International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 21 Issue 2 – APRIL 2016.

LOCALIZATION OF JAMMERS IN BROADCAST NETWORKS

Vidya Nanda Hruday Pidikiti, Mule Raja Sekhar Reddy, Vignesh KV, B Arbaz, Rajathi

Department of Computer Science and Engineering,SRM University, Chennai

***Abstract*--We consider the problem of jamming-immune broadcast communications under an internal threat model. TDBS does not rely on commonly shared codes, or the presence of jamming-resistant control channels for monitoring broadcasts. Instead, each node follows a unique pseudo-noise (PN) frequency hopping pattern. Contrary to conventional PN sequences designed for multi-access systems, the PN pattern in TDBS display association to enable broadcast. Considering the specific characteristics of reactive jammer nodes, a new strategy to shut down them by effectively recognising all trigger nodes, whose transmissions evoke the jammer nodes, has been suggested and implemented. Such a trigger-identification procedure can work as an application-level service and add as advantage to existing reactive-jamming resistant models. In this paper, on one side, we evaluate several optimization problems to provide a complete Triggers Identification and Jammer Location service framework for unreliable wireless sensor networks. Additionally, we provide a refined algorithm with regard to two sophisticated jamming models, in order to elevate its robustness for various network scenarios.**

Keywords: **Wireless sensor network, Jamming Techniques, Reactive jamming, Trigger identification, Trigger node.**

I. INTRODUCTION

Cost and Reliability are two major factors that need to be given major significance in message transmission between sensor nodes. Jamming attacks are usually implemented by set of nodes which performjamming, these are employed inside the wireless sensor network (WSN), and every node broadcasts interference signals toward its neighbour sensor nodes to distort their message delivery. It has become the critical threat component in WSNs that needs to be avoided, as it is responsible for the loss of data during transmission. Jamming is a light weight attack which does not require much of the network infrastructure information for its deployment. Specifically, based on the different attack strategies acquired, Jamming attacks are broadly divided as active Jamming and reactive Jamming [1]. Active jammer nodes always keep disrupting the authorisedcommunication via continuous unnecessary transmissions over the channels. On the other hand, reactive jammer nodes remain dormant till an ongoing transmission is sensed over the channel. These type of jamming attack can be easily put into effect but difficult to detect .The reactive jammers are activated when neighbour node starts to take part in communication. This node which is particularly responsiblefor the cause of reactive jammer to become active is referred to as trigger node. The effect of reactive jammers can be only controlled by identifying the trigger nodes and disabling them. The main idea of a jamming detection scheme is to design an algorithm to minimize the impact of reactive jammers on neighbouring nodes. An assumption that at least a part of all deployed nodes runs our detection algorithm and engages in jamming detection. Fallowing the detection of a jamming attack, the nodes raise a jamming alert message which is then either or reported to the network authority regarding the all trigger nodes in the network. By eliminating these nodes from transmission path the effect of jamming can be minimised.

II. ARCHITECTURE OF SYSTEM

Based on the categories of jamming attacks mentioned above, the reactive jamming is more devastative attack that should be taken care of. The paper takes into account the reactive jammer as it is responsible for disrupting the message delivery of adjacent nodes with strong interference signals. The outcome of the attack are increased energy consumption, disruption of routes extended packet delays, and loss of link reliability.

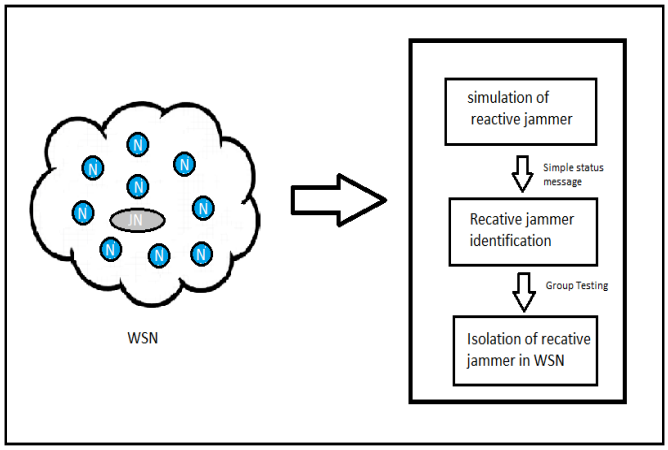


Fig 1: System Architecture

Thiswork shows system architecture for resistance against reactive jamming attack. The identification service framework starts off with the identification of boundary nodes which are the nodes that partiallycommunicate with its neighbors after finding the boundary nodes jammer region is evaluated. Next the testing schedule is performed in order to identify the trigger nodes each of the nodes undergo this trigger identification procedure to determine itself as a trigger node or non-trigger node. The trigger nodes are usually responsible for the activation of the jammers.

