Lightweight Decentralized Algorithm for Localizing Reactive Jammers in Wireless Sensor Network

[1,]Vinothkumar.G, [2,]Ramya.G, [3,]Rengarajan.A
P.G.Scholar [(1, 2)], Associate Professor [(3)]
[1,2,3,]Veltech Multitech Dr.Rangarajan Dr.Sakunthala Engineering College, Chennai, India

Abstract:
In wireless sensor network one of the most security threats is the reactive jammer because of the mass destruction to the sensor communication and it is difficult to disclose. So we have to deactivate the reactive jammers by identifying all the trigger nodes, because the transmission invokes the jammer. Such a trigger identification procedure can work as an application-layer service and benefit many existing reactive jamming defending schemes. In this paper, on the one hand, we leverage several optimization problems to provide a complete trigger-identification service framework for unreliable wireless sensor networks. On the other hand, we provide an improved algorithm with regard to two sophisticated jamming models, in order to enhance its robustness for various network scenarios. Theoretical analysis and simulation results are included to validate the performance of this framework..

Keywords: Reactive jamming, jamming detection, trigger identification, error tolerant non adaptive group testing, optimization, NP-hardness.

1. Introduction

The security of wireless sensor networks has attracted numerous attentions, due to its wide applications in various monitoring systems and vulnerability toward sophisticated wireless attacks. Among these attacks, jamming attack in which a jammer node disrupts the message delivery of its neighboring sensor nodes with interference signals, has become a critical threat to WSNs. However a reactive variant of this attack, where jammer nodes stay quiet until an ongoing legitimate transmission (even has a single bit) is sensed over the channel, emerged recently and called for stronger defending system and more efficient detection schemes. Existing countermeasures for reactive jamming attacks consists of jamming detection and jamming mitigation. On the one hand detection of interference signals from jammer nodes is non-trivial discrimination between normal noises and adversarial signals over unstable wireless channels. A mapping service of jammed area has been presented in which detects the jammed areas and suggests that routing paths evade these areas. This works for proactive jamming, since all the jammed nodes are having low PDR and thus incapable for reliable message delay. However, in the case of reactive jamming, this is not always the case. By excluding the set of trigger nodes from the routing paths, the reactive jammers will have to stay idle since the transmissions cannot be sensed. Even though the jammers move around and detect new sensor signals, the list of trigger nodes will be quickly updated, so are the routing tables.

The basic idea of our solution is to first identify the set of victim nodes by investigating corresponding links PDR and RSS, then these victim nodes are grouped into multiple testing teams. Once the group testing schedule is made at the base station and routed to all the victim nodes, they then locally conduct the test to identify each of them as trigger or non-trigger.

.

2. Problem Models

2.1 NETWORK MODEL

Consider a wireless sensor network consisting of n sensor nodes and one stations can be split into small ones to satisfy the model. Each sensor node is equipped with a omnidirectional antennas, m radios for in total k channels throughout the network, where k>m.

2.2 Attacker Model

We consider both a basic attacker model and advanced attacker models in this paper.

2.3 Basic Attacker Model:

Three concepts are introduced to complete this model.

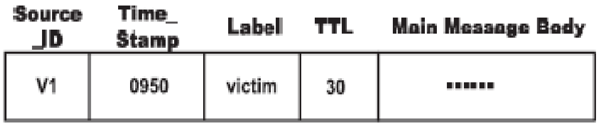
Jamming range(R): Similar to the sensors, the jammers are equipped with omnidirectional antennas with uniform power strength on each direction. The jammed area can be regarded as a circle centered at the jammer node.

Triggering range(r): On sensing an ongoing transmission, the decision whether or not to launch a jamming signal depends on the power of the sensor signal Ps.

Jammer distance: Any two jammer nodes are assumed not to be too close to each other, i.e., the distance between jammer J1 and J2 is ð(J1; J2) > R.

