A Defensive Mechanism for Deterring Reactive Jamming Attacks in WSN

Akash S.P, Anil Kulkarni, Vinod.N.Biradar

Abstract— Reactive Jamming Attacks had evolved as a major security threat during the last decade due to its massive destructions to genuine wireless sensor communications until a jammer node defending scheme was developed. This scheme deactivates reactive jammers by efficiently identifying all trigger nodes whose transmissions invoke jammer nodes. In this existing solution the jamming zone identification procedure is carried out only during the initial time of operation but an attacker can come into existence at any point of time during the operation and also certain jammers show their behavior during very late time. Hence the existing solution may fail to identify such jammers. To avoid the problem faced in this existing solution, in this paper we propose and develop an energy efficient detection mechanism which identify trigger nodes frequently and deter these jamming attacks. Simulation results are included to validate the performance of this framework.

Index Terms— Wireless sensor network, Reactive jamming, Jamming detection, Trigger-Identification , Non adaptive group testing, Periodic trigger detection and Clique independent set.

1 INTRODUCTION

A Wireless sensor networkdocument is a collection of nodes organized into a cooperative network [2]. Each node consists of processing capability (one or more micro controllers, CPU's etc) may contain multiple types of memory (program, data, flash etc), have a RF transceiver, have a power source and accommodate various sensors and actuators. The nodes communicate wirelessly and often self organize after being deployed in a adhoc fashion. Currently wirless sensor networks are being deployed in an accelerated phase [3]. As in any networks wireless sensor network are also prone to attacks where normal functioning of network are interrupted by attacks known as jamming and attackers are called as jammers. In this paper we mainly focus on particular type of jamming known as *reactive jamming attacks* which has evolved as critical security threat to wireless sensor networks. This jamming is caused by *reactive jammers* which silently listens to the commencing activity on the channel and when it senses any ongoing transmissions on the channel it immediately sends ou an interference signal and disrupts the message delivery [5].

Existing countermeasures against reactive jamming attacks provides an application layer real-time trigger identification service for defending reactive jammers which efficiently identifies all the trigger nodes whose transmissions invoke these jammers, using a lightweight decentralized algorithm [1].

This existing countermeasure fails to identify certain jammers, that come very late into existence during the operation and jammers which show their behavior very lately, because they carry out jamming zone identification procedure only during the initial time of operation and thus cannot defend such jammers.

To avoid this problem we propose and develop an energy efficient trigger identification mechanism which checks for the trigger frequently. But starting the trigger process frequently will reduce the energy level and also the lifetime of the sensor network. So we propose a mechanism based on measuring the *packet delivery ratio* (PDR) periodically by the base station. For any packet received from the node base station sends an acknowledge to the node. Based on acknowledgement sent the node calculates the packet delivery ratio. Periodically every base station request nodes to send their packet delivery ratio and if this PDR is less than the predetermined threshold from nodes in particular area then base station starts trigger process to identify jammers. In this way we can identify jammers that get activated very lately. This mechanism is also energy efficient because trigger process is not started unless there is a fall in PDR below threshold.

2 PRELIMINARIES

2.1 Attacker Model

Conventional reactive jammers [4] are defined as malicious devices, which keep idle until they sense any ongoing transmissions and then emit interference signals to disrupt the sensed signal (jammer wake up period) instead of whole channel which means once the sensor transmissions finishes, the jamming attacks will be stopped (jammer sleep period). Three concepts are introduced to complete this model.

1) Jammer range R- Similar to sensors, jammers are equipped with omnidirectional antennas with uniform power strength on each directions. Jammed area can be regarded as circle centered at jammer node with radius R for simulating an efficient jammer node. All the sensors within this range are jammed during jammer wake up period. The value of R is approximated besed on boundary sensor positions and can be refined.
2) Triggering range r- On sensing an ongoing transmission the decision whether or not to launch a jamming signal depends on power of sensor signal Ps, arrived signal power Pa and power of background noise Pn.
3) Jammer distance- Any two jammer nodes are assumed not to be too close to each other. This distance between two nodes can be given base on Euclid's principle, which should be less than R to avoid

transmissions and receptions interence and also the deployment of these jammers should maximize jammed areas with limited number of jammers.

