International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 4, April - 2014

Detecting and Defending Reactive Jammers using Trigger nodes in Wireless Sensor Network

Apurva A.Bodkhe
Dept. of Computer science & Engineering
G. H. Raisoni College of Engineering & Technology
Nagpur, India

Archana R. Raut
Assistant Professor, Dept. of Computer science & Engineering
G. H. Raisoni College of Engineering & Technology
Nagpur, India

***Abstract*: Jamming resembles to denial-of-service attack and thus prevent legitimate users to send its data as the jammers purposefully emits radio frequency signals to corrupt wireless transmissions. In wireless sensor network which is having a broadcast nature as well as limited resources such as battery power, memory, computational capabilities these jammers can create mass destruction to legitimate sensor communication. Reactive jamming attack is a light weight attack performed by the adversary but they are easy to launch and difficult to identify. Hence in this paper various techniques to identify the jamming attack has been discussed moreover the emphasis is laid on detecting the reactive jammers and a more efficient method has been proposed to identify and defend the reactive jammers in wireless sensor network using the sensing trigger nodes.**

Keywords*: *Wireless Sensor Network, Jamming attack, Reactive jammers, Trigger nodes.

I. INTRODUCTION

Wireless sensor network is widely used now-a-days and has many applications in today's scenario. Ranging from data gathering to monitoring applications, hence security of data over these networks becomes an important aspect so that the data or the network does not get susceptible to any intruder or third party. Security challenges are increasing day by day as the adversary are finding new ways to detect the confidential transmissions hence there is a great need to think differently over the situation. Since the traditional ways of defending the attack is not fulfilling the need of security, hence a new approach towards this problem is need. Thus giving a new dimension as to how the security issues can be handled is discussed 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.

The jamming attack is one of the major security issues where a jammer node interferes with the signal of neighboring sensor nodes and thus disrupts the message delivery of its neighboring nodes. The jammers nodes can have different characteristics depending upon which they have been classified as: (i)Constant Jammer, (ii)Deceptive Jammer, (iii)Random Jammer, (iv)Reactive Jammer. Among these jammers the most harder to detect is the reactive jammer since compared to others which are active in nature i.e. they try to block the channel without having any prior information of the traffic pattern on the channel while the reactive jammer stay quiet when the channel is idle, 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.

II. BASIC TECHNIQUES

The main focus is on the identification of the reactive jammers. This identification can be on the basis of radio interference, or in a scenario where there is poor connectivity involving congestion and device failures thus it becomes very difficult to differentiate between jamming attack or a real time situation of congestion. Thus to have a closer look at the situation many methods [1], [2] have been are there which are as follows:

A. Signal Strength

One of the methods is to determine the strength of the signal by measuring the signal strength and analyzing the signal strength distribution to have the account of the presence of the attacking jammer. The approaches to identify the jamming signal involve comparing average signal magnitude with that of the threshold calculated from the overall noise level. With the study on this method it has been found that the reactive jammer can keep the increase in the effective RSS(Received signal Strength) value very low and hence it avoid being detected.

B. Carrier Sensing Time

A constant Jammer keep the channel constantly 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. Similar to the Signal strength method a channel is idle or not can be determined by comparing the noise level with the fixed threshold. To distinguish between a congestion and jammed scenario carrier sensing time can be used as the sensing time in first will be bounded and in later sensing time will be unbounded.

C. Packet Delivery Ratio

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

III. Advanced Techniques

The above discuss methods involve some basic statistical method which only can be used get the information regarding whether the there is a congestion in a network or a jammed situation. Identification of jammer nodes cannot be done through the above methods; it requires some advanced detection strategies [3] such as to combine PDR with the Signal strength which can give more efficient results compared to the basic methods. Since there may be many other techniques to defend the jammers it would not be always possible to detect and defend them using these techniques due to its (Reactive Jammer) vague properties. The adversary may be in continuous efforts to disrupt the network while the security experts would always find ways to defend them. Instead a way out would be as said by Sun Tze's famous *The Art of War*:

He who cannot defeat his enemy should retreat

Thus a way-out of this is to evade the jammers using the following techniques [4]:

A. Channel Surfing

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

B. Spatial Retreat

This technique is best suitable in a mobile network where the communicating nodes are mobile. This technique is 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

C. Region based Signal to Noise Ratio

To know the jamming effects based on the level of disturbance the network can be divided into three categories: unaffected nodes, jammed nodes and boundary nodes. And 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. While the SNR based model determines the SNR at the receiver which can estimate the jamming effects more accurately.