2.4 Advanced Attacker Model:

To evade detections, the attackers may alter their behaviors to evade the detection, for which two advanced reactive jamming models: probabilistic attack and asymmetric response delay time.



Source _ID	Time_ Stamp	Label	TTL	Main Message Body
V1	0950	victim	30	******

Fig1: sensor periodical status report message

2.5 SENSOR MODEL

Besides monitoring the assigned network field and generating alarms in case of special events, each sensor periodically sends a status report message to the base station. The header is designated for anti-jamming purpose, which is 4-tuple: **Sensor_ID** as the ID of the sensor node, **Time_Stamp** as the sending out time indicating the sequence number, as well as a **Label** referring to the nodes current jamming status, and **TTL** as the time to live field.

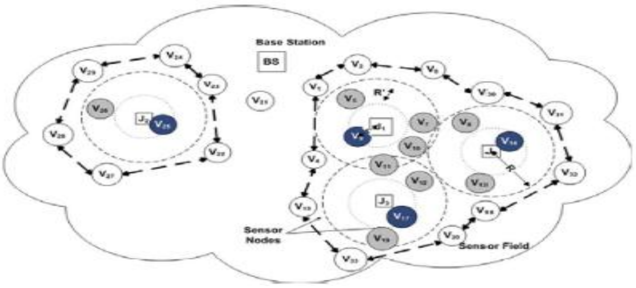


Fig 2: Nodes in Gray and Blue are victim nodes
And in blue is also a trigger node.

3. Kernal Techniques

3.1 Error Tolerant Randomized Non- Adaptive Group Testing:

Group testing was proposed since WWII to speed up the identification of affected blood samples from a large sample population. The traditional method of grouping items is based on a designated 0-1 matrix Mt, n where the matrix rows represent the testing group and each column refers to an item.

3.2 Minimum Disk Cover in a Polygon:

Given a simple polygon with a set of vertices inside, the problem of finding a minimum number of variable radii disks that not only cover all the given vertices, but also are all within the polygon, can be efficiently solved.

3.3 Cliques-Independent Set:

Clique-Independent set is the problem to find a set of maximum number of pair wise vertex disjoint maximal cliques, which is referred to as maximum clique-independent set.

4. Trigger Node Identification

The decentralized algorithm for trigger identification is a light weight procedure and the calculations are occur at the base station, the transmission overhead and complexity is low.
3 main steps of the procedure follow:

4.1 Anomaly Detection:

The base station detects potential reactive jamming attacks; each boundary node tries to report their identities to the base station. The base station waits for the status report from each node in each period of length P. If no reports have been received from node v with a maximum delay time, then v will be regarded as victim.

4.2 Jammer Property Estimation:

The base station calculates the estimated jammed area and jamming range R based on the locations of the boundary nodes.

4.3 Trigger Identification:

a. Base station creates an encrypted message Z and broadcast to all boundary nodes.
b. Boundary nodes keep broadcasting the Z to all victim nodes in the area.
c. All victim nodes execute the procedure and identify themselves as trigger or non-trigger.

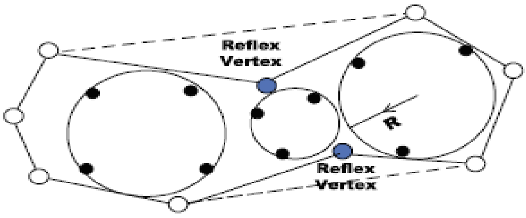


Fig 3: Estimated R and jammed area

4.4 Discovery of Interference Free Items:

It is possible to discover the set of victim nodes within the same jammed area, i.e., with a distance R from the same jammer node. Any two nodes within the same jammed area should be at most 2R far from each other.

