International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Articles available online http://www.ijoer.in

Vol.3., Issue.2, 2015

RESEARCH ARTICLE

ISSN: 2321-7758

A NOVEL FRAMEWORK FOR MOBILE JAMMER LOCALIZATION IN WIRELESS SENSOR NETWORKS

P. PRIYA[1], S.UDHAYAKUMAR[2], PREMKUMAR[3]
[1]M.E Applied Electronics, Sri Eshwar College of Engineering, Coimbatore
[2]Assistant Professor,Sri Eshwar College of Engineering,Coimbatore
[3]Application Engineer, DFX Technology, Coimbatore

Article Received: 07/04/2015 | Article Revised on:14/07/2015 | Article Accepted on:17/07/2015

P. PRIYA

ABSTRACT
Jammers can severely disrupt the normal communications in wireless sensor networks by intentionally emitting radio frequency interference signals aiming at disturbing transceivers' operation. Jamming attacks may be viewed as a typical case of Denial of Service (DoS) attacks which may be defined as any event that diminishes or eliminates a network's capacity to perform its expected function. The information about position of jammers allows the defender to actively evade the jamming attacks. Reactive jamming attack is a light weight attack performed by the adversary, which are easy to launch but difficult to identify. Thus, the main objective of this paper is to provide a general overview on various techniques to identify the jamming attack and proposing a novel framework to identify and defend the reactive jammers in wireless sensor networks. The emphasis islaid on detecting the mobile reactive jammers. A brief overview on various jamming attack models is also reviewed.

Key words–Wireless Sensor Networks, Jamming Attack, Denial of Service, Mobile Reactive Jammer.

1. INTRODUCTION

Wireless Sensor Networks (WSNs) are widely used in many application areas including military applications, control and tracking applications, health related applications, and environment and habitat monitoring applications. It will become an issue of critical importance to provide security as these networks gain popularity. Wireless sensor networks, however, are susceptible to many security threats. One serious threat that is especially harmful is radio interference attack i.e. jamming attacks. Jamming is defined as the act of intentionally emitting electromagnetic energy towards a communication system to disrupt signal transmission. To ensure the successful deployment of wireless sensor networks, localizing the jammers becomes utmost important. As the adversaries are finding new ways to detect the confidential transmissions, there is a great need to think differently over the situation. Moreover the traditional ways of defending the attack is not satisfactory, a new approach towards this problem is necessary. Thus giving a new dimension as to how the security issues can be handled is proposed in

this paper i.e. not only by defending them but how to sense them instead and how-to evade them thus saving energy, time and computational complexities involved earlier.

Based on the characteristics, the jammer nodes have been classified as: (i)Constant Jammer, (ii)Deceptive Jammer, (iii)Random Jammer, (iv)Reactive Jammer. Among these jammers the most difficult to detect is there active jammer since compared to others which are active in nature i.e. they try to interrupt the channel without having any prior information of the traffic pattern on the channel while the reactive jammer stays quiet when the channel isidle, but starts transmitting a radio signal as soon as it senses some activity on the channel. Thus reactive jammers are harder to detect and needs more efficient identification and defending system. Most of the existing jammer localization approaches rely on utilizing indirect measurements such as packet delivery ratios [1], neighbor lists [2], and nodes' hearing ranges [3] are mainly focussed on localizing static jammer.

The proposed method includes intrusion detection based approaches. The main goal of this article is to provide a general overview on existing jammer localization schemes and cover all the relevant work, providing the interested researcher pointers for open research issues in this field and to provide a better optimization in mobile jamming detection.

The remainder of this article is organized as follows: Section 2 comprises an overview on various jamming attack models. Section 3 and Section 4 discusses about some of the basic and advanced techniques to identify the jamming attacks respectively. Section 5 analyzes about the advantages and limitations of existing techniques. Section 6 describes the proposed framework. Section 7 shows the experimental analysis of the proposed work. Finally Section 8 concludes the paper.

2. JAMMING ATTACK MODELS

In this section, we first define the characteristics of a jammer's behavior, and then enumerate metrics that can be used to measure the effectiveness of a jamming attack. These metrics are closely relatedto the ability of a radio device to either send or receive packets. We then introduce four typical jammer attack models that have proven to be effective in disrupting wireless communication.

