International Journal of Scientific Engineering and Technology (ISSN : 2277-1581)
Volume No.3 Issue No.8, pp : 1003- 1007 1 Aug 2014

Cooperative and constrained MIMO communication in wireless Adhoc sensor network

K.Shiva Prasad

Bhoj Reddy Engineering College for Women,Hyderabad , Telangana state ,India

ABSTRACT: ***Providing capable MIMO communication for wireless sensor network is a crucial challenge that is created more difficult to its broadcast nature and restrictions on resources such as electricity, power memory utilization, computation and communication capacities. The Route blockage and non cooperation is a significant security hazard to wireless sensor networks since route blockage and non cooperation is a light weight attack which is simple to establish but challenging to find. This work suggests a brand new proposal to neutralize malicious reactive jammer nodes by changing the characteristic of trigger nodes to act as only receiver. Here the current approach tries to identify the trigger nodes utilizing the group testing technique, which enhances the recognition speed and reduces the message difficulty of the status report sent periodically between the sensor nodes as well as the base station.***

KEYWORDS: Wireless sensor network, Jamming Techniques, Reactive jamming, Trigger identification.

1. INTRODUCTION

Wireless sensor networks has limited resource constraints when it comes to range and power which causes many difficult and intriguing security sensitive issues that can't be handled using traditional security solutions. The broadcast nature of the transmission medium causes it to be prone to attacks using jammers which use the system of injecting interference signals, which explains why they may be considered as the most important and fatally adversarial threat that could interrupt the networks. Jamming attacks do not have to modify communication packets or compromise any sensors to be able to launch the assault. This makes them hard to detect and safeguard against. As a consequence, wireless sensor networks are additional subjected to active and passive attacks. Whereas an energetic attacker is involved in transmission also, a passive attack is started by a malicious node [1] through observation of the ongoing MIMO communication.

1.1. Jamming Techniques

The spot jamming method [2] involves a malicious node that directs all its transferring electricity to a single frequency. It employs not as much power and indistinguishable modulation schemes to override the first transmission. The attack on WSNs because of the strike is easily avoided by browsing to some other frequency. In case of Sweep jamming technique [3], the malicious node can jam multiple MIMO communication frequencies, but this jamming does not change each of the involved nodes concurrently. The attack also contributes to packet loss as well as retransmission of packet information which will increase use of energy in the system.

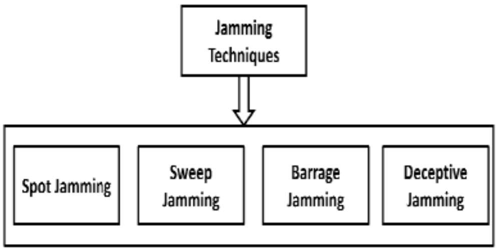


Fig 1: Different types of jamming techniques

Number 1 is an example of the kinds of playing techniques used in general to start jammer strikes. In Battery jamming technique[4], the malicious node jams a band of frequencies simultaneously which reduces the signal-to-noise ratio of the destination node. This performing technique reduces the output power of the node and increases the range of jammed frequencies. Deceptive jamming[5] has the ability to flood the system with useless data which may deceive the sensor nodes present within the network. The obtainable bandwidth utilized from the sensor nodes is decreased. The nodes which make use of this technique do not reveal their lifestyle.

1.2. Jamming Types

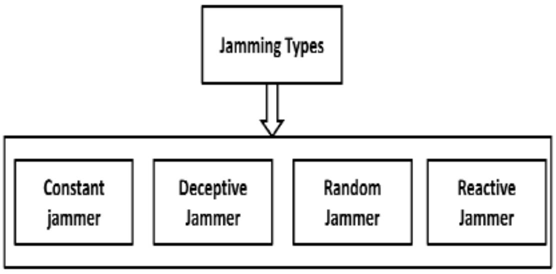


Fig 2: Types of jammers

Figure 2 represents several types of jammers that could be used in assaults against wireless sensor systems random jammer, misleading jammer, specifically constant jammer and reactive jammer. The constant jammer [6] emits uninterrupted radio signals within the wireless medium. They do not follow any underlying MAC method and include simply random bits. This jammer keeps the channel busy and impedes the conversation between your nodes. The deceptive jammer [7] utilizes the wireless sensor nodes to be attacked by misleading jamming techniques. The haphazard jammer [8] rests for an indiscriminate time and wakes up-to jam the system for an arbitrary time. The last playing strategy indicated above is the reactive jammer [9] which listens for on-going activity on the channel. On recognition of legitimate activity, a random signal is instantly sent out by the jammer node to disrupt the applicable MIMO communication signals prevalent on the route leading to collision.

