A NOVEL JAMMING AND JAMMER INTRUSION DETECTION SYSTEM FOR WIRELESS SENSOR NETWORKS

A THESIS

Submitted by

VIJAYAKUMAR K P

in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

FACULTY OF INFORMATION AND COMMUNICATION ENGINEERING

ANNA UNIVERSITY

CHENNAI 600 025

NOVEMBER 2016

ABSTRACT

Sensor networks are usually composed of tiny sensor nodes which consist sensing, computing, communicating components and memory. These nodes are deployed in a region called sensor field to sense the environment. Wireless sensor networks (WSNs) are becoming increasingly attractive in numerous application areas ranging from military to healthcare. Sensor nodes have very limited memory space, energy, and computational power. These nodes work in an infrastructureless and dynamically changing environment and route the collected data to the sink node for further interpretation.

There are several attacks in the sensor networks that are categorized into routing attacks and data traffic attacks. The data traffic attacks are classified into jamming, wormhole, selective forwarding, sinkhole and sybil attack. In data link layer, the sensor network is vulnerable to jamming and energy-exhausting attacks, because the sensor nodes use wireless medium for data communication and operate at a very low radio power. The jamming attacks are launched by the jammers. The jammers aim to disturb the communication among sensor nodes or corrupt legitimate transmissions of sensor nodes by causing intentional packet collisions at a medium. Jamming attacks may be viewed as a special case of Denial of Service (DoS) attacks. Hence a mechanism is needed, to detect various types of jamming attacks and to detect the intrusion of jammer (a node which performs jamming activity).

The main objective of this thesis is to present a novel jamming and jammer intrusion detection system for WSN to detect the presence of jamming and detect the intrusion of jammer in the WSN. The proposed system uses two jamming detection metrics such as packet delivery ratio (PDR), received signal strength indicator (RSSI) for detecting the presence of jamming and intrusion or entry of jammer in the cluster based wireless sensor networks

(CWSN) for downstream data communication by using cluster head code (CHC). This thesis proposes four novel jamming detection systems and jammer intrusion detection system.

First, a novel jamming detection technique (JDT) to detect the presence of jamming in the downstream direction for CWSN is proposed. The proposed technique is deployed in base station (BS) and in cluster heads (CHs). The proposed technique is novel in two aspects: Firstly, whenever a CH receives a packet, it verifies whether the source node is a legitimate node or a new node. Secondly, if a source node is declared as a new node in the first step, then the JDT observes the behavior of the new node to find whether the new node is a legitimate node or a jammed node. In order to monitor the behavior of the existing node and a new node, the second step of JDT uses two metrics namely PDR and RSSI. The metrics PDR and RSSI of every member in the cluster is measured and assessed by the CH. And finally the CH determines whether the members of the cluster are jammed or not. The CH can detect the presence of jamming in the cluster at the member level. The BS can detect the presence of jamming in the WSN at CH level. The simulation result shows that the proposed technique performs extremely well and achieves jamming detection ratio as high as 99.85 percent.

Second, a novel jammer detection framework (JDF) is proposed to detect various jamming attacks and jammer intrusion in CWSN. Jammer intrusion detection and jamming detection are two separate issues. In the proposed system, a novel jammer detection framework to detect the intrusion of jammer and the presence of jamming in a CWSN is proposed. The proposed framework is novel in three aspects: whenever the CH receives a packet, it first verifies whether the source node is a legitimate, a new node or a jammer node. Second, when the source node is declared as a new one in the first step, then the JDF validates whether the new node is a legitimate node in the previous cluster or a jammer node by using CHC. Third, the JDF observes

the behavior of the newly joined node and the existing nodes to identify whether the nodes in the cluster are jammed or not. Additionally, it also classifies the types of jamming, if the presence of jamming is detected. Simulation result shows that the proposed framework performs extremely well and achieves jamming detection ratio as high as 99.88 percent. Finally, the analyses on energy consumption during normal scenario, during jammer intrusion detection, and during jamming detection are carried out.

Third, the fuzzy logic based jamming detection algorithm (FLJDA) is proposed to detect the presence of jamming in CWSN. The FLJDA keeps an eye on the existing nodes and a new node to determine their behavior by applying fuzzy logic. In order to monitor the behavior of the nodes, the FLJDA computes the jamming detection metrics namely PDR and RSSI for detecting the presence of jamming. The CH detects the presence of jamming in the cluster at a member level. The BS detects the presence of jamming at the CH level. Therefore all the sensor nodes are employed with fuzzy logic based jamming detection algorithm. The fuzzy logic is applied to identify the optimum level or range of the jamming detection metrics (PDR, RSSI) to figure out the presence of jamming correctly. The simulation results of the proposed system provide true detection ratio as high as 99.89 percent.

Fourth, the jamming detection approach based on fuzzy assisted multi criteria decision making system (JDA) is proposed to detect the presence of jamming in downstream communication for CWSN. The proposed approach is deployed in the CH. The JDA functions in two aspects: First, the CH periodically measures the jamming detection metrics namely PDR and RSSI of every node in the cluster to determine the behavior of the sensor nodes. In order to determine the behavior of members in the cluster, the CH compares the measured PDR with the PDR threshold. If the measured PDR is lesser than the PDR threshold, then the CH applies Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) method on the

PDR and the RSSI metrics to determine the presence of jamming. These metrics are considered as the criteria and the nodes or the members are considered as alternatives. Next, the fuzzy logic is used to optimize the result of TOPSIS and identify the presence or absence of jamming accurately. The simulation result shows that the JDA achieves detection ratio at 99.6 percent.

The performances of the proposed systems are evaluated and analyzed based on the simulations carried out by using the MATLAB 7.1 and Network Simulator-2 (NS2). This novel jamming and jammer intrusion detection system achieve an elevated scope for detection and classification of various types of jamming and detection of jammer intrusion in downstream communication for CWSNs.