2.1. Characteristics of a Jammer

A common assumption is that a jammer continuously emits RF signals, so that legitimatetraffic will be completely blocked. The common behaviour of all jamming attacks is that their communications arenot compliant with MAC protocols. The objective of a jammer is to interfere the wireless communications by either preventing a real traffic source from sending out apacket, or by preventing the reception of legitimate packets.

2.2 Metrics

2.2.1 Packet Send Ratio (PSR)

The PSRcan be easily measured by a wireless device by keeping track of the number of packets that are successfully sent out by the source and the number of packets that it intends to send out at the MAC layer. If Pintends to send out *n* messages, butonly *m*of them go through, the PSR is *m/n*.

2.2.2 Packet Delivery Ratio (PDR)

The PDRcan be easily measured by a wireless device by 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, then the PDR is defined to be 0.

2.3 Jammer Attack Models

There are four typical jammer attack models.

2.3.1 Constant Jammer

The constant jammer continuously emits a radio signal to the channel withoutfollowing any MAC-layer etiquette. Moreover, theconstant jammer does not wait for the channel to become idle before transmitting.Thus , a constant jammer can effectively prevent legitimate traffic sources from getting hold of channel and sending packets.

2.3.2 Deceptive Jammer

The deceptivejammer constantly injects regularpackets to the channel without any gap between subsequent packet transmissions.Thus a normalcommunicator will be deceived into believing there isa legitimate packet and will be duped to remain in thereceive mode.Hence, even if a node has packets to send,it cannot switch to the sendmode because a constantstream of incoming packets will be detected.

2.3.3 Random Jammer

A random jammer alternates between sleeping and jamming. After jamming for *tj* units of time, it stops emission and enters a sleeping mode for a period of

t_s units of time. It will resume jamming after sleeping for *ts* time.*tj*and *ts* can be either fixed or random values. A special feature about this model is that it tries to takeenergy conservation into consideration, which is especially important.

2.3.4 Reactive Jammer

The three models discussed above are active jammers which are usually effective because they keep the channel busy all the time. The reactive jammer stays quiet when the channel is idle, but starts transmitting a radio signal as soon as it senses activity on the channel. As a result, a reactive jammer targets to disrupt the reception of a message. The fact about the model is that a reactive jammer does not necessarily conserve energy because the jammer's radio must continuously be on in order to sense the channel. Another fact is that active jammers are relatively easy to detect whereas reactive jammers maybe harder to detect.

3. BASIC JAMMING DETECTION TECHNIQUES

The main focus is on the detection of the reactive jammers. This identification can be on the basis of radio interferences, or in a scenario where there is poor connectivity involving congestion and device failures. Thus it becomes very difficult to differentiate between jamming attack and a real time situation of congestion. Thus to have a detailed look at the situation many methods have been are there which are as follows:

3.1 Signal Strength

The most important method is to determine the strength of the signal by measuring and analyzing the signal strength distribution to have the account of the presence of the jammer. The approaches to detect the jamming signal involve comparing average signal magnitude with that of the threshold value calculated from the overall noise level.

3.2 Carrier Sensing Time

A constant Jammer keeps the channel busy thus preventing the source to send out packets hence carrier sensing time can be used to know whether the device is jammed or not. This is easy to determine whether a channel is idle or not comparing the noise level with the fixed threshold. To distinguish between jammed scenario and a congestion, sensing time in first will be bounded and in later sensing time will be unbounded. But in the case of reactive jammer, this method fails to detect the presence of jammer.

3.3 Packet Delivery Ratio

PDR refers tothe ratio of packets that are successfully delivered to a destination compared to the number of packets that have been sent out by the sender. But here detecting thereactive jammer is a mere challenge because in this packets are sent very rarely and typically only when it istriggered by some another signal. However PDR can beused to distinguish between the jamming scenario and a congested network scenario.

4.ADVANCED JAMMING DETECTION TECHNIQUES

The above discussed methods involve some basic statistical techniques which only can be used to get the information regarding whether there is a congestion in a network or ajammed situation. The adversaries may be in continuous efforts to disrupt thenetwork while the security experts would always find waysto defend them. Thus some of the methods currently used to eliminate the jammers are thefollowing techniques:

4.1 Channel Surfing

Radio communication operates usually on the single channel and therefore if any intruder comes in the range of the communication the communicating device may migrate toanother channel which is free of attacks. This probably happens in the physical layer of the network and is called as the frequency hopping. Using the above technique jammers can be avoided by continuously switching from one frequency channel to another until it finds the free channel to transmit its signal.