1.3. System Architecture

The inference after evaluating the previously discussed jamming attacks is that reactive jamming is a much more destructive attack that opposes protected MIMO communication in wireless sensor network. This document considers the route blockage and non cooperation since it creates a crucial threat to wireless sensor systems while the reactive jammer nodes can disrupt the information delivery of its own neighboring sensor nodes with powerful interference signals. The results of the attack will be the loss of connection reliability, increased power consumption, extended package delays, and disruption of end-to-end routes.

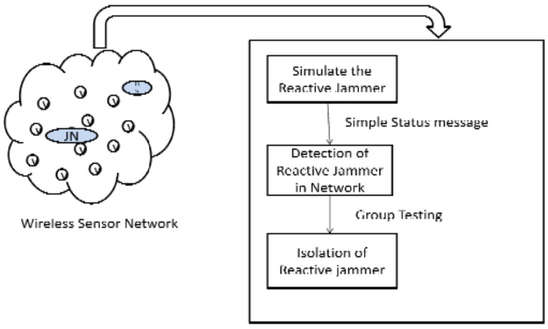

JN
Wireless Sensor Network
Simulate the Reactive Jammer
Simple Status message
Detection of Reactive Jammer in Network
Group Testing
Isolation of Reactive jammer

Fig 3: System Architecture

This work presents system design for defense against route blockage and non cooperation. The first outline of the overall cause identification service construction begins with the id of the group of patient nodes. These nodes are subsequently grouped into several testing teams. When the group testing is carried out at the bottom stop, the nodes themselves locally run each individual node to be identified by the testing procedure for a trigger or low trigger. The identification outcomes could be stored locally for use by routing techniques or could be transmitted to the bottom station for playing localization procedure. The rest of the task is organized as follows. Part 2 explains the community model, as well as the opponent model along with jamming features. Section 3 describes the implementation strategy for cause id support by utilizing group testing. Section 4 describes the efficiency assessment by investigation of the moment complexity involved in addition to assessment of the time taken to carry out the testing rounds and also the information complexity.

2. SYSTEM MODELS AND NOTATION

2.1. Network Model

The design views an invisible sensor system that consists of one bottom station and n sensor nodes. Each sensor node has omni directional antennas, along with m radios that adds up to a total of k stations through the community, where k>m. Here the energy strength in each course is thought to be standard, therefore the transmission range of each and every sensor may be considered as a constant r and the system is modelled for a unit disk graph (UDG). where any node set (i, l) is supposed to be linked if the Euclidean length between (i, t) < r.

2.2. Attacker model

An ongoing transmission can be sensed by the jammer nodes to determine whether or not to start a playing signal conditioned upon the power of the thought sign. The supposition made here is that reactive jammers have omni-directional antennas with uniform electricity strength on every direction which is like the home of the detectors. The packed area produced by the reactive jammers lies on the heart of the system area, using a distance R, where jammer array R is required to be higher than the range of all detectors in the network to be able to achieve a strong and effective jammer design. Most of the sensors in this array will probably be crammed during the jammer wake-up period. The value of R may be calculated based in the positions of the border detectors and casualty nodes within the networks. Another assumption is that any two jammer nodes are not in close-range together so as to make the most of the stuffed region.

2.3. Sensor model

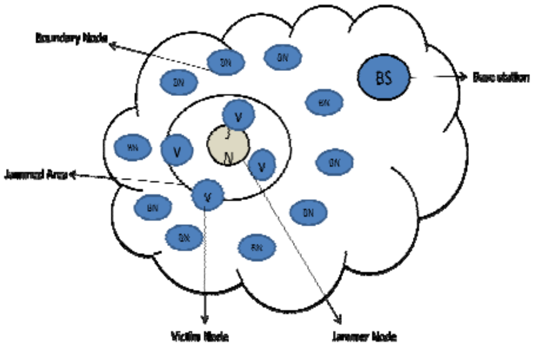


Fig 3: Categorization of Sensor Nodes

The jamming status is exploit to categorise the sensor nodes into four types as exposed in Figure 3.Trigger Node TN is a sensor node which awakes the jammers, victim nodes VN are those inside a distance R from an trigger jammer, boundary nodes BN and unaffected nodes are free from the consequence of jammers.