IV. Literature Review

The basic techniques discussed earlier i.e. the RSS, CST, PDR, together has a disadvantage that they only can work to identify the interference in the signal. Though there are enough schemes or methods by which the jamming signals can be discovered but to locate the jammer nodes depending on the signals is not solved yet. On the other hand the advanced techniques make use of multiple frequency bands and MAC channels however; the high computational overhead and excessive wastage of the frequency band badly reduces the efficiency of the resource limited network environment. To take an example of the channel surfing method the frequency hopping take place till it does not find a suitable channel free of any adversary. Since here we are considering an environment where resources are tightly bounded i.e. Wireless Sensor Network we cannot ignore these resources to be utilized vaguely. Since in WSN's the sensors have to scan all the channels to find a free channel even in the middle of communication can cause communication stalls. Thus if this happen frequently then it will result in longer transmission duration and more energy consumption. Another problem in the Spatial retreat is that it has considered that the jammer is stationary hence if the jammer is mobile then its movement may cause the network to become severely unbalanced. All these methods[5] have assumed that that the jammers capabilities are limited and powerless to catch the actual traffic from the camouflage of these diversities. However due to silent behaviour of reactive jammers, they have more powers to destruct the other mitigation methods.

V. Proposed Solution

To overcome the disadvantages discussed in above section a method [6] is proposed against reactive jamming attack in Wireless Sensor Network by using trigger nodes. Trigger nodes are named as such due to its properties i.e. the trigger nodes are only the normal nodes taking part in the communication in the network (Figure. 1) but when the network gets jammed, the victim nodes under that jammed area performs the group testing where each nodes transmits signal and check for any disruption in the transmission, the node which triggers the activation of reactive jammer node is called as the trigger node.

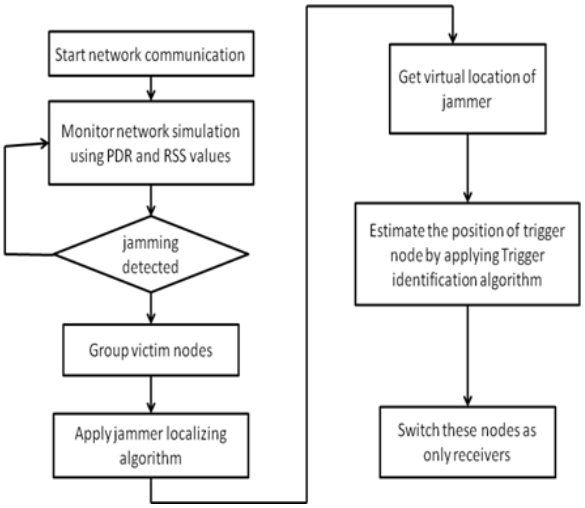

Fig. Proposed Solution Flowchart.

A. *Network Model*

1) *Sensor Node:* Sensor node positions cannot be known before- hand and for each simulation it will differ and the sensor nodes as well as jammers would remain static till one round of simulation ends. For this consider network as a connected graph G (V,E) where V is a set of N nodes and E representing communication links between nodes. Sensors will have omni-directional antennas with uniform strength on each direction. Each sensor node would have a Sensor_ID so as to uniquely identify each sensor node in the network. Sensor nodes would send a report message periodically to the Base station consisting of Sensor_ID, Status(Victim node/Trigger node/Boundary node/Unaffected node), Message details.