4.2 Spatial Retreat

This technique is appropriate in a mobile network where the communicating nodes are mobile. This technique can be used when there is a jammed area in a mobile network such as user with cell phones or WLAN. If the mobile nodes are disrupted by the jammer nodes then the mobile nodes should simply escape to a safe location where there is no interference.

4.3 Region and Signal to Noise Ratio Based Model

Network nodes are classified in to three categories: unaffected nodes, jammed nodes and boundary nodes, based on the level of disturbance due to jamming effects. Consider two jamming models: region based and signal-to-noise ratio, here the region based model determines the impact of jamming by examining received jammed signal strength on the victim nodes while the SNR based

model determines the SNR at the receiver which can estimate the jamming effects more accurately.

5. LITERATURE REVIEW

The basic techniques discussed earlier i.e. the RSS, CST,PDR, together has some disadvantages that they only focussed on identifying the interference in the signal. Though there are necessary schemes or methods by which the jamming signalscan be discovered but to locate the jammer nodes dependingon the signals and thereby securing the transmission from jamming attack is not solved yet.

The advanced techniques however make use of multiple frequency bandstand MAC channels also results in high computational overhead and excessive wastage of the frequency band which badly reduces the efficiency of the resource limited network environment. For example, in the channel surfing method the frequency hopping take place till it does not finda suitable channel free of any adversary. Thus if this happens frequently then itwill result in longer transmission duration and more energy consumption which is not fair and efficient. Major problem in the Spatial retreat is thatit has considered that the jammer is stationary but if the jammer is mobile then its movement may cause the network to become severely unbalanced. All these methods have assumed that that the jammers' capabilities are limited and power less to catch the actual traffic from the camouflage of these diversities. However the silent behaviour of reactive jammershave more powers to destruct the other mitigation methods.

6.PROPOSED FRAMEWORK

To overcome the disadvantages discussed in above section a novel method is proposed against reactive jamming attack in Wireless Sensor Network by exploiting the characteristics of reactive jammer. Reactive jammer nodes are those which remain idle when there is no activity in the channel but starts emitting radio signal if it senses the activity. Hence an intrusion detection scheme called game-theory based approach is used totrap the reactive jammer node.

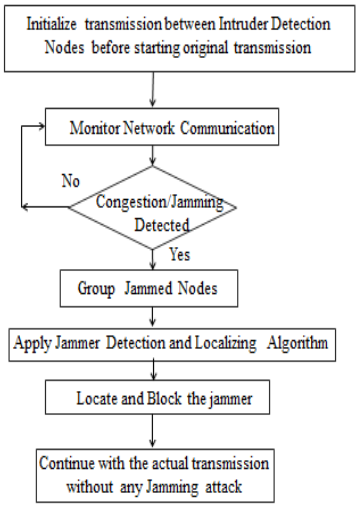


Fig.1. Proposed Framework Flowchart

The subtasks that has to be carried out are as foilows:

Step 1: Initialize Duplicate message transmission between intruder detection nodes.

Step 2: Monitor Network Communication for any interruption.

Step 3: Check whether Jamming or Congestion exists using jamming detection algorithm.

Step 4: If jamming is detected then apply jammer localizing algorithm to locate and trap the reactive jammer in the region of duplicate communication.

Step 5: Continue the real transmission without any jamming attack.

6.1 Intruder Detection Based Approach

The detection mechanism has been developed in such a way that the reactive jammer can be trapped by initialising the duplicate message transmission between intruder detection nodes. Since the reactive jammer starts emitting radio signal as soon as it senses the activity in the channel, it will be moved towards the direction of duplicate communication where it will be blocked and thereby the actual transmission will be carried out efficiently without any jamming attack.

6.1.1 Network Model

- Sensor Node:Sensor nodes are randomly deployed along with the intruder detection nodes. Duplicate sets of source and destination are designed to act as intruder detection nodes. All the sensor nodes remain static but the jammer is kept mobile till one round of simulation ends.Sensors will have omni-directionalantennas with uniform strength on each direction. Eachsensor node would

have a Sensor_ID so as to uniquelyidentify each sensor node in the network. Sensor nodeswould send a report message periodically between neighbor nodes.