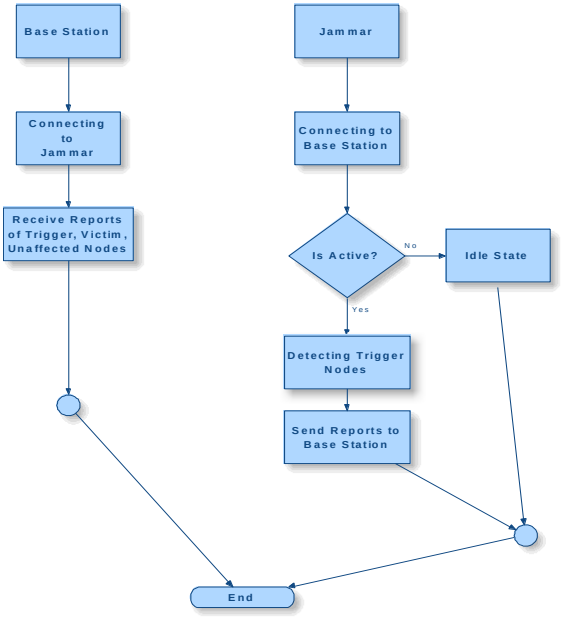


Fig 2: Dataflow diagram

III. SYSTEM MODELS AND NOTATION

A) Network Model

We assume a WSN comprising of n sensor nodes and one base station (larger networks with multiple base stations can be broken down into smaller ones to satisfy the model). Each sensor node is furnished with a globally omnidirectional antennas , synchronized time clock, m radios for in total k channels throughout the network, where k > m. For clarity, each direction is considered to have uniform power strength, so the range of transmission of individual sensor node can be taken as a fixed rs and the whole network as a unit disk graph (UDG) G ¼ ðV ;EÞ, where every node pair i; j is connected if the Euclidean distance between i; j: _ði; jÞ _ rs.

B) Attacker Design

Conventional reactive jammers are stated as destructive devices, which remain dormant till they detect any unauthorised transmissions in progress and then release jamming signals which is either packet or bit to interrupt the sensed signal (called jammer wake-up period), instead of the entire channel, which means once the sensor transmission finishes, the jamming attacks will be ceased (called jammer sleep period). Three concepts are proposed for the model to be completed.

Jamming Area

Denoted by R. equivalent to the sensors in WSN, jammers consists of omnidirectional antennas with constant power dissipation in all directions. The jammed region can be compared to that of the circle with jammer node at its centre and with a radius R, where R is assumed greater than rs, for imitating a most effective and efficient jammer node. Each and every sensor node lying inside this region will be jammed during the jammer wake-up period. R value can be related to depending on the boundary nodes position (whose neighbours are jammed but themselves not), and then further refined. Sensors within this range will be jammed during the jammer wake-up period. The value of R can be approximated based on the positions of the boundary sensors (whose neighbours are jammed but themselves not), and then further refined.

Triggering Circle

On hearing an ongoing transmission, the decision to initiate a jamming signal is based on the sensor signal power Ps, the power of arrived signal at the jammer Pa with sensor distance r, and the background noise power Pn.

Jammer distance

Jammer nodes are considered not close to each other, i.e., the distance between jammer J1 and J2 is _ðJ1; J2Þ > R. The assumptions are based on the fact that:

1) Jammers are usually employed to restrict the sensor nodes for communicating with the Base station if the jammer regions overlap the effectiveness of jammers decrease.

