International Journal of Innovations in Engineering and Technology (IJIET)
http://dx.doi.org/10.21172/ijiet.123.06

Secure Enroute Mechanism For Jammer Attack In Wsn

Girish Deshpande[1]
[1]*Asst.Professor, Dept of Computer Science and Engineering, KLS GIT,Belagavi,Karnataka*

Abstract- The jamming attack is one of the major security issues where a jammer node interferes with signal of neighboring nodes. Providing an efficient security for wireless sensor network is a crucial challenge which is made more difficult due to its broadcast nature and restrictions on resources such as energy, power memory usage, and computation and communication capabilities. The Reactive Jammer Attack is a major security threat to wireless sensor networks because reactive jammer attack is a light weight attack which is easy to launch but difficult to detect .This work suggests a new scheme to neutralize malicious reactive jammer nodes by changing the characteristic of trigger nodes to act as only receiver. Here the current approach attempts to identify the trigger nodes using the group testing technique, which enhances the identification speed and reduces the message complexity of the status report sent periodically between the sensor nodes and the base station.
Keywords: Wireless Sensor Network, Jammer, Jamming Techniques, Jamming Attacks, Trigger Identification.

I. INTRODUCTION

Wireless sensor networks have limited resource constraints in terms of energy and range which leads to many challenging and intriguing security-sensitive problems that cannot be handled using conventional security solutions. The broadcast nature of the transmission medium makes it prone to attacks using jammers which use the method of injecting interference signals, which is why they can be considered as the most critical and fatally adversarial threat that can disrupt the networks. Jamming attacks do not have to modify communication packets or compromise any sensors in order to launch the attack. This makes them difficult to detect and defend against. As a consequence, wireless sensor networks are further exposed to passive and active attacks. A malicious node initiates a passive attack [1] through inert observation of the ongoing communication, whereas an active attacker is involved in transmission as well. Wireless networks are intended for transferring information between two or more points that are not physically connected. Wireless networks are prone to jamming attacks. Figure 1 shows an example of jamming attack. Jamming attacks are intentional interference attacks on wireless networks. Jamming attacks are intense denial-of-service attacks in the wireless medium. A denial-of-service isany type of any type of attack where the attackers attempt to prevent legitimate users from accessing the service. In this attack, network resources are made unavailable to the user. Jamming attacks reflect under external threat model wherein jammer is not apart of the network. Jamming can be regarded as one of the ways of degrading network performance. Typically, jammers corrupts the information of the original nodes by sending the radio frequency signals or by blocking the message so that the message would not be able to reach the intended receiver.

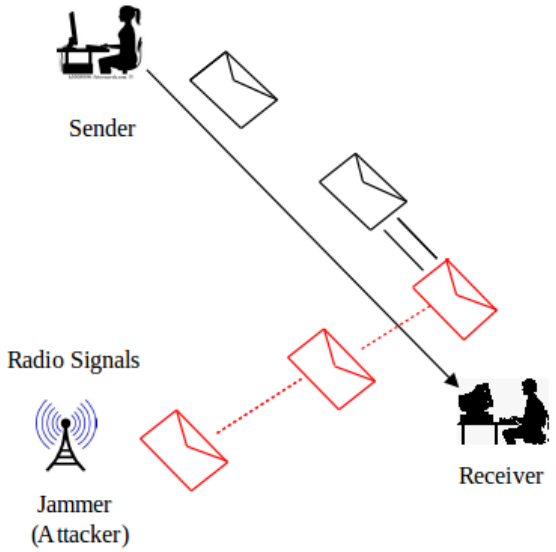


Fig 1: Jamming Attack

Mobile Ad hoc Network [MANET] [1] is self-organizing network of mobile devices which does not relay in any fixed infrastructure. Mobile devices in MANET can take part in the communication if they are within the range of network, and can move freely within transmission range of network. Mobile devices which are outside the transmission range of network cannot take part in communication. The dynamic nature of MANET with limited resources can vary with time such as battery power, storage space, bandwidth makes QoS provisioning, a challenging problem.
Congestion within the network happens when the aggregated demands exceed available resources. But merely increasing network resource is unable to address the congestion problem. Various congestion control methods have been proposed to solve this issue.

II. LITERATURESURVEY

2.1 System Models

1)Network Model:

This model consists of n sensor nodes and a base station in wireless sensor network. Each sensor node has omni-directional antennas with m radios which makes a total of k channels throughout the network, where k>m. Here the power strength is assumed to be uniform, hence the transmission range is constant r and the network is modelled as a unit disk graph (UDG).