- Jammer Node:Reactive jammers keep idle until they sense any ongoing legitimate transmissions and thenemit jamming signals to disrupt the communication till the sensor transmission finishes. Jammers wouldalso have omni-directional antennas. The jammed areacan be considered as a circle centred at the jammer node, with a radius R. All the sensors within this range will be jammed during the jammer wake-up period.

6.2 Jamming Detection With Consistency Checks

The idea behind this approach is to identify whether the packet was jammed or just sent over a weak link. Detection of jammer nodes cannot bedone through the basic methods and it requires some advanced detection strategies such as to combine PDR with the Signal strength which can give more efficient results compared to the basic methods. This can be achieved as follows: Whenever a node receives a packet transmission, it not only receives the packet, but also records the RSS andPDR for each node.

The intention behind this process is that if the RSS value is Low and PDR is either Zero or Low, this indicates that itis non-jammed or neighbor failure or neighbor absence, butif the RSS value is High and PDR is either Zero or Low, this indicates thatthe node is jammed. So by analyzing these two values for each victim node wecan detect jamming in the network.

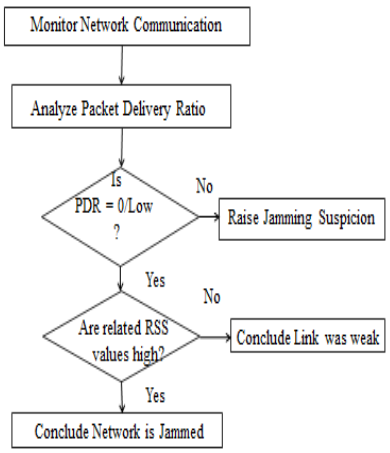


Fig.2. Jamming Detection Flowchart

In a normal scenario, where there are no interference or software faults, high signal strength corresponds to a high PDR. However, ifthe signal strength is low, which means the strength of the wireless signal is comparable to that of the ambient noise floor, the PDR will be also low. On the other hand, a low PDR does not implylow signal strength. So it is necessary to check the consistency of PDR measurements with observed signal strength readings.

Initially intruder detection nodes are involved in the communication in the network but when thenetwork gets jammed, from the victim nodes under that jammedarea we can check whether the PDR and Signal strength measurements are consistent with each other or not.

6.2.1 Jamming Detection Algorithm

Based on the above observations in the PDRSS_Detect_Jam algorithm, a wireless node will finalize that it is not jammed if at least one of its neighbors has a high PDR value. Jamming detection algorithm that checks the consistency of PDR measurements with observed signal strength readings is given below.

```
PDRSS_Detect_Jam
{PDR(N): N∈ Neighbors} = Measure_PDR()
MaxPDR = max{PDR(N): N∈ Neighbors}
If MaxPDR< PDRThresh then
SS = Sample_Signal_Strength()
CCheck=SS_ConsistencyCheck(MaxPDR,SS)
If CCheck== False then
Post NodeIs Jammed()
End
End
```

In the PDRSS_Detect_Jam algorithm, however, if allneighbors' PDR values are low then the node mayor maynot be jammed so we need to further check thepossibilities by measuring the received signal strength. The function Sample_Signal_Strength() reactively measures the signal strength values for a window of time after thePDR values fall below a threshold and returns the maximum value of the signal strengths denoted as SSduring the sampling window. It is noticed that the duration of the sampling window should be carefully carried out basedupon the jamming mode, and the traffic rate. The function SS_ConsistencyCheck() takes as input themaximum PDR value of all the neighbors, denoted as*MaxPDR*,and the signal

strength reading *SS*. A consistency checkis performed to see whether the low PDR values are consistent with the signal strength measurements. If the signal strength *SS* is too large to have produced the observed

MaxPDR value, then SS_ConsistencyCheck() returns False,else it returns True. Thus the jammer is detected and localized in the duplicate network communication scenario itself. As the jammer is localized and trapped between the duplicate message transmission, we can continue the real network communication without any jamming attack. Since the mobile reactive jammers spend energy in listening the channel as well as emitting radio interference the power of the jammer will get diminished.