2.2 Sensor Model

Besides monitoring the assigned network field and generating alarms in case of special events, each sensor periodically sends status report messages to the base station which contains information about monitored results, battery usage and other related content. According to jamming status, sensor nodes can be categorized into trigger nodes TN, victim nodes VN, boundary nodes BN and unaffected node UN. Trigger nodes are those sensor nodes whose signal awake jammers and victim nodes are those which are disturbed by the jamming signal.

3 Non-Adaptive Group Testing

Group testing was proposed to speed up the identification of affected blood samples from a large population [6]. We use this technique as the nature of our work is to identify all triggers out of a large pool of victim nodes. The key idea of this testing is to test items in multiple designated groups instead of individually identifying.

4 Proposed Scheme

We propose a lightweight decentralized energy efficient trigger detection procedure which consists mainly of three steps.

1) *Aberration detection*- The base station detects potential reactive jamming attacks, each boundary nodes tries to report their identities to base sation.

2) *Jammer area estimation*- The base station estimates the jammed area and jamming range R based on locations of the boundary nodes.

3) *Frequent trigger detection*- This trigger detection procedure is carried out initially during the operation and also periodically whenever PDR fall below the predetermined threshold value.
   - The base station makes a short encrypted testing schedule message X which will be broadcasted to all boundary nodes.
   - Boundary nodes inturn keeps broadcasting X to all victim nodes within estimated jammed area for a period Q.
   - All victim nodes locally execute this testing procedure X and identify themselves as triggers or non triggers

Each sensor periodically sends status report message to the base station. However, once the jammers are activated by message transmissions, the base station will not receive these reports from the sensors. By comparing the ratio of received report to a predefined threshold, the base station can thus decide whether a jamming attack has happened or not in the networks. When generating the status report message each sensor can locally obtain its jamming status and decide value of label field. If a node n hears a jamming signal it will not send out messages but keep its label as victim. If n cannot sense jamming signals its report will be delivered to base station as usual. If it does not receive "ACK" from its neighbour on the next hop of the route within a time out period it retransmits, but it does not receive "ACK" even after its quite possible that neighbor is a victim node and update label tuble as boundary node "BN" in its status report. If status report is successfully delivered to the base station with tuple "TN"then the corresponding node is regarded as unaffected. All messages are queued in buffer intermediate nodes and served in droptail/priority queue manner. The "TTL" values are reduced one per hop and when "TTL" is 0 the message will be dropped. The base station waits for the status report from each node n for a period of length P and if reports are not received with a maximum delay then n is regarded as victim. If aggregate report amount is less than, then base station starts creating testing schedules for trigger nodes, based on which routing tables will be updated locally. Packet delivery ratio falling below for some node, but area wise better, will not start testing procedure because even due to some other reasons such as congestion PDR drop can occur.

5 System Requirement Specification

Type	*Used*
Operating system	UBUNTU (10.04 version)
Simulator	NS-2 (2.34 version)
Language	TCL
Channel	Wireless
Radio propogation model	Two Ray ground propogation
Interface queue type	Droptail/priority queue
Simulation area	900m * 900m
Number of nodes	50,60,70
Transmission range	40m
Maximum packet in interface queue	60
MAC layer protocol	IEEE 802.11
Simulation duration	100 sec
Packet rate	1 packet/ sec
Packet type	CBR (UDP)

6 Performance Analysis

6.1 Number of Messages for Detecting Jammers

Below performance graphs could be used to analyze the number of messages for detecting jammers during trigger zone identification operation. The metrics used for comparing are Number of messages, number of jammers, jamming range and number of nodes. By changing these metrics, in the x-axis and y-axis, accordingly we obtain three performance graphs which can be used to analyze the number of messages required for detecting jammers in the existing solution (clique) and pro-

posed solution. We can observe from the graph that proposed solution consumes fewer messages to detect jammer than the existing solution (clique).