2) _ðJ1; J2Þ should be greater than R, because the jammer transmitted signal should not affect the signal reception of other jammer. Otherwise, the recent jammer will not able to correctly determine any sensor transmission signals, since they are usually combined with high RF noises, unless the jammer spends a lot of efforts in denoising to recognize.

3) Jammers communications are impractical, which will display anomaly detections at the network authority level of jammers.

D) Sensor Model

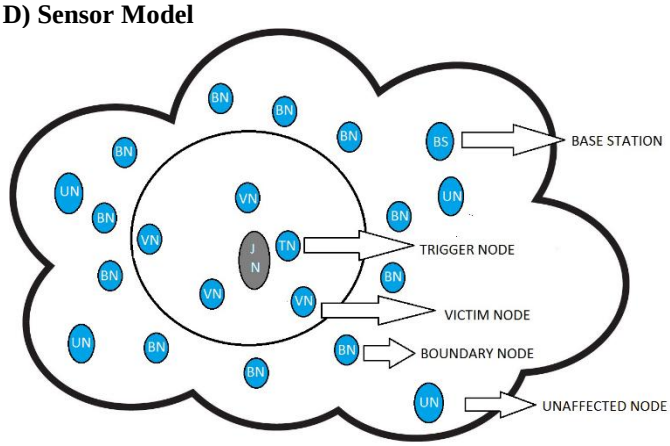


Fig 3: Categorization of Sensor Nodes

There exists three kinds of nodes in a jammed wireless networks. They are trigger node (TN), victim node (VN), boundary node (BN), unaffected node (UN)

E) Triggers Identification and Jammer Location

The process is broadly split into three main steps. The first step implements anomaly detection where the base station identifies threatening reactive jamming attacks. Each boundary node identifies itself to the base station. In the next step jammer property estimation is gauged where the Base station (BS) evaluates jamming region based on the boundary nodes location. The third step is trigger detection where the base station performs a short testing schedule by broadcasting message M to every boundary node in the network. Afterwards the boundary nodes keep jammed sector for a time period P. Consequently the victim nodes execute the testing procedure locally based on M and specify themselves as trigger or non-trigger nodes to the base station. In this work we assume that there is no overlap between the jammer nodes.

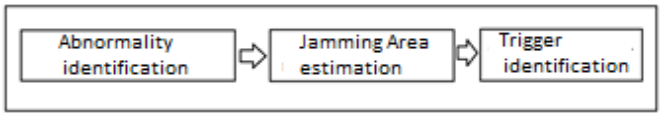


Fig 4: Trigger identification procedure

The testing period is reduced by using non-adaptive Group Testing (GT) method which involves testing the grouped items in pools instead of testing them individually.0-1 Matrix Mt×n is used for grouping where the matrix rows indicates the testing group and each column represents items. M [i, j] = 1 represents that the jth item takes part in the ith testing group, and the number of testing depends on the number of rows. The consequence of each group is represented as an outcome vector with size t where 0 conveys the negative testing result (no trigger in this testing group) and 1 refers to positive result (triggers in the testing group). The testing for non-adaptive GT is minimum if M is required to be d-disjunct, where the union of any d columns does not contain any other column [2].

Step 1: AbnormalityIdentification

Message reports regarding the status of the sensor nodes are periodically sent to the base station. There is a chance that jammers may be activated during the communication of sensor nodes with the base station .Once the nodes are deployed they will restrict the messages passing through them. The base station based on the ratio of received report compared with prior defined threshold can be used to decide whether jamming has occurred in a network.

SENDER ID	TIME STAMP	LABEL	TTL	ENERGY	MESSAGE BODY
Y1	0671	14	VICTIM	104.5	_____

Fig 5: Status Report Message

During the generation of status report message, each sensor nodes give the value of label based on the status of the nodes, initially it is set as trigger (TN). In precise, if jamming signal is heard by the node v, it will not be able to send out messages so it keeps its label of the report status to victim. If v doesn't sense any jamming signals, its reports are routed to the base station as usual, however, if it does not receive acknowledgement (ACK) from its neighbour within a timeout period during its next hop, two more retransmissions are tried. It is quite possible that neighbour is a victim node if no ACKs are received, then status report of v Label is updated as boundary node (BN). Unaffected nodes are those nodes whose status reports are successfully delivered to the base station with Label as TN .Intermediate nodes are used to queue the message and forward them in a first come first serve (FCFS) manner. If TTL = 0 the message is avoided in order to restrict self-loops. The base station waits until it receives status report from all nodes if it doesn't get response within maximum delay time it represents the node v as victim.

