the testing procedure.

REFERENCES

1. D.Z. Du and F. Hwang, Pooling Designs: Group Testing in Molecular Biology. World Scientific, 2006.

2. M. Goodrich, M. Atallah, and R. Tamassia, “Indexing Information for Data Forensics,” Proc. Third Applied Cryptography and Network Security Conf. (ACNS), 2005.

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

4. O. Sidek and A. Yahya, "Reed Solomon Coding for Frequency Hopping Spread Spectrum in Jamming Environment," Am. J. Applied Sciences, vol. 5, no 10 ,pp. 1281-1284, 2008.

5. Sharir, "Optimal Cover of Points by Disks in a Simple Polygon," Proc. 18th Ann. European Symp. Algorithms, 2010.

6. J. Cao, Y. Zhang, G. Cao, and L. Xie, "Data Consistency for Cooperative Caching in Mobile Environments," Computer, vol. 40, no. 4, pp. 60-66, Apr. 2007.