2) *Jammer Node:* d Reactive jammers keep idle until they sense any ongoing legitimate transmissions and then emit jamming signals (packet or bit) to disrupt the sensed signal (called jammer wake-up period), instead of the whole channel, which means once the sensor transmission finishes, the jamming attacks will be stopped (called jammer sleep period). Jammers would also have omni-directional antennas. The jammed area can be regarded 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. Any two jammer nodes are assumed not to be too close to each other, i.e., the distance between jammer J1 and J2 is d(J1,J2) >R. 1) No large overlapping between jammed areas of different jammers should be there as it lowers down the attack efficiency. 2) The d(J1,J2) should be greater than R, since the transmission signals from one jammer should not interfere the signal reception at the other jammer.

B. *Jamming Detection*

The idea of the approach is to identify whether the packet was jammed or just sent over a weak link. This is achieved as follows: Whenever a node receives a packet transmission, it not only receives the packet, but also records the RSS and PDR for each node. The intuition behind this process is that if the RSS value was Low and PDR=0, this indicates that it is non-jammed or neighbor failure or neighbor absence, but if the RSS value was High and PDR=0, this indicates that the node is jammed. Also if the PDR is Low with packets corrupted and RSS value is Low this indicates non-jammed or neighbour being far away. And if the PDR is Low with packets corrupted and RSS value is High this indicates node jammed. So by analyzing these two values for each node we can detect jamming in the network(Fig.2). In a normal scenario, where there are no interference or software faults, high signal strength corresponds to a high PDR. However, if the signal strength is low, which means the strength of the wireless signal is comparable to that of the ambient background noise, the PDR will be also low. On the other hand, a low PDR does not necessarily imply low signal strength. It is the relationship between signal strength and PDR that allows us to differentiate between the following two cases, which were not possible to separate using just the packet delivery ratio.

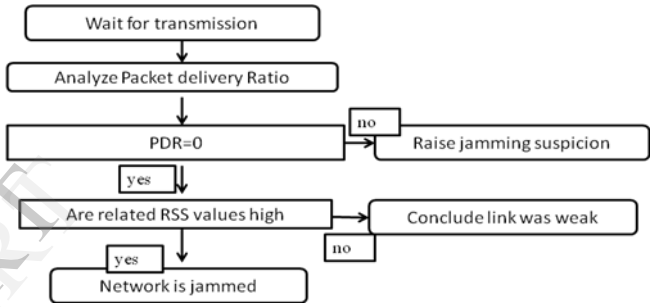

Fig 2. Jamming Detection Algorithm flow depending upon RSS and PDR values

C. *Victim node Collection*

For collection of all victim nodes (Figure. 3) we define a broadcast message *n*-dimension *msg* which is broadcasted as a message from the base station to all *n* node. Once a node receives this message, it will set its corresponding entry in *msg* to 1 if the node senses any one of the channels is jammed and hop to another normal channel to transmit the broadcast message. The base station will receive a collection of messages *msg* from all nodes. At last, the base station will identify all victim nodes by calculating the union*msg* of all broadcast messages *msg* (i.e., the entry i is 1 *iff* there is one message *msg* $\in$ M with the entry i equal to 1, where $1 \leq i \leq n$.). Thus M is the set of victim nodes.

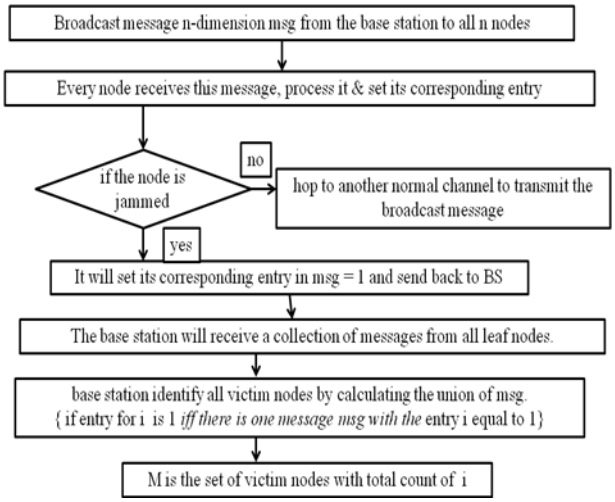

Figure 3. Victim nodes Collection Algorithm flowchart.

