International Journal of Computer Science & Mechatronics
A peer reviewed international journal | Article Available at www.ijcsm.in | ICI-JIF-5.381
©smsamspublications.com | Vol.4.Issue.2.2018

Anti-Jamming Strategy for Wireless Network

ISSN: 2455-1910

Mr. Pavan Gunda[1], Ms. Ramalakshmi Boyapati[2],
[1]Assistant Professors of IT, [2]Assistant Professors of CSE,
SIR CR Reddy College of Engineering, Eluru, AP.INDIA.
Email: gsraghupavan9@gmail.com, ramalakshmi.boyapati@gmail.com

ABSTRACT: Jamming attacks can severely interfere with the normal operation of wireless networks and, consequently, mechanisms are needed that can cope with jamming attacks. No single measurement is sufficient for reliably classifying the presence of a jammer is an important observation. Various detection schemes are developed based on measurements which can remove ambiguity when detecting a jammer. But the major drawback of the existing approaches is that the complete processing and decision making while detecting the jammer is done at the node level where nodes are resource-starved and so nodes may not be able to communicate with others during jamming. In this paper, we propose an anti-jamming mechanism where detection is done network level means at base station. Here, the base station computes a Jamming Index (JI) for each node and asserts its validity and then decide the lower cut-off value of JI to conclude that all nodes whose JIs are greater than the lower cut-off value are 'Jammed' while the others are 'Not Jammed'. Our proposed mechanism is robust and economical.

Keywords: -Jamming, Jamming Index (JI), radio jamming…

I **INTRODUCTION:** Wireless networks are progressively becoming more affordable, and consequently are being deployed in a variety of different modalities, ranging from wireless local area networks to mesh and sensor networks. The shared nature of the wireless medium, combined with the commodity nature of wireless technologies and an increasingly sophisticated user-base, allows wireless networks to be easily monitored and broadcast on. Adversaries may easily observe communications between wireless devices, and just as easily launch simple denial of service attacks against wireless networks by injecting false messages.

To ensure the dependability of future deployments of wireless networks, mechanisms are needed that will allow wireless networks of all types to cope with the threat of jamming attacks. Jamming can disrupt wireless transmission and can occur either unintentionally in the form of interference, noise or collision at the receiver side or in the context of an attack. A jamming attack is particularly effective since (i) no special hardware is needed to be launched, (ii) it can be implemented by simply listening to the open medium and broadcasting in the same frequency band as the network and (iii) if launched wisely, it can lead to significant benefits with small incurred cost for the attacker.

This paper examines how radio jamming may be conducted and explores the task of detecting jamming attacks. The ability of wireless devices to detect that they are jammed allows the wireless network to identify regions of poor radio conditions, and therefore take an appropriate response to such threats. We propose an anti-jamming method. For each node, the base station computes a Jamming Index (JI) based on fuzzy inference and asserts its validity. The jamming detection is done by the base station based on the input values of the jamming detection metrics received by it from the respective nodes.

II RELATED WORK: Radio interference attacks are a serious threat to the operation of a wireless network, regardless of the type of wireless network. To cope with such threat of jamming attacks, it is important to understand the different threat models that may be employed by adversaries, the methods that are needed to diagnose these threats, and the counter measures that may be employed to defend against jamming attacks.

Xu *et al.* carried out intense study of the jamming attack detection mechanism with experiments using the MICA2 Mote platform. Firstly, they collected data about various percentages of the PSR and PDR (measured at the transmitter end) for constant, deceptive, random, and reactive jammers. They then studied the levels of carrier sensing time, energy consumption, and the received signal strength as well as the received signal spectrum under normal and jamming conditions for two application layer protocols: Constant Bit Rate (CBR) and Maximum Traffic and tried to identify the jammer type through spectral discrimination using the Higher Order Crossing (HOC) method. They conclude that if PDR is used with consistency checks like, checking own PDR and signal strength and comparing the same with those of the neighbors, and/or ascertaining own distances from the neighbors, then the combination can very effectively detect and discriminate various forms of jamming.

