FRAMEWORK FOR JAMMER DETECTION IN CLUSTERED WIRELESS SENSOR NETWORKS

Riya Sara Xavier[1]

[1]*Department of Computer Sci. & Engg, Thejus Engineering College, Vellarakkad, Thrissur, Kerala, India*

***

Abstract - *Sensor networks are enormously used in numerous applications from military to health care. As sensor nodes operate at a very low radio power and utilize limited communication range it is vulnerable to jamming attacks. Here, a framework is proposed to detect the intrusion of jammer and the presence of jamming in a clustered wireless sensor network. The framework works in three aspects: when a cluster head receives a packet it begins by confirming whether the source node is a legitimate node, new node, or a jammer node. The moment, when the source node is pronounced as a new one in the first step, at that point the system approves whether the new node is legitimate node in the previous cluster or a jammer node by using cluster head code. Finally, the system watches the behavior of the recently joined nodes and the existing nodes to identify whether the nodes within the cluster are jammed or not. Furthermore, it also classifies the type of jammer, in the event that the presence of jamming is detected. The proposed system performs extremely well and achieves high jamming detection rate.*

Key Words: **Wireless Sensor Networks, Jamming, Jammer.**

1. INTRODUCTION

A Wireless Sensor Network (WSN) is a kind of network that incorporates an expansive number of circulating, self - directed, miniature, moo fueled gadgets called sensor nodes. These systems certainly cover a large number of spatially disseminated, small, battery-operated, embedded devices that are organized to collect, prepare, and exchange information and it has capabilities of computing and processing. The sensor nodes work in an infrastructure less and powerfully changing environment and course the collected information to the destination node for further elucidation. In a clustered wireless sensor networks, nodes are divided into clusters. Clustering is a two-layer hierarchy where the cluster heads (CHs) frame the higher layer and cluster members (CMs) frame the lower layer. Communication among CMs is carried out through CH and communication among CHs is carried out through the base station (BS). The CM may take off from a cluster and connect in another cluster, and a new node may join in a cluster. The benefits of clustering include achieving energy productivity by reclustering, diminishing collision, reducing the communication overhead, improving throughput, and network lifetime. Jamming attack may be a genuine security danger in wireless sensor networks. The jammers objective is to anticipate the communication between sensor nodes or degenerate true blue transmissions of sensor nodes by causing purposefulness packet collisions at the medium. Therefore, wireless sensor systems are appropriate in their look for jammers. In this paper the main focus is on detecting the entry of jammer and jamming in a cluster. To get an idea of jammer intrusion detection, it is assumed that a genuine member moves from one cluster to another cluster. At this point, the jammer impersonates as an authentic part and enters into a new cluster posing to be as legitimate member. In order to identify jamming within the network (to identify whether the cluster members are jammed or not), a mechanism is needed to monitor the behavior of the cluster members periodically and also determine the type of jammer.

2. LITERATURE REVIEW

[1] Explains a boundary node selection threshold (BNST) algorithm to choose nodes, to track jammers by estimating signal-to-noise Ratio (SNR), jammer-to-noise ratio (JNR), and jammer received signal strength (JRSS). A node can become a boundary node by comparing the SNR threshold, the average SNR estimated at the boundary node, and the received BNST value. The algorithm works in three steps. Within the first step, the most extreme distance between two jammed nodes is found. Following, the greatest distance between the jammed node and its unjammed neighbors is computed. At last, maximum BNST esteem is estimated.

[2] Recognizes the node's maliciousness level for securing WSN's from jamming attacks The System identifies the maliciousness level utilizing Packet Delivery Ratio. First, it secures the network from those outside nodes that are already reported as jammers. Secondly, it recognizes those nodes that are becoming an adversary.

[3] Explains a mechanism to detect jamming attack in three ways. It begins by updating the jammer to incorporate versatile military jammers; next, it graduates from the existing node-centric framework to the network-centric framework making it strong and economical at the nodes, and finally, it tackles the issue through fuzzy inference system, as the choice with respect to intensity of jamming is at times crisp.

