A Novel Method for Jammer Localization in Large Scale Sensor Networks

Adoor Vikramaditya Rau[#1], Raghuvara R[#2], Vikram Shashimohan[#3], Muralidhar Kulkarni[#4]

[#]*Department of Electronics and Communication Engineering,*
National Institute of Technology Karnataka (NITK), Surathkal

[1]adoor8888@gmail.com

[2]raghuvara.ravikumar@gmail.com

[3]vikram788@gmail.com

[4]mkulkarni@nitk.ac.in

Abstract—**Sensor networks, by their very nature, are vulnerable to network security threats, with Denial of Service by radio jamming being one of the most common. It is more useful to detect jamming reactively than to proactively avoid it. We describe a method of countering jamming wherein some nodes just outside the jammed region form *groups* and transmit their locations to the Base Station for localization. These nodes are *downstream* in the hop-count based gradient broadcast routing sense. We also estimate the exact position of the jammer using the centre of curvature method. Simulation results show that the error in estimation of the jammer location is as low as 1.03m, accurate enough for real-time response.**

I. INTRODUCTION

A wireless sensor network is an ad-hoc network of nodes, each of which has an RF transceiver, a processing unit (a low-power microprocessor or a DSP chip), a memory unit and a battery - all enclosed in a s mall package. These networks are primarily used for information gathering, as opposed to computation or communication. Typical sensor network applications include proactive monitoring (where data is collected and transmitted at regular intervals of time), such as environmental and industrial sensing, and reactive event detection (where events/anomalies are detected and only then are transmissions made reporting them), such as structural monitoring, detection of forest fires and detection of intrusions into secure spaces like national borders.

As these networks are resource constrained, they are vulnerable to threats such as Denial of Sleep and Denial of Service attacks. This paper seeks to address the issue of radio jamming, which is the most common form of Denial of Service attacks.

Jamming is a high-priority event that precedes intrusion detection because it effectively disrupts the network's functioning, thereby allowing intrusions to go undetected. Additionally, the jammer's area of influence (range) is much larger than that of an intruder (the sensors' sensing range), and is therefore easier to detect. Jamming attacks can be countered by physical layer defences [1, 2] (coding, channel hopping, etc.), but these methods invariably require complex hard ware and large power, which makes them unfeasible. Therefore, it is more useful to *detect* jamming and localize the jammer than to completely *avoid* it.

This paper addresses the issue of radio jamming and proposes a technique for global detection of jamming where only the nodes downstream with respect to the sender participate in group formation. We also propose the centre of curvature method to localize the jammer and estimate its position to a satisfactory degree of accuracy.

II. BACKGROUND AND RELATED WORK

The issues of jamming detection and counter-measures have been studied extensively in the context of Wireless Sensor Networks. While some of the existing methods detect jamming, some others modify routing to avoid jammed areas, and even others completely avoid jamming by employing coding, channel hopping etc.

In [1], Stankovic et al. define different types of energy efficient jamming attacks and propose defences against each in the form of encryption, channel hopping, packet fragmentation and redundant encoding. Cakiroglu et al. make use of energy consumed, Received Signal Strength Indicator (RSSI), Packet Delivery Ratio (PDR), Packet Send Ratio (PSR) and combinations of two or more of these to detect jamming in [2]. The CUSUM method of sequential change detection has been discussed by Page in [11].

Wood et al. address the issue of detecting jamming and mapping the jammed area in [3]. Xu et al. propose methods for jamming detection that involve RSSI, carrier sensing time, PDR and combinations of these in [4].

Localization algorithms in WSNs are divided in two broad

978-1-4244-7202-4/10/$26.00 ©2010 IEEE

categories: range-based and range-free techniques. Range-based techniques estimate the actual distance between an unknown node and special nodes, called anchor nodes whose positions are known. Range-based localization can be performed using various parameters such as RSSI [5, 6], timing difference [7] and the angle of arrival [8]. Range-free localization schemes, on the other hand, are indirect techniques as they do not involve measurement of actual distances between the unknown nodes and the anchor nodes, but instead use parameters like hop count [9], etc. However, none of these schemes can be used to localize a jammer as they rely on a co-operative entity or use extra hardware.

III. Global Detection of Jamming

A. Assumptions

The following assumptions are made while modelling the network and the jammer

- The network is flat and asynchronous – all nodes are equivalent in functionality, and have no knowledge of the sleep schedules of other nodes.
- Nodes know their own geographical locations.
- The network uses a hop-count based gradient broadcast routing protocol – packets are routed downstream, from nodes with higher hop -counts to those with lower hop-counts.
- Nodes transmit at a fixed, preset power level, are static post-deployment.
- The network is broadcast in nature – nodes do not directly address neighbours.
- The jammer has infinite energy, and jams continuously in time i.e., it is a constant active jammer
- The jammer's radius (of area of influence) is much larger than the sensing radius and the communication radius of the nodes.