D. Grouping algorithm using location coordinates of the Victim nodes

Since Victim nodes are known and collected at the Base Station, the Base station finds out the Location Coordinates of those nodes (Figure. 4). Then selecting a random victim node from pool of collected Victim Nodes(VN). Now this VN searches for another victim node within its range since every node in the network has its Transmission range. Thus by knowing the location coordinates of the nodes within its range it adds that node into its group. Further the added VN repeats the process until it forms a group of 10 VN's. If the count goes beyond 10 then it forms another group. Also if a VN do not find any further VN node in its range then it forms a new group. Thus multiple groups are formed based upon the jamming region and density of jammed nodes.

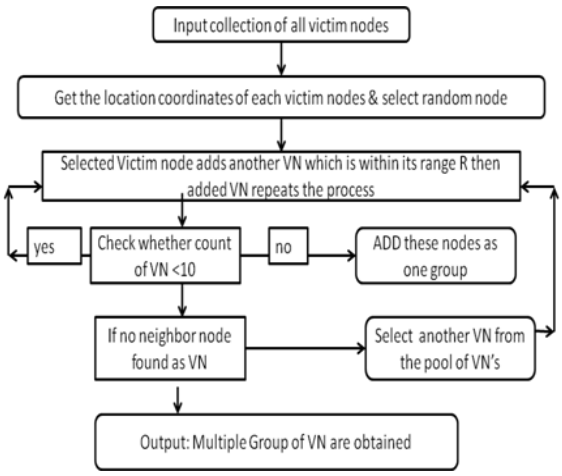

Figure 4. Grouping algorithm using location coordinates of the Victim nodes.

E. Virtual Jammer Positioning Algorithm

Now Groups are formed (Figure. 5) by using the above algorithm these groups are divided as set G= {G1, G2 …}. Each group consist of Victim nodes which are sparsely distributed over the group region so by collecting the coordinates of each node within that group and averaging over their coordinates the estimated position of the jammer can be obtained as (*Xjammer*, *Yjammer)*. Thus for every group we will get an estimated position of a jammer within that group. Since the jammer properties described above states that the jammer is omnidirectional and have a range of R with that when the grouping is done each group can only contain MAX 10 Victim nodes due to which the group area gets restricted thus its increases the probability of finding a jammer within each group.

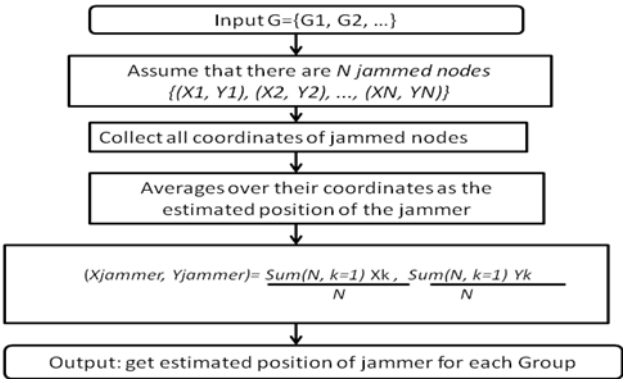

Figure 5. Virtual Jammer positioning algorithm

F. Trigger identification algorithm using Virtual position of jammer

As the jammer virtual positions are known hence for each group Trigger Algorithm can be applied (Figure. 6). For that the virtual position of jammer (*Xjammer*, *Yjammer)* estimated for each group is taken depending upon that all the Victim nodes nearest to jammer are collected. And let these VN's transmit signals one at a time. Then the VN which senses noise or jamming when it transmits identify that VN as a Trigger node. Next step is to disable the communication of these trigger nodes so that it cannot further trigger the jammer to jam the network.