2)Attacker Model:

Jamming nodes decide whether or not react depending on the power of the sensed signal. Here we assume that reactive jammers have omni-directional antennas which have uniform power strength in every direction which is equal to the property of the sensors. Jammers which acts on a network need to lie at the centre of the network area so that its radius R covers all the sensors in order to achieve a powerful and efficient jammer model. All the sensors within this range will be jammed during the jammer wake-up period. Depending on the positions of the boundary sensors and the victim nodes in the network, the value of R can be calculated.

3)Sensor Model:

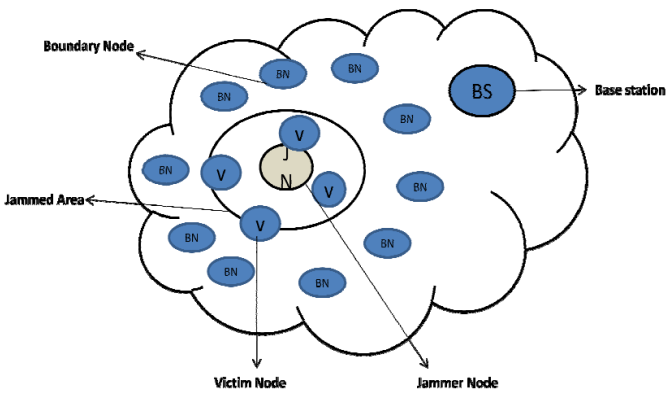


Fig 2: Categorization of Sensor Nodes

In WSN, all nodes communicate information between one another using sensor. The jamming status is used to categorize the sensor nodes into four types as shown in Figure 2. Trigger Node TN is a sensor node which awakes the jammers, victim nodes VN are those within a distance R from an activated jammer, boundary nodes BN and unaffected nodes are free from the effect of jammers.

III. DISADVANTAGESOFEXISTINGSYSTEM

As a consequence, wireless sensor networks are further exposed to passive and active attacks.The attack also leads to packet loss and retransmission of packet data that will increase consumption of energy in the network.

IV. PROPOSEDSYSTEM

Trigger identification service is mainly divided into three main steps
The first step executes anomaly detection where the base station detects impending reactive jamming attacks. Each boundary node identifies itself to the base station.
In the second step jammer property estimation is performed where the base station calculates jamming range based on the location of boundary node.
The third step is trigger detection where the base station broadcasts a short testing schedule message M to all the boundary nodes.
Thereafter the boundary nodes keep broad jammed area for a period P. Subsequently the victim nodes locally execute the testing procedure based on M and identify themselves as trigger or non-trigger.

V. ADVANTAGESOFPROPOSEDSYSTEM

Random Early Detection (RED) is well known technique used for active queue management and for congestion avoidance in computer networks.Mobile ad hoc network can be perfectly used in military applications as setting up this type of network is cost effective and takes less time.It distributes the probability symmetrically rather than linearly.

VI. EXPLANATION

6.1. Jamming Technique

Figure 3 shows different types of jamming techniques. The spot jamming technique [2] involves a malicious node that directs all its transmitting power to a single frequency. It makes use of identical modulation schemes and less power to override the original signal. The assault on WSNs due to this attack is easily avoided by surfing to another frequency. In case of Sweep jamming technique [3], the malicious node can jam multiple communication frequencies, but simultaneously. The attack also leads to increase in consumption of energy in the network.

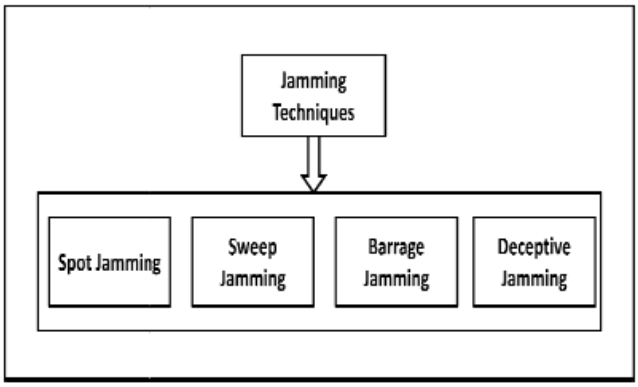


Fig 3: Different types of jamming techniques

Barrage jamming technique [4] jams networks simultaneously on different frequencies which decreases the signal technique and increases the range of jammed frequencies and reduces the output power of the jammed node. Deceptive jamming technique [5]has the capability to flood the network with useless data which can mislead the sensor nodes present in the network.The available bandwidth used by the sensor nodes is reduced.