B. The Proposed Algorithm

Detection of jamming is a combination of local detection– occurring at the node level and global detection, occurring at the network level. A simple, inexpensive method of local detection is the CUSUM technique, which is a sequential change detection technique [11]. We propose a novel algorithm for global detection of jamming:

- Jammed nodes locally detect jamming (based on CUSUM) and periodically transmit "*I AM JAMMED!*" messages, overriding the MAC protocol.
- The message includes the sender's node ID and location information (LI).
- Nodes that receive these messages participate in the localization of the jammer *only if they are downstream* with respect to the sender.
- The group formation is initiated after a wait period T_w (starting with the first alarm received), when all distinct "*I AM JAMMED*!" messages have been received.
- The first node to complete this wait period broadcasts the Ids and LIs of all the jammed nodes it has heard from (called a local group), along with its own hop count.
- All one hop neighbours that have heard jammer alarms compare their local groups and append any new members to form a new group.
- This process continues till local groups of all one hop neighbours are stabilized. This process is limited by a timer T_g which depends on the number of nodes in the group. If the average number of such nodes is n, then

$$max(T_g) \propto (T_{packet}.\ n!)$$

where T_{packet} – Time taken for one packet transmission.

- A local leader is selected with lowest hop count (and hence closest proximity to the Base Station) by comparison with its local group. This node transmits the local group information to the Base Station.
- Localization of the jammer is completed at the Base Station (with higher computational capacity).

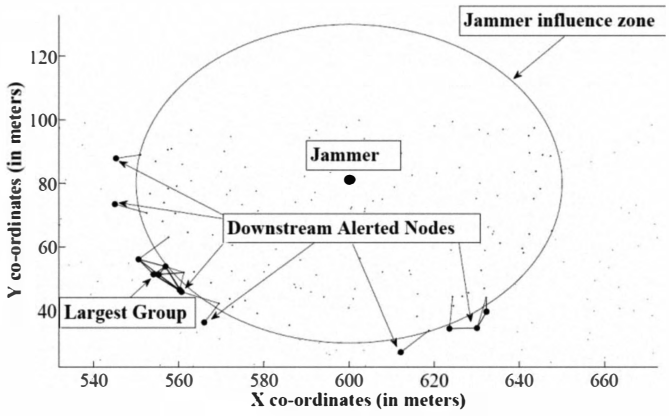

Fig.1 Group formation with only downstream nodes participating

IV. LOCALIZATION

Once the packets from the various groups formed at the circumference of the jammer's area of influence reach the base station, the location of the jammer must be estimated.
The jammer's region of influence is assumed to be circular owing to the omni-directionality of its antenna. The jammer's location can thus be assumed to be at the centre of this circle. We propose to use the least squares method, hitherto unused for jammer localization, to address this problem. The algorithm is described in [10], which seeks to minimize Δ, where:

$$\Delta = (X - a_0)^2 + (Y - b_0)^2 - r^2 \qquad (1)$$

where

$$X = X' - mean(X')$$
$$Y = Y' - mean(Y)$$

and
X' – x-coordinates of the alerted nodes
Y' – y-coordinates of the alerted nodes
a_0 – x-coordinate of jammer's estimated location
b_0 – y-coordinate of jammer's estimated location
r – best-fit circle radius

This is shown to reach the minimum value when

$$r^2 = mean((X - a_0)^2 + (Y - b_0)^2) \qquad (2)$$

Substituting this value in (1), rearranging the terms and taking into account

$$mean(X) = 0$$
$$mean(Y) = 0$$

we get

$$a_0 X + b_0 Y = \frac{1}{2}(X^2 - mean(X^2) + Y^2 - mean(Y^2)) \qquad (3)$$

which can be solved to obtain the centre of the circle.

V. EVALUATION

A. Simulation Methodology

The proposed global detection algorithm was evaluated in terms of the number of groups and the number of members in each group, over several iterations on MATLAB with the following network parameters:

Length of ROI: 1000m
Width of ROI: 100m
Number of nodes: 1000
Jamming Radius Rj: 50m
Communication Radius R_c: 10m

The algorithm for jammer localization was evaluated similarly to obtain a distribution of the error in position.

B. Results

With a large likelihood of 2-7 sensor nodes in the largest group (Fig. 2.), the number of packets generated to report jamming to the base station is reduced. This reduces the energy consumption, and prevents flooding of the network with redundant packets.