4.5 Estimation of Trigger Upper Bound:

As mentioned in the attacker model, r depends not only on power of both sensors and jammers, but also the jamming threshold θ and path loss factor ζ.

$$\mathbf{r \geq ((Pn.\theta) / (Ps.Y))^{\wedge}(1/\zeta)}$$

4.6 Analysis of Time and Message Complexity:

4.7 Time complexity:

By time complexity mean the identification delay counted since the attack happens till all nodes successfully identify themselves as trigger or non-trigger. Therefore, the complexity break downs into four parts:

[1] Detection of interference signals at local links Td.
[2] Routing of sensor report to the base station from each sensor node, and the schedule to each victim node from the base station, aggregated as Tr.
[3] Calculation of CIS and R at the base station Tc;
[4] Testing at each jammed area Tt.

4.8 Message Complexity:

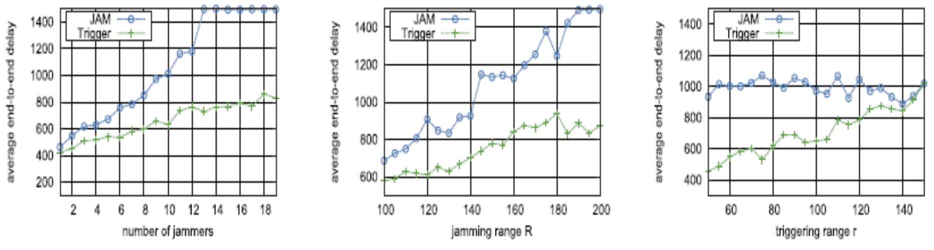
On the one hand, the broadcasting schedule Z from the base station to all victim nodes costs O(n) messages in the worst case.On the other hand, the overhead of routing reports toward the base station depends on the routing scheme used and the network topology as well as capacity.

5. Experimental Evaluation

5.1 Overview:

As a lightweight distributed trigger-identification service, our solution will be experimentally evaluated from four facets:

[1] In order to show the benefit of this service, we compare it with JAM in terms of end-to-end delay and delivery ratio of our routes from the base station to all the sensor nodes.
[2] In order to show the acceleration effect of CIS we compare the complexity solution with varying parameters.
[3] In order to show the accuracy of estimating the jamming range we provide the range and error rate using disk cover algorithm.
[4] In order to show its performance and robustness toward tricky attackers, we assess its false positive/negative rate and the estimation of R, for those two advanced jammer models.



(a) Average end-to-end delay by J (b) Average end-to-end delay by R (c) Average end-to-end delay by θ

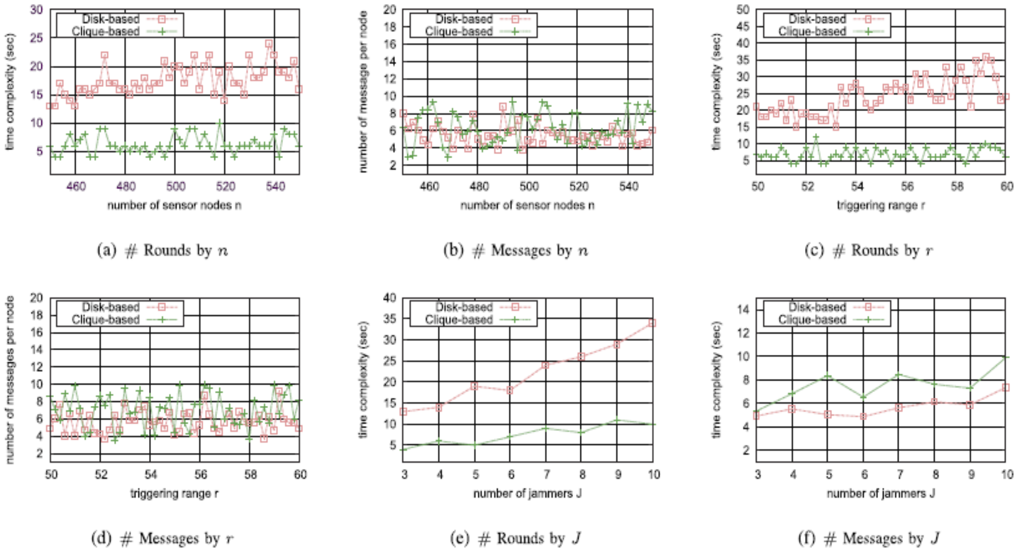
Fig 4: Benefits of Routing

5.2 Benefits for Jamming Routing:

This method is dedicated for proactive jamming attacks, which sacrifices significant packet delivery ratio due to unnecessarily long routes selected, though the effects of jamming signals are avoided. The length of routes based on JAM quickly climbs up to the upper bound, while that of our trigger method is much lower and more stable.