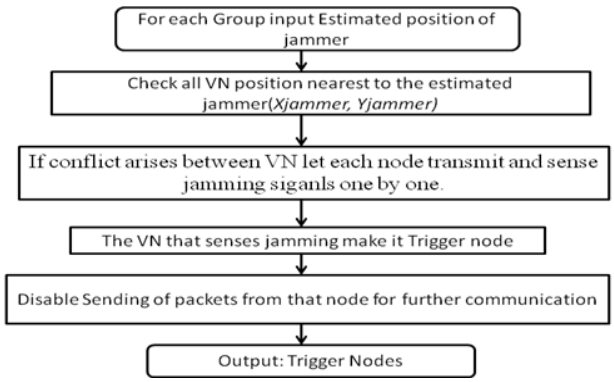

Figure 6. Trigger identification algorithm using Virtual position of jammer.

VI. RESULTS

A. *Number of Packets Sent or Received*

It is important to know for every node in the network that how many packets it has sent or received during the overall simulation time as it can be used to identify that which nodes had less packet sent or received ratio. This can be known by plotting the no. of packets sent to total no. of sensor nodes in the network similarly for the received no. of packets. This information also helps in calculating Packet delivery ratio for each node.

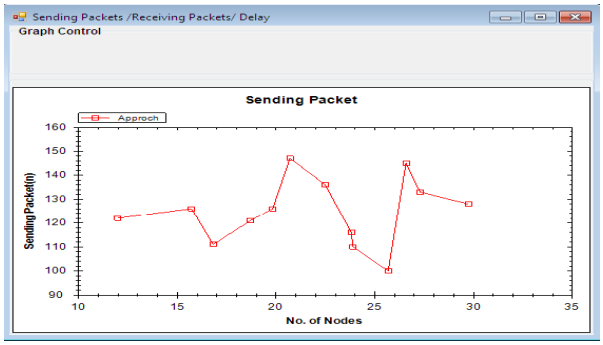

Figure 7 a) A graph showing no. of packets sent by each no. of nodes in the network.

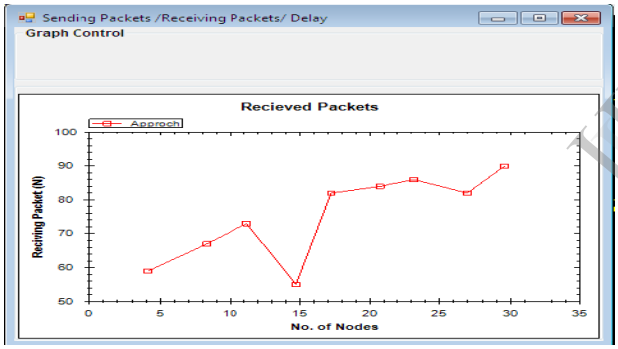

Figure 7 b) A graph showing no. of packets received by each no. of nodes in the network

B. *PDR and RSS values*

The packet delivery ratio serves as a primary jamming detector. Rather than relying on a single PDR measurement to make a decision, here the measurements of the PDR and RSS are used in order to combat false detections due to legitimate causes of link degradation, here the signal strength is also used as a consistency check. To see whether a low PDR value is consistent with the signal strength that is measured. First, from the point of view of a specific wireless sensor node, it may happen that all of its neighbors have died (may be from consuming battery resources or device faults) or it may be that all of a node's neighbors have moved beyond a reachable radio range. A second case would be the that the wireless node is jammed. The key observation is that in the first case, the signal strength is low, which is consistent with a low PDR measurement. While in the jammed case, the signal strength should be high, which contradicts the fact that the PDR is low.

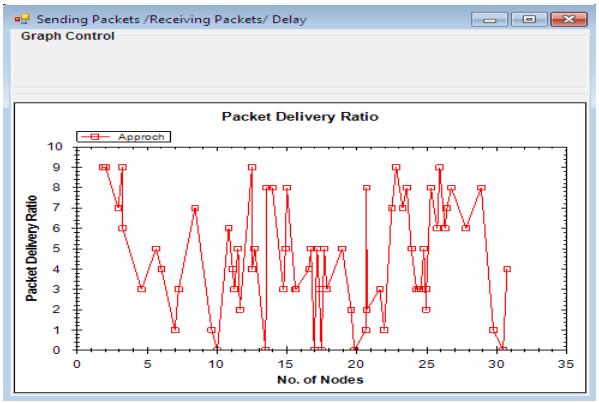

Figure 8 c) A graph showing PDR for each node in the network.