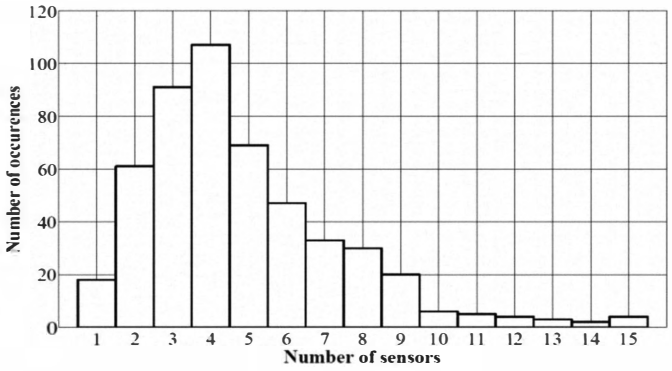

Fig. 2 Distribution of number of members of the largest group, with all nodes reporting

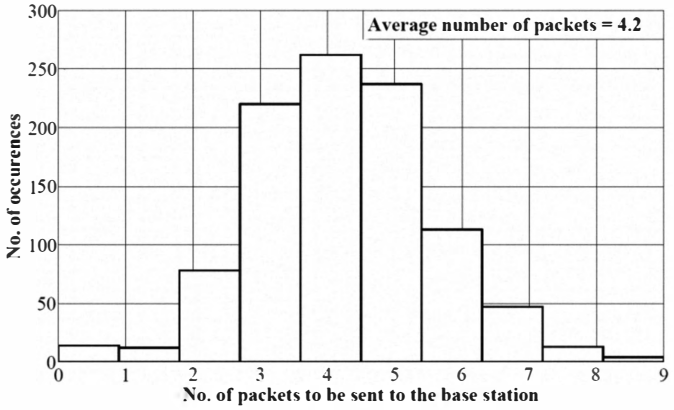

Fig. 3 Histogram of number of reporting downstream groups

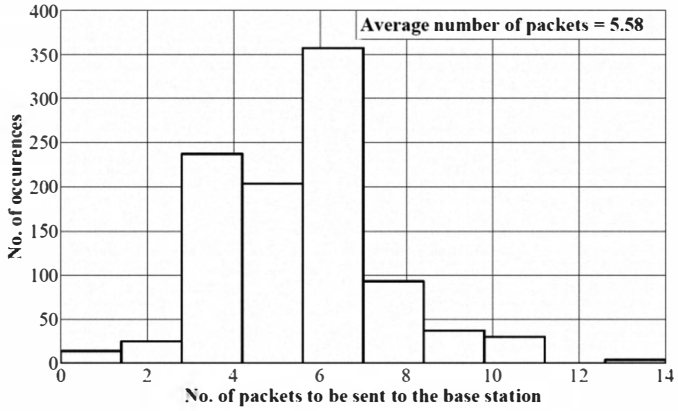

Fig. 4 Histogram of number of reporting groups, with all groups reporting

From Figs. 3 and 4, the average number of groups formed during global detection and jammer localization is quite small: 4.2 with only downstream nodes reporting, and 5.58 with all nodes reporting. Since each group generates only one packet, the number of packet transmissions also reduces.

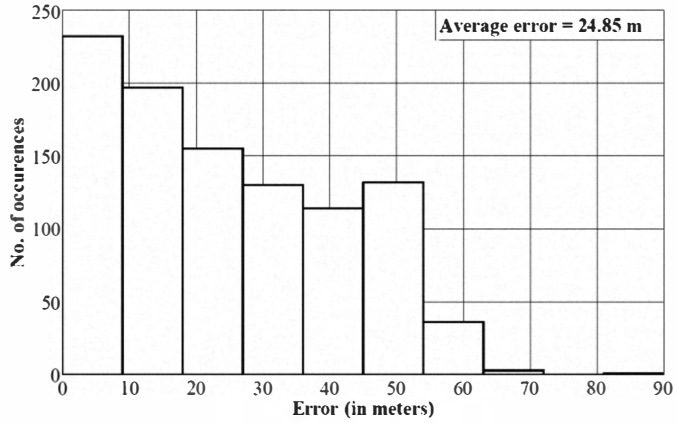

Fig. 5: Distribution of jammer localization error with only the largest downstream group reporting

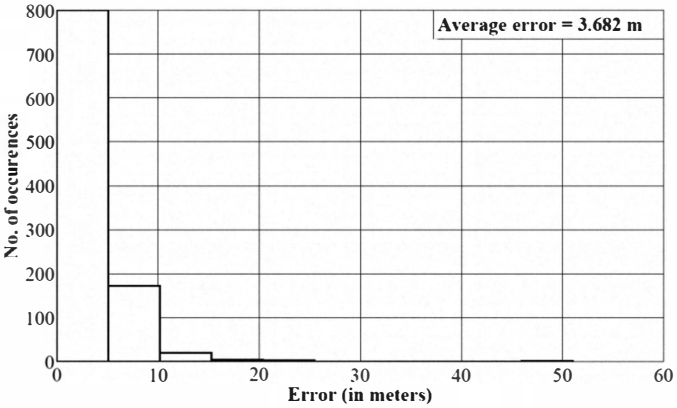

Fig. 6: Distribution of jammer localization error with all downstream groups reporting