[4] Explains the characteristics of modern WSNs that make them helpless to jamming attacks, along with the different sorts of jamming which can be exercised against WSNs. Common jamming strategies and an outline of different sorts of jammers are looked into and commonplace countermeasures against jamming are analyzed. Countermeasures are classified into proactive, reactive, and mobile agent- based countermeasures. The role of proactive countermeasures is to make WSN immune to jamming attacks instead of reactively react to such incidents. The fundamental characteristic of reactive countermeasures is that they empower response as it were upon the occurrence of a jamming attack, detected by the WSN nodes.

[5] Here the author explains two jamming detection algorithms. The fundamental algorithm is referred as basic jamming detection mechanism, in which bad packet ratio, packet delivery ratio, and energy consumption metrics are used to determine the existence of jamming. In order to determine this, these metric values are compared with their corresponding thresholds. Secondary algorithm referred as advanced jamming detection mechanism uses additional variables and flags in order to improve the fundamental algorithm in detecting jamming attacks.

3. METHODOLOGY

Jamming attack is a serious security threat for sensor networks, thus a framework is proposed for clustered wireless sensor networks. The framework is implemented in all CH or BS. It employs a CH centric approach, which implies all the decision making and processing is done by the CH. When this framework receives a packet, then it detects whether the source node is a legitimate node or jammer node or new node using three steps namely:

(1) Verification
(2) Validation and
(3) Auditing

The primary thought of the framework is to perform both jammer intrusion detection by using verification and validation, and jamming detection using auditing. Each CH should maintain look-up tables for verification, validation, and auditing. The look-up tables utilized within the system are cluster member and head (CMH) table, jammer table, Cluster head code (CHC) table. These look up tables are kept inside a data bank. The CMH table consists of Node ID and node type. The node ID represents the identity (address) of the nodes. Node type represents the type of the source node (CH, CM, or BS). The objective of this table is to determine the type of the source node. The Jammer table includes S.No. and node ID. The S.No. represents the entry number. The node ID represents the identity (address) of the jammer node. The source node is declared as jammer node, if address of the source node is found in the jammer table. The CHC table is formed by two fields namely, cluster heads and CHC. The cluster heads field denotes the CHs available in the network. The CHC represents each CH's CHC. This table is used by each CH to authenticate the source node, when a source node moves from one cluster to the other or when a source node wishes to join in a cluster.

3.1 Verification

The responsibility of verification is to detect the jammer intrusion in the cluster based WSN. Verification step is the first step of the framework. This step is responsible for making decision about whether the source node is a legitimate node, a new node, or a jammer node. The verification step refers to the CMH table and jammer table. If the source node is authorized as a legitimate node by the framework (that is the node details is found in the CMH table), then the framework proceeds with auditing step. Or else, if the source node is found in the jammer table, then the framework declares the source node as the jammer node. Otherwise, the framework declares the source node as a new node (source node is not found in both the tables) and proceeds with the validation step.

3.2 Validation

The validation step is equally responsible in detecting the entry of a jammer. This step has to authenticate whether the new node belongs to any of the available CH or not. Validation is used as security mechanism to perform authentication. For this, validation step uses the cluster head code (CHC). CHC is simply a random sequence number periodically generated by the CH for each of its CMs and stored in the CHC table. In order to provide the generated CHC to all its members, CH broadcasts a beacon frame to its members. If a source node is declared as a new node, then the CH demands CHC from the source node by sending beacon frame. The source node replies with its CHC. Now, the CH compares the received CHC against the entry available in the CHC table. If the received CHC is matched with an entry available in table, then the source node belongs to the available CHs. Otherwise, the source node is declared as a jammer node. Then, it proceeds with the auditing step, as the newly joined node or the existing node in a cluster has a chance to become a jammer node in the future.