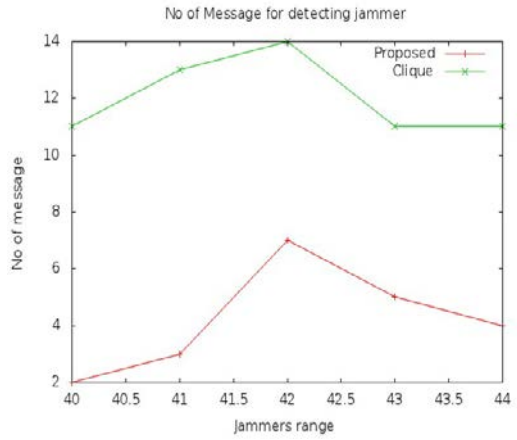

Fig.1. Number of messages for detecting jammers

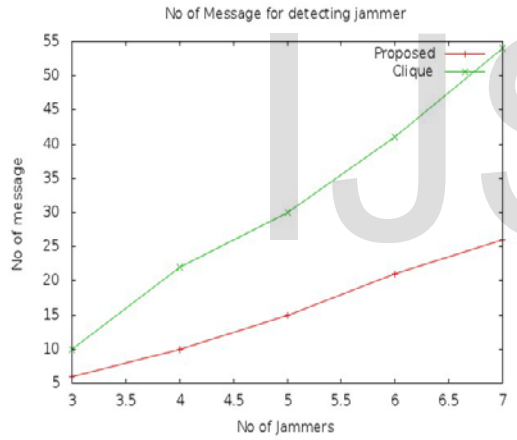

Fig.2. Number of messages for detecting jammers

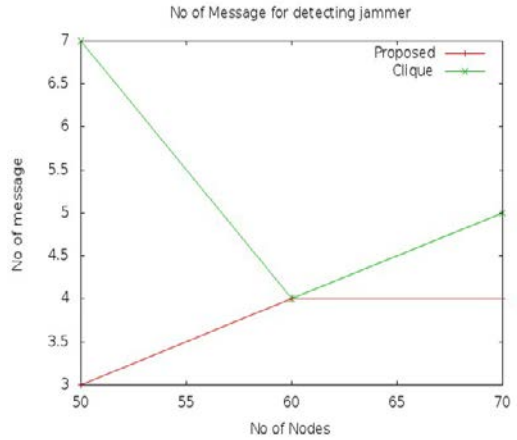

Fig.3. Number of messages for detecting jammers

6.2 Time Complexity for Detecting Jammers

Below performance graphs could be used to analyze the time complexity involved or time required for detecting a jammer node during the trigger zone identification operation. The metrics involved for comparison are time complexity, jamming range, number of jammers and number of nodes. By changing these metrics, in the x-axis and y-axis accordingly, we obtain three performance graphs which can be used to analyze the time complexity for detecting jammer nodes. From these obtained observation we can conclude that proposed solution requires less time to detect jammer compared to existing solution (clique).