3. IMPLEMENTATION APPROACH USING TRIGGER IDENTIFICATION

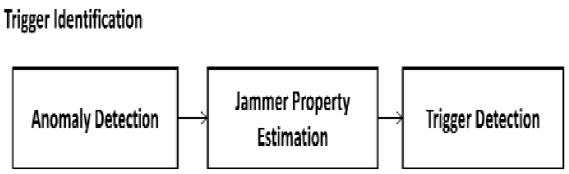
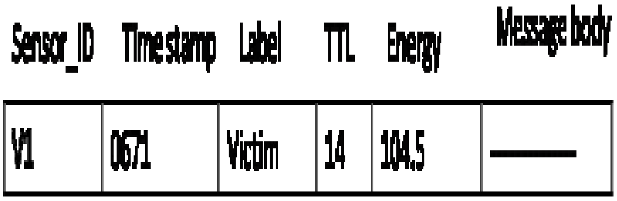


Fig 4: Trigger identification procedure

Trigger id service is mostly divided into three primary steps as shown in Figure 4. The initial step executes anomaly diagnosis where the base station detects impending route blockage and non cooperation. Each boundary node identifies itself to the base station. In the 2nd step jammer home estimate is conducted where the base station computes the estimated stuffed location and playing range on the basis of the place of boundary node. The 3rd measure is trigger detection where the base station shows a short testing program message M to all of the boundary nodes.Thereafter the boundary nodes maintain transmission M to most of the victim nodes within the estimated stuffed region for an interval P. Subsequentlythe victim nodes locally implement the testing process predicated on M and recognize themselves as trigger or nontrigger.

The non-adaptive Group Testing (GT) strategy can be utilized to minimize the testing period by sophisticatedly grouping and testing the items in pools simultaneously, instead of separately testing them. This way of grouping is contingent upon a 0-1 matrix Mtxn where the matrix lines represent the screening group and every column refers to something. M[i, t] = 1 signifies that the jth item participates in the ith testing team, along with the host of testing will be the myriad of rows. The results of each team is represented as an outcome vector with dimension t where zero is an adverse testing outcome (no cause within this testing group) and 1 is a positive result (possible triggers inside the team). To realize the minimum testing span for non adaptive GT, Meters is needed to be d -disjunct, where the partnership of any d columns doesn't include any other order.

Step 1: Anomaly Detection



Sensor_ID	Timestamp	Label	TTL	Energy	Message body
V1	0671	Victim	14	104.5	———

Fig 5: Status report message

Step 2:. Trigger Detection

Once it senses the ongoing transmission by the sensors the jammers promptly air jamming signals. The jammers are determined by cause identification service. Here encrypted testing schedule is adhered by each of the sufferer nodes. Scheduling will be done at the base station on the basis of the set of boundary nodes as well as the worldwide topology. Information regarding topology is stored for a message and transmission to all border nodes. After receiving the check scheduling message, each boundary node broadcasts the concept by using simple inundation method to the adjoining packed area. All casualty nodes stipulate themselves and implement the screening schedule as trigger or non trigger node.

Algorithm :Trigger Nodes Identification Algorithm

All nodes in a group synchronously performs the following to identify three trigger nodes in .

```
INPUT: TestingGroup

OUTPUT: Triggers

Triggers

/* In order to discover a node v with maximum distance to the center of the hexagon, each node sorts all neighbors based on the distance to the center of the hexagon in non-increasing order */

SortedNodes  DecSort(d( ))

In a new trice   do the following:

  ISTN (SortedNodes)

/* In order to discover a node u with maximum distance to v , each node sorts all neighbors based on the distance to v in non-increasing order */

SortedNodes  DecSort(d( ))

In a new trice do the following: u  ISTN (SortedNodes)

if v == u then

Triggers   v else

Construct two disks Dv and Du centered by v and u with radius d(u,v)

Pick two nodes w and 2 which have the closest intersection points from Dv and Du. w is the node with smaller ID.

In a new trice   do the following: if ID == w then

Perform individual testing on w else

Listen to the Noise end if

In a new trice   do the following: if ID == 2 then

Perform individual testing on 2 else

Listen to the Noise end if

if w == TriggerNode and 2 == TriggerNode then

Triggers

 else

if w == TriggerNode

then w 2

end if

Coordinate p   the closest intersection of Dv and Du from w
SortedNodes  IncSort(d( , p))
```

```
In a new trice  do the following: u'   ISTN (SortedNodes)

SortedNodes     SortedNodes \ u In a new trice At do the following: v'   ISTN (SortedNodes)

  — center of the disk with radius r which includes both v and u, passing through v'

and u'.

for i = 0; i   |   |; i + + do

if d( ,  )  r then Triggers U

end if end for

end if

end if
```