6.3 Jammer Localizing Algorithm

The communication range defines a node's ability to communicate with others, and it comprises the following two components: the hearing range and the sending range.

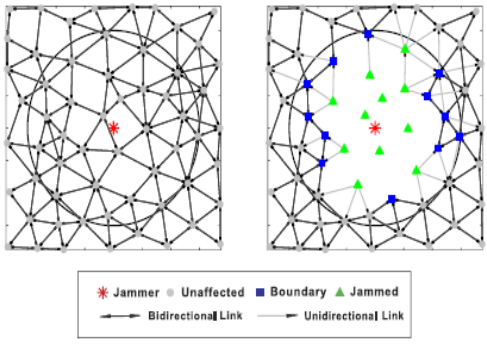
- The hearing range: Consider Node P as a receiver, the hearing range of P specifies the area withinwhich the potential transmitters can deliver theirmessage to P, e.g., for any Transmitter S in P'shearing range, $(SNR)_{S\to P} > \gamma_o$.
- The sending range: Consider P as atransmitter, the sending range of P defines the regionwithin which the potential receivers have to belocated to assure receiving P's messages, e.g., forany ReceiverRin P's sending range,$(SNR)_{P\to R} > \gamma_o$.

The notation γ_o is used to denote the minimum SNR, the threshold required to decode the signal successfully.In a nonjamming scenario, the average ambient noise floor P_N is the same, both the hearing range and thesending range of Node P will be the same.

6.3.1 Effect of Jamming on Network Topology

The communication range changes caused byjamming are reflected by the changes of neighbors at the network topology level. When jammers are present in the network, the network nodes can be classified into three categories based on theimpact of jamming as unaffected node N_U, jammed node N_J , and boundary node N_B.

- Unaffected node: A node is unaffected, if itcan receive packets from allof its neighbors.
- Jammed node: A node isjammed if it cannot receivemessages from any of the unaffected nodes. The fact is that twojammed nodes may still be able tocommunicate with each other.
- Boundary node: A boundary node can receive packets from part of itsneighbors but not from all its neighbors.



(a) Jammer is off (b) Jammer is on

Fig. 3.An example of the topology change of a wireless network due to jamming, where the black solid circle represents the jammer's NLB.

Fig.3, illustrates that prior to jamming effect, neighboring nodes were connected through bidirectional links but when the jammer became active, nodes lost their bidirectional links partially or completely.

In Fig. 3, the nodes marked as triangles lost all their receiving links from their neighbors and became jammed nodes. Interestingly, a fact is that some jammed nodes can still send messages to their neighbors, and they may participate in the jamming localization by delivering information to unaffected nodes. The nodes depicted in rectangles are boundary nodes. They lost part of its neighbors but still maintained partial receiving links.Ultimately, the rest of nodes depicted in circles are unaffected nodes because they can still receive from all their neighbors.

6.3.2 LSQ-Based Jammer Localization

In the previous sections, we have studied that the hearing range of a node may shrink and its neighbor list may change when a jammer becomes active.The levels of changes are determined by the distance to the jammer and the strength of the jamming signals. The basic idea of LSQ-based algorithm is to localize the jammer according to the changes of a node's hearing range.

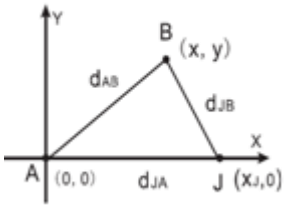


Fig. 4. The coordinate system for the sending range and the hearing range of Node A, wherein A and B are network nodes and J is the jammer.

Consider the example illustrated in Fig. 3, if B happens to be located at the edge of A's hearing range, and then we can obtain the following formula:

$$(x_A - x_J)^2 + (y_A - y_J)^2 = \beta r_{hA}^2 \qquad (1)$$

where r_{hA} is the new hearing range of Node A, and $\beta = \frac{\gamma_o}{P_T/P_J}$ and (x_A,y_A) and (x_J,y_J) are the coordinates of A and JammerJ, respectively. Suppose that the hearing ranges of m nodes have shrunk to r_{hi} where i= {1,2,3,…m}due to jamming. Assume that we can obtain r_{hi} for each of m nodes,then we can localize the jammer by solving the following equations:

$$(x_1 - x_J)^2 + (y_1 - y_J)^2 = \beta r_{h1}^2$$
$$(x_2 - x_J)^2 + (y_2 - y_J)^2 = \beta r_{h2}^2$$
$$(x_m - x_J)^2 + (y_m - y_J)^2 = \beta r_{hm}^2$$

We could linearize the problem by subtracting the m^{th} equation from both sides of the first m-1equations and obtain linear equations to avoid solving complicated nonlinear equations.Thus, we can localize the jammer by examining theneighbor list changes of multiple nodes and constructing a least-squares problem.