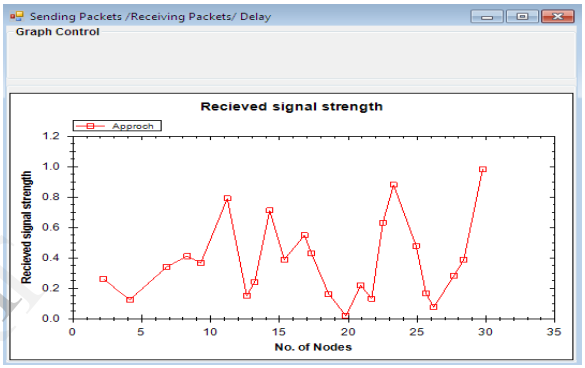

Figure 8 d) A graph showing RSS value for each nodes to identify the possible jamming attack.

C. *Performance Trigger node over Jammer Transmission power*

Now let's consider the interference range of the jammers. Since noise range is relatively larger than transmission range of sensor nodes, more messages of the sensor nodes will be jammed. In contrast, in our system, the larger jammers signal range may imply the increasing number of testing rounds even though this does not determine the damage area of the network. For instance, when the grouping algorithm analyzes the whole jammed region and also minimizes the jammed region size by classifying the nodes more efficiently. In Figure (e) and (f), as the transmission power of jammer gets increased, the number of victim nodes increases since a jammer can transmit farther and contaminates more nodes during the activation. Moreover, more victim nodes require more testing rounds among the group to cull out the trigger nodes among them. In our result, the number of rounds rises as the number of victim nodes increases.

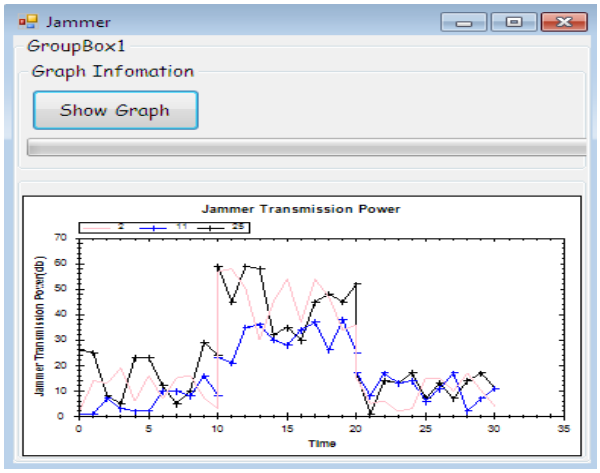

Figure 9 e) A graph showing the Transmission power of 3 jammer nodes w.r.t. Time & identified with their corresponding trigger node id.

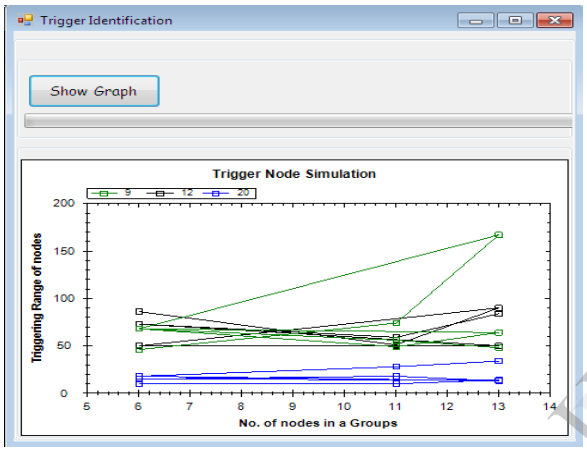

Fig 9 f) Graph showing the Trigger node selection after multiple iterations depending upon Trigger node range.