As shown in algorithm more than, the groups can decide to conduct group testing on themselves in m pipelines. If any jamming signals occur in pipeline, then the existing test will be stopped and the next test has to be scheduled. The groups getting no jamming signals are necessary to resend triggering messages and wait until the predefined round time has passed.

4. PERFORMANCE EVALUATION AND RESULT ANALYSIS

The outcomes of the tests demonstrate this option is time-efficient for protecting route blockage and non cooperation and determining cause nodes. The cause recognition process for reactive playing in network simulation NS2[21] on 900x900 rectangular detector area with n=10 indicator nodes is simulated. The indicator nodes are evenly distributed, with a single base station and T distributed jammer nodes. Within this function, the detector transmission distance r and playing transmission R as 2r is thought to reach better efficacy of the jamming design.

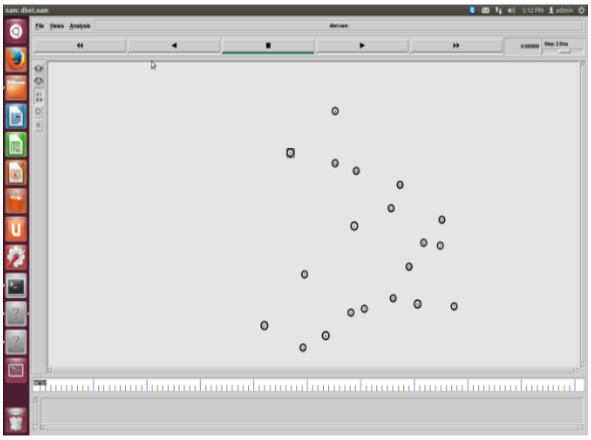


Fig 6: Simulation of reactive jamming

Figure6 shows a network simulated with 10 sensor node with 1 malicious node and 1 base station. The transmission range(r) of ordinary sensor node is set as 50m while jammer transmission range(R) set to 100m(2r).

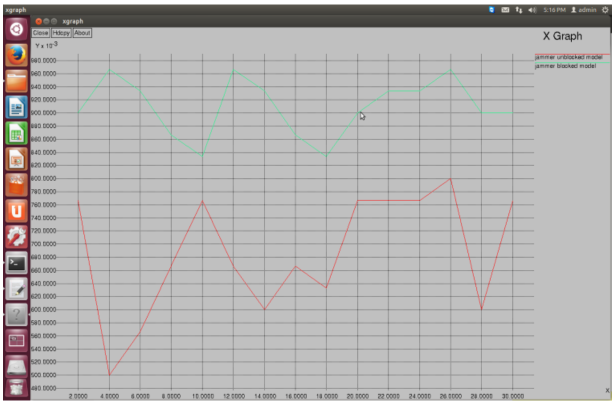


Fig 7: The number of testing rounds t(sec)
Figure7 explains the protocol performance based on PDR in Routing

5. RELATED WORK

Among the reactive countermeasures uses Designed Breadth - First Search Tree algorithm for recognition of jammer node[13]. Once a node receives this information, it'll establish its corresponding entry to one. Another channel is utilized to air the broadcast information, in the event the node senses that anyone of the stations is packed. The base station will obtain a set of messages from all possible leaf nodes.

Another approach for the diagnosis and mapping of stuffed area [14] is offered by Wood and Stankovic to boost system efficiency. Nevertheless this procedure has many drawbacks: first, it cannot nearly defend in the situation that the attacker jams the entire network; second, in case the attacker goals some particular nodes I.e. those that guard a safety entrance to block their digital MIMO communication, then this method doesn't shelter the nodes under assault. Xu [15] suggested two strategies against jammers I.e, route surfing and spatial retreat. Channel surfing is flexible type of FHSS. Rather than switching continuously from one channel to yet another, a node changes to a channel just when it finds that the current channel is free from jammer. The spatial retreat strategy makes two nodes to go in varied ways with separation at least equal to Manhattan miles [16] to escape from a jammed area. The drawbacks of the above mentioned procedures are that they are beneficial only for continuous jammers and they don't have any impact on reactive jamming.