Step 2: Jamming Area estimation

The jamming region D will be calculated by the base station by taking into account the location of boundary and victim nodes. In this work we considered there is no overlap of jammer node areas. By denoting boundary nodes set for the ith jammed area as BNi, the jammer coordinate can be evaluated as

$$(Xj,Yj)= \{ \sum_{k=1}^{BNi} \frac{Xi}{BNi}, \sum_{k=1}^{BNi} \frac{Yk}{BNk} \} \quad [3]$$

Where (Xk,Yk) is the coordinate of a node k is the jammed area BNi and jamming range D is

$$D= \min\{\max(\sqrt{(Xk-Xj)^2+(Yk-Yj)^2})\} \quad [4]$$

Step 3: Trigger Identification

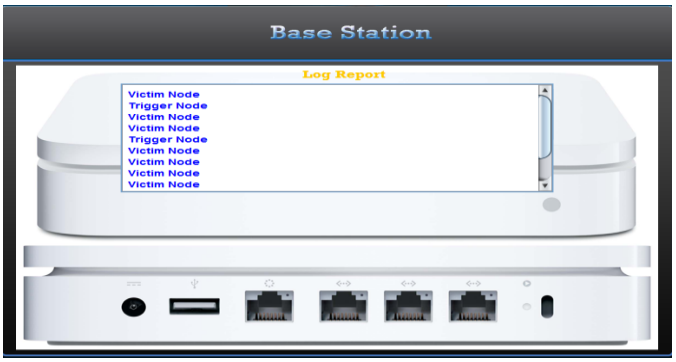
The reactive jammers immediately launch jamming signals once they sense the transmission they are waiting for. Trigger identification service is used for identifying the triggers in a jammed network. A schedule for encrypted testing is represented by all the victim nodes. The information about the scheduling is provided by the base station taking into the account the criteria of global topology and the boundary nodes. The topology Information is stored as a message and broadcast to all boundary nodes. Subsequently on receiving the test scheduling message, all the boundary nodes broadcast the messages by using simple flooding method to its neighbouring jammed region. Each victim nodes undergo testing schedule to specify themselves as trigger or non-trigger node.

In brief the base station generates a short testing schedule message Z which is broadcasted to each of the boundary nodes in the jammed area.

• The message Z is broadcasted by all the boundary nodes to all the victim nodes within the evaluated jammed region for a time period Q.

• The testing procedure is locally executed by all the victim nodes based on Z and a global uniform clock, identify themselves as trigger or nontrigger.

IV. SYSTEM SIMULATION



Benefits for identifying victim nodes, Trigger nodes, unaffected nodes:

1. Finding trigger nodes can help in eliminating the reactive jammers.
2. Having an idea about the sensor nodes in a network will help in avoiding push notifications to the nodes in network.

V. CONCLUSION AND FUTURE WORK

Throughout this paper, it is assumed that jammers remain constant i.e. they does not change their location, while in real WSN this is may not be correct. Due their location change all the work done to mitigate the jamming may be waste. Another

assumption is that all the jammers send only the jamming signal. But in practical sometimes they may send the useful data also. So that it is important to analyze the jamming signal.

REFERENCES

[1]W. Xu, K. Ma, W. Trappe, and Y. Zhang. ―Jamming Sensor networks: Attackand defense strategies.‖ *IEEE Network*,20:41–47, 2006.

[2]Non-adaptive Group Testing: Explicit Bounds and Novel Algorithms Chun Lam Chan, Sidharth Jaggi, Member, IEEE, Venkatesh Saligrama, Senior Member, IEEE, and Samar Agnihotri, Member, IEEE

[3]G. Padmavathi,"A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks," vol. 4, no. 1, pp. 1–9, 2009.

[4]LV Bo,ZHANG Xiao-fa,WANG Chao ,YUAN Nai-chang," Study of Channelized Noise Frequency-spot Jamming Techniques",2008