6.4 Performance Validation

To verify jammer detection and localization utilizing the PDR, RSS value, and nodes' affected communication ranges, we conducted experiments on a network topology which has sensor nodes including single mobile Reactive jammer. Various performance metrics like Packet delivery ratio, Throughput, Packet drop and Delay evaluation shows the above-mentioned jammer localization approaches improves the accuracy of detecting and localizing jammer in wireless sensor networks. Simulation has been carried out using NS2 simulator.

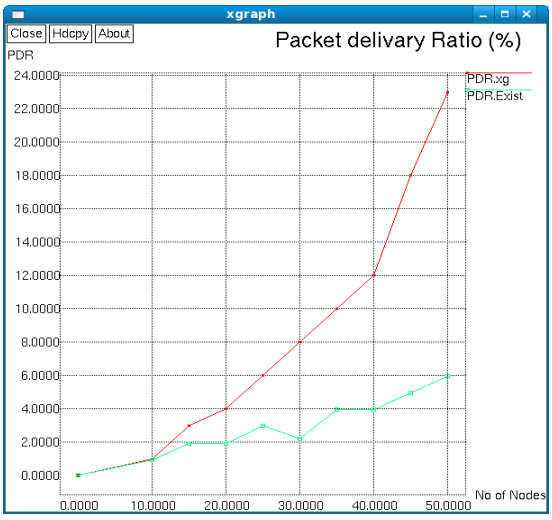


Fig.5. Packet Delivery Ratio

Packet Delivery Ratio (PDR) is defined by the ratio between number of bits transferred and number of bits received. Simulation result shows improved PDR values.

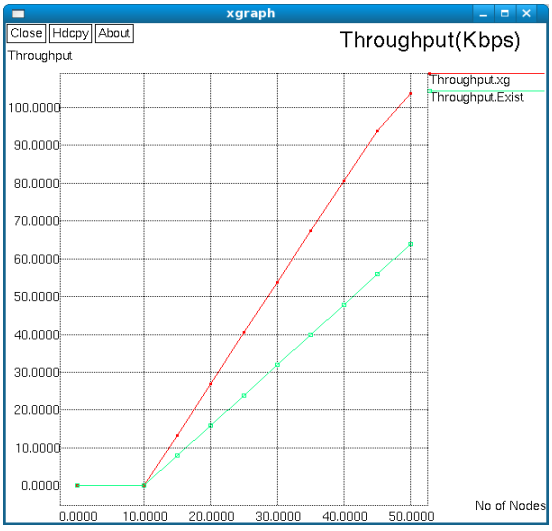


Fig.6. Throughput

Throughput shows the total performance, it also represents number of bits transferredper second. Simulation result shows increased throughput.

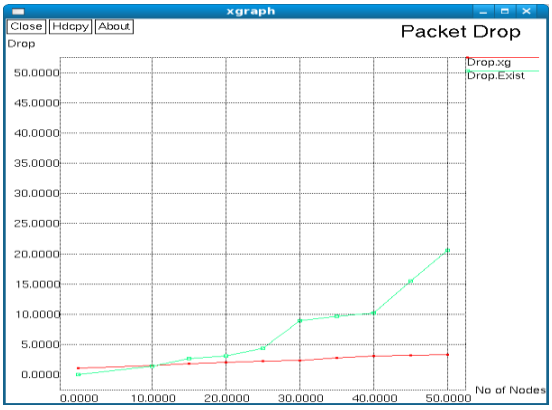


Fig.7. Packet Drop

Packet drop indicates measure of packet loss during transmission. This value should be negligible for achieving successful transmission. The performance shows packet loss is almost zero which indicates efficient packet transmission.

