Defending Reactive Jammer in WSN using A Trigger Identification Services
Harshad Shelar\textsuperscript{1} Jilani Momin\textsuperscript{2} Sainath Patil\textsuperscript{3} Kiran Jaybhaye\textsuperscript{4} Mr. Arun M. Hattarge\textsuperscript{5}

\textsuperscript{1,2,3,4,5}Department of Computer Engineering
\textsuperscript{5}D.C.O.E.R Pune, India

Abstract—This depicts that what we have to do in the above project. In the growing era of internet, today organisation has a big issue about sharing their information via shared network. Today’s era of internet, it is very sensitive to exchange information via a shared network for an organization. They must define their access control in terms of accessing network resources via a shared network. Growing era of internet people are trying to steal the data in many ways so it is necessary to send the data in an encrypted form via network so in the above project we tried to show that our approaches seamlessly integrates security mechanism with wireless sensor network to provide security with trigger identification.

Key words: Wireless Sensor Network (WSN), Jamming Techniques, Reactive Jamming, Trigger Identification

I. INTRODUCTION

Information technology has changed the way to exchange the information in past two decade. An organization ranging from business to government agencies, there is an increasing need to share their information across their inter-organization. For this, we need to make the data sharing much secured with the above concept.

Defending reactive jammer in wireless sensor network has come with a solution to implement the secured data transmission in a shared network. There is a network model, basic attacker model and advanced attacker model to implement information sharing via shared network. To address the need for data security we used to DBMS to manage data locally and provide unified data access.

In the context of sensitive data, we use a distributed system providing data access through a set of brokers called Information Brokering System (IBS).

II. THE PROBLEM

To identify the trigger nodes in the wireless sensor network and remove them in order to prevent the legitimate traffic from getting completely blocked.

III. JAMMING TECHNIQUES

The spot jamming technique involves a malicious node that directs all its transmitting power to a single frequency. It makes use of identical modulation schemes and less power to override the original signal. The assault on WSNs due to this attack is easily avoided by surfing to another frequency. In case of sweep jamming technique, the malicious node can jam multiple communication frequencies, but this jamming does not affect all the involved nodes simultaneously. The attack also lead to packet loss and retransmission of packet data that will increase consumption of energy in the network.

Fig 1: Different types of jamming technique

The above figure is an illustration of jamming techniques used in launch jammer attacks. In barrage jamming technique, the malicious code jams a group of frequencies simultaneously which decreases the signal-to-noise ratio of the destination node. This jamming technique increases the range of jammed frequencies and reduces the output power of the jammed node. Deceptive jamming has the capability to flood the network with useless data which can mislead the sensor node present in the network. The available bandwidth used by the sensor nodes is reduced.

The malicious node that make use of this technique do not reveal their existence.

Fig. 2: Jamming types

Figure depicts several types of jammers that may be used in the attacks against in the wireless sensor network namely constant jammer, deceptive jammer, random jammer, reactive jammer etc. The constant jammer emits uninterrupted radio signals in the wireless medium. They do not follow any underlying MAC protocol and include just random bits. This jammer keeps the channel busy and disturbs the communication between nodes. The deceptive jammer uses misleading jamming technique to attack the wireless sensor nodes. The random jammer sleeps for an indiscriminate time and wakes up to jam the network for an arbitrary time.
V. IMPLEMENTATION APPROACH USING TRIGGER IDENTIFICATION

In this procedure, the time complexity as well as the transmission overhead is low and it is lightweight so that all calculations occur at base station. No external hardware are required. Only the status report messages sent by sensor and the geographic locations of all sensors are maintained at the base stations.

The main steps in this procedure are as follows:

1) Jammer Property Estimation- In this base station calculates the jamming range and the estimated jammed area based on the boundary locations.

2) Trigger Detection-In this the short testing schedule where the broadcast nodes will be receiving the messages from the base stations Then the boundary nodes keep broadcasting to the entire node including the victim nodes which will be receiving the messages within the estimated jammed area for a period T. Then the victim nodes execute the short testing procedure based on the messages and a global uniform clock identify themselves as trigger or non-trigger.

3) Anomaly Detection-In this the potential of the reactive jamming attack is detect by the base station, where each boundary node tries to report their identities to the base station.

Algorithm: Trigger Nodes Identification Algorithm

/*All nodes in a group N synchronously performs the following to recognize trigger nodes in N.*/

1) INPUT: n victim nodes in a testing group

2) OUTPUT: all trigger nodes within these victim nodes

//In order to estimate d i.e. upper bound of error Set γ = (10t-8t² - t - d -1)/2;
//Likelihood for each test Set T=t in n (d+1)²/(t √ (d+1)) 2;

3) Construct a (d,z)- disjunct matrix using ETG algorithm with T rows, and divide all the n victim nodes into T group accordingly {g1,g2,.....,gt};

// Group testing will be done for each round on m groups using m different channels. Here testing can be done in asynchronous manner ,the m group tested in parallel need not wait for each other to finish the testing, instead any finished test j will trigger the test j+m, i.e, the tests are conducted in m pipelines.

4) for i= 1 to [t/m] do

5) Conduct group testing in group gim+1,gim+2,gim+m in parallel;

6) If any node in group gj with j [im+1,im+m] detects jamming noises, finish the testing in this group and start testing on gj+m;

7) If no nodes in group gj sense jamming noises, while at least one other test in parallel detects jamming noises,

8) All the nodes in group gj resend more messages to set off possible hidden jammers; If no jamming signals are detected till the end of the predefined round length (L)

9) Return a negative outcome for this group and start testing on gj+m;

10) End
VI. PERFORMANCE EVALUATION AND RESULT ANALYSIS

The result of these experiments show that this solution is time efficient for identifying trigger nodes and defending reactive jamming attacks. The trigger identification procedure for reactive jamming in network simulator NS2 on 900 * 900 square sensor field with n=10 sensor nodes has been simulated. The sensor nodes are uniformly distributed, with one base station and J distributed jammed nodes. In this work, the sensor transmission radius ‘r’ and jamming transmission ‘R’ as 2r has been considered to achieve better efficiency of the jamming model.

VII. CONCLUSION

In this paper, a novel trigger identification service for reactive jamming attack in wireless sensor network is introduced to achieve minimum time and message overhead. The status report messengers transferred between the base station and all sensor nodes. For isolating reactive jammer in the network a trigger identification service is introduced.

VIII. ACKNOWLEDGMENT

We would like to thank T. Yu, W.-C. Lee, P. Mitra and M. Rabinovich for valuable contribution on the project.

REFERENCES