VII. CONCLUSION

The Basic and Advanced techniques which has been discussed in this paper has not solved the problem i.e. how to locate the jammers and also used traditional ways of security methods of defending only and due to which in the scenario where the resources are limited such as Wireless /sensor Network it would not be efficient to use these technique. As a result, the combination of PDR and signal strength is quite powerful in discriminating a jammed scenario from various network conditions. In this work we have addressed the issue of detecting the presence of jamming attacks, and examined the ability of different measurement statistics to classify the presence of a jammer.We also devised a new way for identifying the nodes, whose broadcasting triggers the Reactive jammers. By utilizing Grouping algorithm using location coordinates of the Victim nodes; Virtual Jammer positioning algorithm; Trigger identification algorithm using Virtual position of jammer this countermeasure achieves low overhead as evaluated by effectiveness of each scheme through empirical Graphs.

ACKNOWLEDGMENT

This work was supported by "G. H. Raisoni College of Engineering, Nagpur", Ms. Archana R. Raut is the Corresponding Supportive Author.

REFERENCES

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

[2] Mario Strasser, Boris Danev, and Srdjan ˇCapkun, "Detection of Reactive Jamming in Sensor Network", ACM Transactions on Sensor Networks, Vol. 7, No. 2, Article 16, Publication date: August 2010.

[3] Incheol Shin, Yilin Shen, Ying Xuan, and My T. Thai, Taieb Znat, "Reactive Jamming Attacks in Multi-Radio Wireless Sensor Networks: An Efficient Mitigating Measure by Identifying Trigger Nodes", ACM FOWANC'09, May 18, 2009.

[4] Patrick Tague, Sidharth Nabar, James A. Ritcey, and Radha Poovendran, "Jamming-Aware Traffic Allocation for Multiple-Path Routing Using Portfolio Selection", IEEE/ACM Transaction on networking, vol. 19, no. 1, February 2011.

[5] Mingyan Li, Iordanis Koutsopoulos, Radha Poovendran, "Optimal Jamming Attacks and Network Defense Policies in Wireless Sensor Networks", IEEE Communications Society subject matter experts for publication in the IEEE INFOCOM 2007 proceedings.

[6] Wenyuan Xu, Wade Trappe, Yanyong Zhang and Timothy Wood,"The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks", ACM, MobiHoc'05, May 25–27, 2005, Urbana-Champaign, Illinois, USA.

[7] Mario, Cagalj, Srdjan Capkun, and Jean-Pierre Hubaux, "Wormhole-Based Antijamming Techniques in Sensor Network", IEEE Transactions on mobile computing, vol. 6, no. 1, January 2007.

[8] Anthony D. Wood, John A. Stankovic, and Sang H. Son, "JAM: A Jammed-Area Mapping Service for Sensor Network", Proceedings of the 24th IEEE International Real-Time Systems Symposium 2003.

[9] Hongbo Liu, Wenyuan Xu, Yingying Chen, Zhenhua Liu, "Localizing Jammers in Wireless Networks", IEEE 2009.

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

[11] Hongbo Liu, Zhenhua Liu, Yingying Chen, Wenyuan Xu, "Localizing Multiple Jamming Attackers in Wireless Network", 31st International Conference on Distributed Computing Systems, 2011.

[12] Vinothkumar.G, Ramya.G, Rengaranjan.A, "Lightweight decentralised algorithm for Localising Reactive Jammers in Wireless Sensor Network", IEEE- Fourth International Conference on Advanced Computing, ICoAC 2012 MIT, Anna University, Chennai. December 13-15, 2012.

[13] Hongbo Liu, Zhenhua Liu, Yingying Chen, Wenyuan Xu, "Determining the position of a jammer using a virtual-force iterative approach", Springer Wireless Netw, 2011.

[14] Wenyuan Xu, Timothy Wood, Wade Trappe, Yanyong Zhang, "Channel Surfing and Spatial Retreats: Defenses against Wireless Denial of Service", ACM, WiSe'04, Philadelphia, Pennsylvania, USA, October 1, 2004.

[15] Hang Wang, Jingbo Guo, Member, IEEE and Zanji Wang, Senior Member, IEEE, "Feasibility Assessment of Repeater Jamming Technique for DSSS", IEEE WCNC proceedings 2007.