3.3 Auditing

The auditing step is responsible for monitoring the behavior of existing members and a newly joined member. The auditing step decides whether the newly joined member or existing members are in normal state or unusual state depending on their behavior. For this it uses two jamming detection metrics such as packet delivery ratio (PDR) and received signal strength indicator (RSSI). The CH estimates these metrics and makes decision about whether a node is jammed. The PDR is defined as the ratio of the total number of packets successfully sent by the node to the total number of packets sent by the node. The RSSI is defined as the ratio of received signal strength to the reference power. Jamming detection level is bounded by threshold values of PDR and RSSI. That is, if PDR decreases below a given threshold value and RSSI is higher than its threshold value, then it can be ascertained that the jamming is present. Predicting this PDR and RSSI threshold is a crucial task in WSN. In this paper, appropriate statistical test (T test) is carried out to find and fix the threshold values. T test is performed on the two sets that are related in certain features, it is used to determine if there is a significant difference between the means of two sets. Here, we consider a PDR or RSSI without jamming and a PDR or RSSI after launching jamming. The mean of their values are computed and the PDR and RSSI thresholds are set accordingly. However, it is not sufficient to determine the presence of jamming alone, further it is necessary to determine the type of jamming launched. Here, jammers are classified into two types: high intensity jammers and low intensity jammers. High intensity jammers continuously jam the communication channel by sending packets or random bits whereas low intensity jammers occupy the communication channel or jam the channel by sending packets or random bits at regular time intervals.

In this paper, the detection of sensor nodes is classified into (i) true detection, (ii) false detection, and (iii) undetection. The true detection is defined as CH that accurately detects the member as jammed. The false detection is defined as CH that wrongly detects the member as jammed though that member is a normal node. The undetection is defined as CH that wrongly detects the member as normal although the member is actually jammed. Or simply stating a jammed node is not detected by the CH. For a fair jamming detection system, the TDR must be equal to 1 and FDR and UDR must be equal to 0.

4. CONCLUSIONS

The framework has considered the issue of jammer intrusion detection in sensor networks, which is not for the most part tended to by the conventional detection methods. The proposed system consists of three key elements, firstly the metric PDR is combined with the metric RSSI for jamming detection; furthermore statistical tests are performed to find out the threshold of detection metrics and to classify various types of jamming; and finally a three-step framework is utilized to detect both jammer intrusion and jamming. The framework has a high true detection rate whereas the false and undetection rates are negligible. Also by using this framework for jammer detection in clustered wireless sensor network, the communication overhead is reduced since cluster head by itself directly estimates the metrics for processing and decision-making (CH does not depend on its member). Therefore, it can be claimed that the cluster member is not burdened that is it is not loaded heavily. In Jammer detection framework a new node may join in a cluster or an existing node may leave from a cluster. Therefore, it supports mobility.

REFERENCES

[1] Waleed Aldosari and Mohamed Zohdy, " Tracking a Jammer in WSN and selecting boundary nodes by estimating signal-to-noise ratios and using an extended Kalman Filter" Department of Electrical and Computer Engineering, Oakland University, USA; 8 October 2018.

[2] K.P Vijaykumar, P. Ganeshkumar, M.Anandaraj, "Jamming Detection System in Wireless Sensor Networks", IJARCET, April 2014 R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[3] S Misra, R Singh, SVR Mohan, "Information warfare-worthy jamming attack detection mechanism for wireless sensor networks using a fuzzy inference system". Journal of Sensors, 2010.

[4] A Mpitziopoulos, D Gavels, C Konstantopoulos, G Pantziou, "A survey on jamming attacks and countermeasures in WSNs". IEEE Commun. Surv.Tutorials, 2009.

[5] M Cakiroglu, AT Ozcerit, "Jamming detection mechanisms for wireless sensor networks". ICST, Belgium, 2008.