across

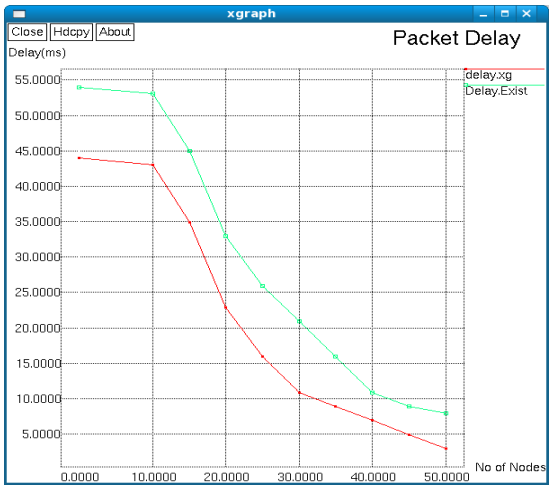


Fig.8. Packet Delay

Packet delay is the total time taken for a packet to transmit from the source to the destination the network. The graph shows better improvement than the existing method.

7. CONCLUSION

In this article, we had an overview on the characteristics of four different jammer attack models that may be employed against a wireless sensor network. Then we analysed some of the existing jammer localization schemes that employs indirect measurements for detecting jamming attacks. To address the limitation caused by existing methods, we proposed the jammer localization by utilizing intrusion detection based approaches. The primary focus of this work is to provide a jamming-aware network communication in the wireless networks. This analysis will serve as the basis for researcher pointers for open research issues in this field and to provide a better optimization in jamming detection. Our simulation results show that our novel based - framework achieves better performance than the existing methods. Our future work will be to localize multiple mobile jammers in the wireless sensor networks.

References

[1] K. Pelechrinis, I. Koutsopoulos, I. Broustis, and S.V. Krishnamurthy, "Lightweight Jammer Localization in Wireless Networks: System Design and Implementation," Proc. IEEE GLOBECOM,2009.

[2] H. Liu, Z. Liu, Y. Chen, and W. Xu, "Determining the Position of a Jammer Using a Virtual-Force Iterative Approach," Wireless Networks, vol. 17, pp. 531-547, 2010.

[3] Z. Liu, H. Liu, W. Xu, and Y. Chen, "Exploiting Jamming-Caused Neighbor Changes for Jammer Localization," IEEE Trans. Paralleland Distributed Systems, vol. 23, no. 3, pp. 547-555, Mar. 2012.

[4] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks," MobiHoc '05: Proc. Sixth ACM Int'l Symp. Mobile Ad Hoc Networking and Computing, pp. 46-57, 2005.

[5] Wenyuan Xu, Ke Ma, Wade Trappe, and Yanyong Zhang,Rutgers University, "Jamming Sensor Networks: Attack andDefense Strategies", IEEE Network, May/June 2006.

[6] I. Shin, R. Tiwar, T. N. Dinh, M. T. Thai and T. Znati, "A localizedalgorithm to locate reactive jammers with trigger nodes in wirelesssensor networks". Manuscript, 2009.

[7] M. Cakiroglu and A. T. Ozcerit "Jamming Detection Mechanismsfor Wireless Sensor Networks." 3rd InfoScale, Brussels, Belgium,2008.

[8] Y. W. Law, M. Palaniswami, L. V. Hoesel, J. Doumen, P. Hartel, andP. Havinga, "Energy-efficient link-layer jamming attacks against wirelesssensor network MAC protocols," *ACM Trans. Sen. Netw.*, vol. 5, no. 1,pp. 1–38, 2009.

[9] Yulia Ponomarchuk and Dae-Wha Seo "Intrusion Detection based on Traffic Analysis andFuzzy Inference System in Wireless Sensor Networks," Future Technology Research Association International vol. 1, 2010.

[10] Y. Ponomarchuk and D.W. Seo, "Intrusion detection based on trafficanalysis in wireless sensor networks", in Proceedings of the 19th AnnualWireless and Optical Communications Conference (WOCC 2010),pp. 229-235, 2010.

[11] F. Vincylloyd, Dr. B. Anand, J. Jijin Godwin," Development of OLSR based Selective Jamming Attack Detection Mechanism in Wireless Sensor Networks," Australian Journal of Basic and Applied Sciences, pp. 229-237,Mar. 2015.