The notion of Wormhole [17] may be used to evade the places which disturb the regular MIMO communication of the sensor nodes. These options can only effectively decrease the level of the jamming attacks, but their functionality really depends on the validity of recognition of the packed locations, I.e. transmission overhead could be needlessly concerned when the jammed region is much larger than its actual size. Victim nodes can't efficiently avoid jamming signals because they cannot possess information over positions of concealed reactive jammer nodes, notably in dense sensor systems.

This paper proposes an unique execution shift towards support of the network against reactive jamming attack i.e. trip identification service [18-19]. This is often thought of as a device because every one of the computations are complete at the base station. This strategy attempts to moderate the time complexity as well as the transmission overhead. The edge that this strategy attempts to achieve may be the elimination of additional hardware requirement. The requirement of the system is really to send simple position report messages from each sensor and the information regarding the geographic locations of all sensors maintained at the base station.

6. CONCLUSION

In this paper, a novel trigger id service for route blockage and non cooperation in wireless sensor system is launched to achieve minimal time and information overhead. The position report information are transferred between the base station and all sensor nodes. For isolating reactive jammer in the network a trigger id support is introduced, which needs all testing teams to schedule the trigger node recognition algorithm using team testing after anomaly diagnosis. By pinpointing the trigger nodes within the community, reactive jammers could be removed by producing trigger nodes as only receivers. This detection scheme is thereby well suited for the safety of the sensor network against the jammer. What's More, probe into energy-efficient and stealthier jamming models with simulations reveals robustness of the present projected scheme. The end result can be saved in the network for additional operations I.e. to do best routing procedure without playing. This function achieves the removal of enemies to preserve the soundness of wireless sensor networks.

REFERENCES

i. *G. Padmavathi,"A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks," vol. 4, no. 1, pp. 1-9, 2009.*

ii. *LV Bo,ZHANG Xiao-fa,WANG Chao ,YUAN Nai-chang," Study of Channelized Noise Frequency- spot Jamming Techniques",2008*

iii. *XI You-you,CHENG Nai-ping, "Performance Analysis of Multi-tone Frequency Sweeping Jamming for Direct Sequence Spread Spectrum Systems",2011.*

iv. *Williams united state ," Multi-Directional Barrage Jamming System",1975.*

v. *J. Schuerger, "Deceptive Jamming Modelling In Radar Sensor Networks," pp. 1-7.*

vi. *W. Xu et al., "Channel Surfing and Spatial Retreats: Defenses Against Wireless Denial of Service," Proc. 2004 ACM Wksp. Wireless Security, 2004, pp. 80-89.*

vii. *W. Xu et al., "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks," MobiHoc '05: Proc. 6th ACM Int'l. Symp. Mobile Ad Hoc Net. and Comp., 2005, pp. 46-57.*

viii. *W. Xu et al., "Channel Surfing and Spatial Retreats: Defenses Against Wireless Denial of Service," Proc. 2004 ACM Wksp. Wireless Security, 2004, pp. 80-89.*

ix. *W. Xu et al., "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks," MobiHoc '05: Proc. 6th ACM Int'l. Symp. Mobile Ad Hoc Net. and Comp., 2005, pp. 46-57.*

x. *Y. Law et al., "Link-Layer Jamming Attacks on S-Mac," Proc. 2nd Euro. Wksp. Wireless Sensor Networks, 2005, pp. 217-25.*

xi. *A. Wood and J. Stankovic, "Denial of Service in Sensor Networks," IEEE Comp., vol. 35, no. 10, Oct. 2002, pp. 54-62.*

xii. *D. Report, C. Science, and J. Bacaj, "Detecting Attacks in Wireless Sensor Networks," 2011.*

xiii. *A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, "A survey on jamming attacks and countermeasures in WSNs," IEEE Communications Surveys & Tutorials, vol. 11, no. 4, pp. 42-56, 2009.*

xiv. *M. Wilhelm, I. Martinovic, J. B. Schmitt, and V. Lenders, "Short Paper: Reactive Jamming in Wireless Networks — How Realistic is the Threat ? PHY packet," pp. 0-5, 2011.*

xv. *W. Xu, W. Trappe, Y. Zhang, T. Wood, \The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks", in Proc. of the 6th ACM international symposium on Mobile ad hoc networking and computing, pp. 46-57, 2005.*