5.3 Improvements on Time Complexity:

The time complexity of our new clique based detection s proved to be asymptotically lower than the previous. Parameter values lower than these intervals would make the sensor network less connected and jamming attack less severe, while higher values would lead to impractical dense scenarios and unnecessary energy waste.



(a) # Rounds by n (b) # Messages by n (c) # Rounds by r

(d) # Messages by r (e) # Rounds by J (f) # Messages by J

Fig 5: Time and Message Complexity

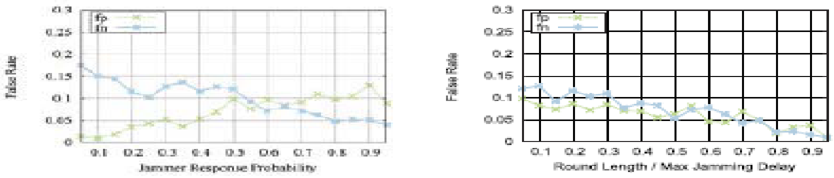
5.4 Accuracy in Estimating Jammer Properties:

Two observations are straightforward from these results:

[1] All the estimated values are above the actual ones, however, less than 10 percent difference. This meets our
[2] requirement for a tight upper bound of R.
The error rates in the case of fewer jammers are lower than those with more jammers. This is because the jammer areas can have larger overlaps, which introduces estimate inaccuracies.

5.5 Robustness to various Jammer Models:

Jammers in the simulation respond each sensed transmission with probability 0.5 as well. All the simulation results are derived by averaging 10 instances for each parameter team. We consider the extreme cases where jammers respond transmission signals with a probability as small as 0.1, or delay the signals upto 10 testing rounds later.



(a) Probabilistic Jammer Response (b) Random Jamming Delay

Fig 6: Solution Robustness

6. Further Enhancement

We further enhance our work to give more protection for trigger nodes. Trigger nodes will be given a **security code** to have protected communication once they had been identified. By doing this problem is controlled from spreading over the entire network. And we are **using Channel Surfing** to prevent from jamming. That means when we transmit a data successfully the channel was changed for next data.

7. Conclusion

Thus we are providing an efficient trigger identification service framework, we leverage several optimization problem models and provide corresponding algorithms to them, which includes the clique-independent problem, randomized error-tolerant group testing, and minimum disk cover for simple polygon. The efficiency of this framework is proved through both theoretically analysis toward various sophisticated attack models and simulations under different network settings.

References

[1] W. Hang, W. Zanji, and W. Jingbo, "Performance of DSSS against Repeater Jamming", Proceeding IEEE13thInternational conference Electronics, Circuits and systems 2006.

[2] I. Shin, Y. Shen, Y. Xuan, M.T. Thai, and T. Znati, "Reactive Jamming Attacks in Multi-Radio Wireless Sensor Networks: An Efficient Mitigating Measure by Identifying Trigger Nodes," Proc.

[3] Second ACM Int'l Workshop Foundations of Wireless Ad Hoc and Sensor Networking and Computing ,in conjunction with MobiHoc, 2009.

[4] M. Strasser, B.Danev, and S. Capku, "Detection of Reactive jamming in Sensor Networks", ACM Trans. Sensor Networks, vol.7, pp. 1-29, 2010.

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

[6] W. Xu, T. Wood, W.Trappe, and Y. Zhang, "Channel Surfing and Spatial Retreats: Defenses against Denial of Service", Proc. ACM Workshop against Denial of Service