Rajani *et al.* use '*the swarm intelligence and ant system'* wherein they create an agent (ant) which proactively uses the WSN node's information (key performance parameters), as it traverses a route from node to node, to predict or anticipate jamming, and accordingly, changes the route to avoid jamming.

Cakiroglu *et al*. have proposed two algorithms for detecting a jamming attack. The first algorithm is based on threshold values of three detection parameters: Bad Packet Ratio (BPR), Packet Delivery Ratio (PDR), and Energy Consumption Amount (ECA). If all three parameters are below the thresholds, or if only the PDR exceeds the threshold, then it is concluded that there is no jamming; otherwise, there is jamming. The second algorithm is an improvement over the first one where the neighboring nodes' conditions, ascertained through queries to be raised and replies there-to to be received within the threshold time periods, are also considered to enhance the jamming detection rate. The results of the simulations are very encouraging, thus establishing the effectiveness of the algorithms.

III METRICS FOR JAMMING ATTACK DETECTION: The main objective of any jammer is to be interfering in legitimate wireless communications. By either preventing a real traffic source from sending out a packet, or by preventing the reception of legitimate packets, a jammer can achieve this goal. In this paper for jamming detection, we selected two metrics. They are:

Signal-to-Noise Ratio (SNR): SNR is calculated as the ratio of the received signal power at a node to the received noise power (or jammer power) at the node. It is almost an effective metric to identify a jamming attack at the physical layer as there can be no jamming at the physical layer without the SNR dropping low.

Bad Packet Ratio (BPR): BPR as the ratio of the number of bad packets received by a node to the total number of packets received by the node over a given period. We find BPR to be a very effective metric which can indicate all types of jamming, is easily calculable. The number of bad packets and the number of total received packets are readily available for computing the BPR without imposing any significant burden on the system.

Along with above two metrics, we are using the following two metrics which are used to measure the effectiveness of a jammer:

Packet Send Ratio (PSR): The ratio of packets that are successfully sent out by a legitimate traffic source compared to the number of packets it intends to send out at the MAC layer. The PSR can be easily measured by a wireless device by keeping track of the number of packets it intends to send and the number of packets that is successfully sent out.

Packet Delivery Ratio (PDR): The ratio of packets that are successfully delivered to a destination compared to the number of packets that have been sent out by the sender. If no packets are received, the PDR is defined to be 0.

IV ANTI-JAMMING METHOD: Existing jamming detection methods are decentralized approaches means detection is done at node level. But our proposed Anti-jamming method follows a centralized approach; where in the jamming detection is done by the base station based on the values of the metrics received by it from the respective nodes. Mainly, there are three inputs required to be sent by the nodes to the base station:

1) The number of total packets received by it during a specified time,

2) The number of packets dropped by it during the period, and

3) The received signal strength (RSS).

The received signal strength (RSS) is defined as the power content of the radio signal received at the receiver. It is a measurable quantity and can either be measured by the RF power meter of the node or can be calculated using formulae as per the selected propagation model. The RSS by itself is not a logical metric to indicate jamming.

A jammer may not only prevent a wireless node from sending out packets but may also corrupt a packet in transmission. Consequently, we next evaluate the feasibility of using packet delivery ratio (PDR) as the means of detecting the presence of jamming. The packet delivery ratio can be measured in the following two ways:

(a) At the sender side, the PDR can be calculated by keeping track of how many acknowledgements it receives from the receiver.

(b) At the receiver side, the PDR can be calculated using the ratio of the number of packets that pass the CRC check with respect to the number of packets (or preambles) received.

Initially, the base station computes the 'power received by the node from the jammer', if any, by finding the differential between the current RSS and normal RSS values. Thereafter, the base station computes the BPR and SNR from these values, as specified above. Then the base station uses the values of BPR and SNR as inputs to get 'Jamming Index' (JI) as output of the system. The JI value varies from 0 to 100, signifying 'No Jamming' to 'Absolute Jamming' respectively.