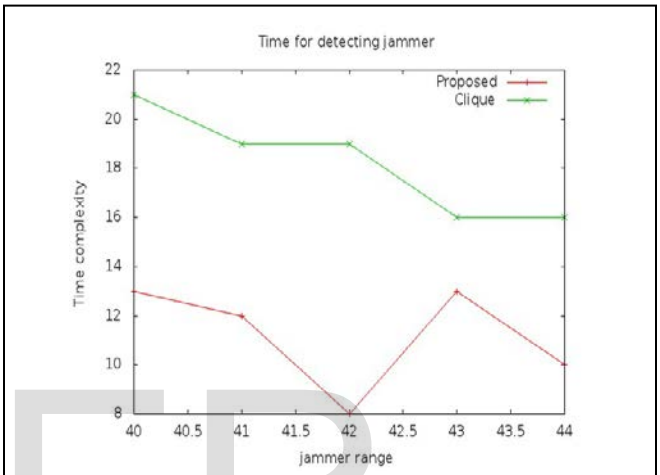

Fig.4. Time complexity for detecting jammers

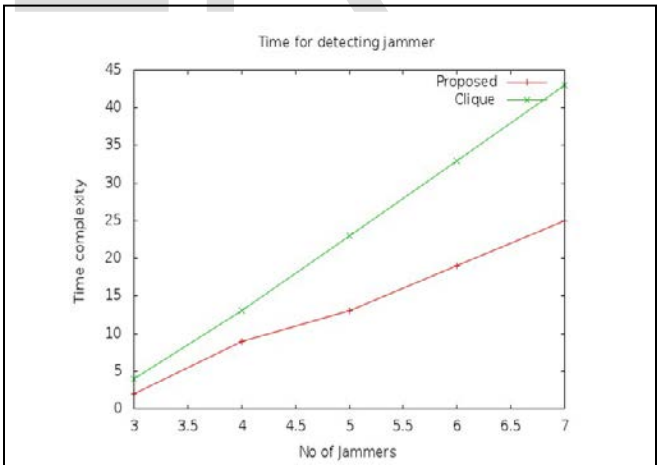

Fig.5. Time complexity for detecting jammers

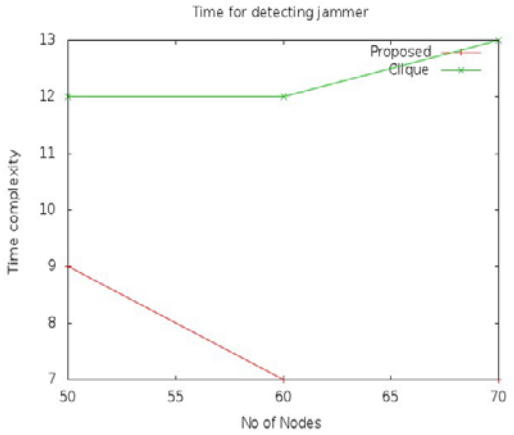

Fig.6. Time complexity for detecting jammer

7 Conclusion

As a summary in order to provide an energy efficient defenseve mechanism for deterring reactive jamming attacks we leverage several optimization problems and provide effective solutions and also performance analysis to them. The efficiency of this framework is proved both through theoretical analysis and simulations under different network settings.

Acknowledgment

I want to thank Prof. Anil Kulkarni for his esteemed guidance in completion of this paper and also Vinod Biradar for his kind support.

References

[1] Ying Xuan, Yilin Shen, Nam P. Nguyen, My T. Thai, "A Trigger Identification Service For Defending Reactive Jammers in WSN,"IEEE Transactions on Mobile Computing, vol.11, No.5, 2012

[2] J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler and K. Pister, System Architecture Directions for Networked Sensors, ASPLOS, November 2000.

[3] Wireless Sensor Networks, John A. Stankovic, Department of computer science, University of Virginia, Charlottesville, Virginia 22904, June 19 2006.

[4] W.Xu, K. Ma, W. Trappe and Y. Zhang, "Jamming Sensor Networks: Attack and Defend Startergies,"IEEE vol.20, no 3,pp 41-47, May/June 2006.

[5] W. Xu, W. Trappe, Y. Zhang, T. Wood, "The Feasibility of Launching and Detecting Jamming Attacks in Wireless networks,"in Proc 6th ACM International Symposium on MANET and computing, pp.46-57, 2005.

[6] D.Z. Du and F. Hwang,"Pooling Designs: Group Testing in Molecular Biology," World Scientific 2006.