Defending Reactive Jammers in WSN using A Trigger Identification Service

Harshad Shelar[1] Jilani Momin[2] Sainath Patil[3] Kiran Jaybhaye[4]
[1,2,3,4]Department of Computer Engineering
[1,2,3,4]D.C.O.E.R Pune, India

Abstract— In the last decade, the greatest threat to the wireless sensor network has been Reactive Jamming Attack because it is difficult to be disclosed and defend as well as due to its mass destruction to legitimate sensor communications. As discussed above about the Reactive Jammers Nodes, a new scheme to deactivate them efficiently is by identifying all trigger nodes, where transmissions invoke the jammer nodes, which has been proposed and developed. Due to this identification mechanism, many existing reactive jamming defending schemes can be benefited. This Trigger Identification can also work as an application layer .In this paper, on one side we provide the several optimization problems to provide complete trigger identification service framework for unreliable wireless sensor networks and on the other side we also provide an improved algorithm with regard to two sophisticated jamming models, in order to enhance its robustness for various network scenarios.

Key words: Trigger Identification,, Error Tolerant Non-adaptive Group Testing, Reactive Jamming, NP Hardness, Jamming Detection

I. INTRODUCTION

Due to its wide applications in various monitoring systems and invulnerability, the security of wireless sensor networks has attracted numerous attentions. The most critical threat to the WSNs are the jamming attack where the jammer disrupts the delivery of nearest nodes with interface signal. Due to the researches on this issue, it can be explained and solved more efficiently.

In recent years, the most effective measures and technique against the Reactive Jamming are the Jamming Detection and Jamming Mitigation. At the same time various network diversities are investigated to provide immediate solutions.

Here in this paper, for reactive jammers in wireless sensor network, we present an application-layer real time trigger identification, which gives the list of trigger nodes having lightweight algorithms. The above technique provides great potential to develop as jamming defending.

This technique of trigger identification is very exciting due to its hardness and ability to identify the trigger nodes from the set of the victim nodes that are affected due to the jamming signals from the reactive jammers.

II. RELATED WORK

In our project our main aim is to find first the affected nodes by corresponding links PDR and RSS, where these affected nodes are grouped into multiple testing teams. Then the group testing schedule is done to identify whether the nodes are triggered or non-triggered at the base station. Then the result may be routed or may be sent to the sent to the base station for jamming.

III. THREE KERNEL TECHNIQUES

In this we have the kernel techniques that we have to resort to in the protocol. Most damage is done by the reactive jammers that can do larger damage due to its hardness to detect and efficient attack. For this we brought up with the group testing process, i.e. the randomized error tolerant group testing by means of disjunct matrix and designed random, which avoids unnecessarily large isolated areas. In existing solutions, they can handle only the single jammer case due to the lack of knowledge of the range of the jammer and inevitable overlapping of the jammed areas bring up the analytical difficulties. So keeping this in mind we resort the two another techniques as a minimum disk cover problem in within simple polygon problem and a clique independent set problem.

To speed up the identification of blood samples from a large sample population the method of group testing was proposed. This testing has helped various fields such as medical testing and medical biology in the recent decades.

IV. TRIGGER IDENTIFICATION PROCEDURE

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 a 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.

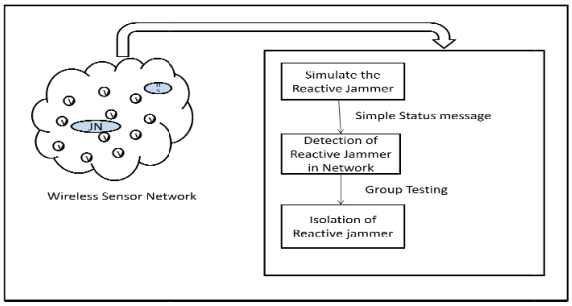

Fig: System Architecture

V. CONCLUSION

In this paper we have solved the jamming problem more efficiently. The only point that left of the jammers was the jammer mobility. The latency of the identifying the node was not fast hence it would not have been efficient with the nodes with the higher speed. One of the main leftover of the system was the application of the service. The routing of the jammers and the localizations of the jammers are promising but still it needs to be developed for the real time requirement.

As studied for identifying the trigger identification service framework, we studied different techniques, procedures as well as executed various algorithms which include the clique identifying problem, randomized error tolerant group testing and minimum disk cover for simple polygon. The efficiency of this framework has been determined in both by theoretically and through various models which attack on the service under network settings. With many possible applications these frameworks consist of huge potential to detect the trigger nodes and also need the further studies.

REFERENCES

[1] M. Strasser, B. Danev, and S. Capkun. "Detection of reactive jamming in sensor networks." ETH Zurich D-INFK Technical Report, August 2009.
[2] H. Wang, J. Guo, and Z. Wang. "Feasibility assessment of repeater jamming technique for dsss." WCNC2007. IEEE, pages 2322–2327, March 2007.
[3] H. Liu, W. Xu, Y. Chen, Z. Liu, "Localizing Jammers in Wireless Networks", PWN 2009.
[4] Z. Liu, H. Liu, W. Xu, Y. Chen, "Wireless Jamming Localization by Exploiting Nodes' Hearing Ranges", DCOSS 2010.
[5] Y. Xuan, Y. Shen, Nam P. Nguyen and My T. Thai" Trigger Identification Service for Defending Reactive Jammers in WSN." MAY 2012.