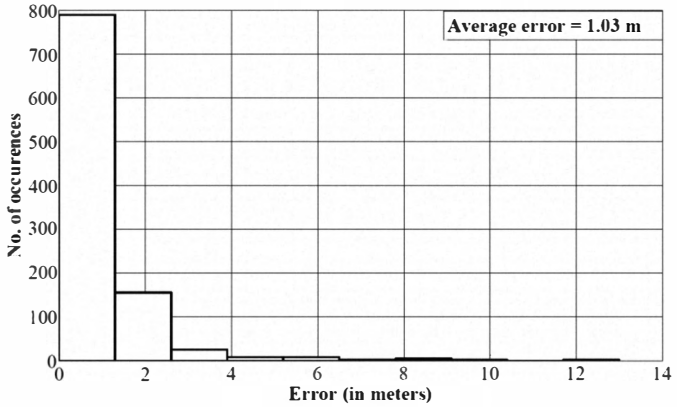

Fig. 6: Distribution of jammer localization error with all groups reporting

From Figs. 5,6 and 7, we see a decrease in the jammer position error with increase in the number of groups participating in the global detection process (as expected). The decrease is very sharp (24.85m to 3.682m) from the case where only the largest downstream group reports (hence generating only one packet) to the one with all downstream nodes reporting.

The decrease is lesser between the cases with only downstream groups reporting (3.682m) and all groups reporting (1.03m). However, the trade-off here involves not only more packets, but also increased time for jammer localization (routing of packets from upstream groups).

Furthermore, situations may arise where links have to be reversed for packets to be routed from upstream groups to the Base Station, which results in a further increase in the number of packets, the time taken and the energy consumed.

VI. Conclusions

In this paper, a novel scheme for global detection of jamming and jammer localization has been proposed, which results in fairly accurate estimation of the jammer's location. By using only downstream nodes, the algorithm reduces the number of packet transmissions required, and hence the time taken and energy consumed in the process. Localization is carried out at the computationally more capable Base Station, thereby allowing for fast, accurate jammer localization. Future work may include extending the algorithm to more sophisticated jamming attacks, and also mobile jammers.

References

[1] Anthony D. Wood, John A. Stankovic, and Gang Zhou, "DEEJAM: Defeating Energy-Efficient Jamming in IEEE 802.15.4-based Wireless Networks", *IEEE Communications Society Conference on Sensor, Mesh and Ad-Hoc Communications and Networks*, 2007

[2] Murat Çakıroglu and Ahmet Turan Özcerit, "Jamming Detection Mechanisms for Wireless Sensor Networks", *3rd International Conference on Scalable Information Systems*, 2008

[3] Anthony D.Wood, John A. Stankovic, and Sang H. Son, "JAM: A Jammed-Area Mapping Service for Sensor Networks", *The Real Time Systems Symposium*, 2003

[4] Wenyuan Xu, Wade Trappe, Yanyong Zhang and Timothy Wood, "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks", *Proceedings of ACM International Symposium on Mobile Ad Hoc Networking and Computing (Mobihoc)*, 2005, pp. 46-57

[5] Paramvir Bahl and Venkata N. Padmanabhan, " RADAR: An In-Building RF-based User Location and Tracking System", *IEEE Infocom*, 2000

[6] Paolo Barsocchi, Antonio Blasco Bonito, Stefano Chessa, "Localization in open fields by using RSSI on IEEE 802.15.4", *15th IMEKO TC4 Symposium on Novelties in Electrical Measurements and Instrumentation*, 19-21 September, 2007, Iasi, Romania, pp. 1154-1160.

[7] Andy Ward, Alan Jones, Andy Hopper, "A New Location Technique for the Active Office", *IEEE Personal Communications*, Volume 4, Issue 5, Oct 1997, pp. 42-47

[8] N. Priyantha, A. Chakraborthy and H. Balakrishnan, "The Cricket Location-Support System" *in Proceedings of International Conference on Mobile Computing and Networking*, 2000, Boston, MA, pp. 32-43

[9] Sungwon Yang, Jiyoung Yi and Hojung Cha, "HCRL: A Hop - Count - Ratio based Localization in Wireless Sensor Networks", *Fourth Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks* , 2007, San Diego, C.A.

[10] URL:http://www.mathworks.com/matlabcentral/newsreader/view_thread/152405

[11] E. S. Page, "Continuous inspection schemes", *Biometrika*, vol. 41, 1954