The fuzzy logic processing is used to estimate jammed index. A rule base, comprising of the range of rules consisting of fuzzy outputs corresponding to SNR and BPR fuzzy inputs, was formed using the opinion of experts with rich theoretical and practical experience in jamming and counter jamming disciplines of information warfare. The rule base was further refined by getting the system outputs by the experts. The rule base is given as follows:

1. If SNR is LOW and BPR is LOW then JI is HIGH.
2. If SNR is LOW and BPR is MEDIUM then JI is HIGH.
3. If SNR is LOW and BPR is HIGH then JI is HIGH.
4. If SNR is MEDIUM and BPR is LOW then JI is LOW.
5. If SNR is MEDIUM and BPR is MEDIUM then JI is MEDIUM.
6. If SNR is MEDIUM and BPR is HIGH then JI is HIGH.
7. If SNR is HIGH and BPR is LOW then JI is NO.
8. If SNR is HIGH and BPR is MEDIUM then JI is LOW.
9. If SNR is HIGH and BPR is HIGH then JI is MEDIUM.

Based on these fuzzy values, base station computes the jamming index (JI) value for each node which varies from 0 to 100. All legitimate nodes in the network will participate in the detection protocol by transmitting a baseline amount of traffic, e.g. by sending heartbeat beacons. This allows each node to reliably estimate PDR over a window of time and conclude that the PDR is 0 if no packets are observed during that time.

V CONCLUSION: Wireless networks are being deployed in a variety of forms, ranging from ad hoc networks to wireless LANs to sensor networks. The shared nature of the wireless medium will allow adversaries to pose non-cryptographic security threats by conducting radio interference attacks. In existing system, the decision for jamming detection is taken by the nodes themselves, which we consider not feasible due to the resource constraints of the WSN nodes and their ineffectiveness in communicating with other nodes during jamming. In this paper, we choose to do all processing and decision making at the base station on a holistic picture. By using signal strength or the packet delivery ratio individually, one is not able to definitively conclude the presence of a jammer. Having done so, we then selected bad packet ratio (BPR) and signal-to-noise ratio (SNR) as the input to fuzzy system based which gave the jamming index (JI) of various nodes as output.

VI REFERENCES:

[1] D. J. Thuente and M. Acharya, "Intelligent jamming in wireless networks with applications to 802.11b and other networks," in Proc. 25th IEEE Communications Society Military Communications Conference (MILCOM'06), Washington, DC, Oct. 2006, pp. 1–7.

[2] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," IEEE Computer, vol. 35, no. 10, pp. 54–62, Oct. 2002.

[3] Sudip Misra 1, Ranjit Singh 1 and S. V. Rohith Mohan," Mechanism for Wireless Sensor Networks Using a Fuzzy Inference System."

[4] I. F. Akyildiz, X. Wang, and W. Wang, .Wireless mesh networks: A survey, Computer Networks, vol. 47, no. 4, pp. 445.487, Mar. 2005

[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/Jun. 2006.

[6] Rajani, M.; Lisa, A.O. Jamming attack detection and countermeasures in wireless sensor network using ant system. Availableonline:http://www.cognitiveintelligence.com/documents/SPIE 2006.pdf/ (accessed on 12 October 2009 at 1:15 PM).

[7] Xu, W.; Trappe, W.; Zhang, Y.; Wood, T. The feasibility of launching and detecting jamming attacks in wireless networks. MobiHoc '05: In Proceedings of the Sixth ACM International Symposium on Mobile ad hoc Networking and Computing, Alexandria, VA, USA, 07-07 November 2005; pp. 46-57.

[8] C. Karlof and D. Wagner. Secure routing in wireless sensor networks: attacks and countermeasures. In Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications, pages 113-127, 2003.