6.2. Types of Jamming Attacks

Figure 4 shows different types of jammers. Jammers are classified as
1)Constant jammer: [6] It continually emits a radio signal, and can be implemented using either a waveform generator that continuously sends a radio signal or a normal wireless device that continuously sends out random bits to the channel.
2)Deceptive jammer: [7] The deceptive jammer uses misleading jamming techniques to attack the original nodes in WSN. The deceptive jammer continuously sends regular packets on the channel without any gap between the packets.
3)Random jammer: [8] A random jammer alternates between sleeping and jamming. During its jamming phase, it behaves like a constant jammer or a deceptive jammer.

4)Reactive jammer: [9] This type of jammer is quiet until the medium is idle and when it senses transmission on the medium it starts injecting false data which avoids the legitimate user to send data. Among all the above four jammers the reactive jammer is very difficult to detect.

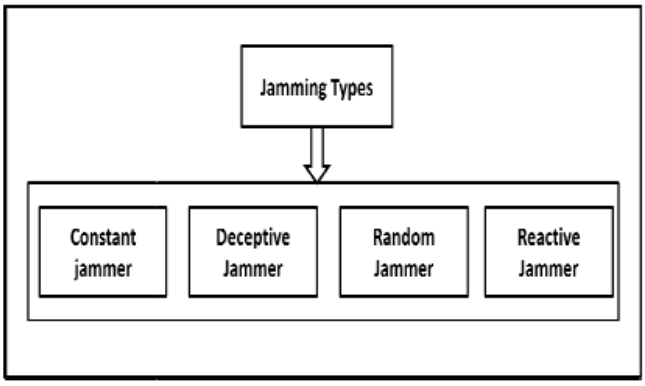


Fig 4: Types of Jammers

6.3. System Architecture

The inference after comparing the above mentioned jamming attacks is that reactive jamming is far more destructive attack. This paper considers the reactive jammer attack since it creates issues in networks as the reactive jammer nodes can disrupt the message delivery of its neighbouring sensor nodes with strong interference signals. The consequences of the attack are the loss of link reliability, increased energy consumption, extended packet delays and disruption of end routes.

Figure 5 shows the system architecture used for our WSN system. This work presents system architecture description of the overall trigger of the set of sufferer nodes. Testing of these nodes is carried out at the base station. Procedure to identify each individual node can be stored locally for use by routing schemes or can be sent to base station for localization jamming process. The jammer [7] uses misleading jammer [9] which listens for on-going activity on the signals prevalent on the channel leading to collision and opposes secure communication in wireless sensor network. This imposes a critical threat to wireless sensor for defense against reactive jamming attack. The initial identification service framework begins with the identification of anomaly and then grouped into several testing teams. Once the group testing is done at the base station, the nodes themselves locally execute to prove themselves as a trigger or non trigger. The identification outcomes can be stored at individual nodes locally or it may be sent to the base station for testing the localization process. Implementation approach describes the performance evaluation along with evaluation of the time taken to execute the testing rounds and also the message complexity.

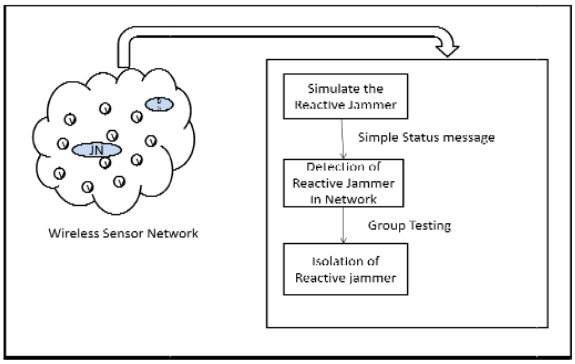


Fig 5: System Architecture

Algorithm : Trigger Nodes Identification Algorithm
/*All nodes in a group N synchronously performs the following to recognize trigger nodes in N.*/
INPUT: n victim nodes in a testing group
OUTPUT: all trigger nodes within these victim nodes

//In order to estimate 'd' i.e. upper bound of error
Set γ= (10t- 8t2 – t-d -1)/2;
//Likelihood for each test
Set T=t ln n(d+1)2/(t-√(d+1))2;
Construct a (d,z)- disjunct matrix using ETG algorithm with T rows, and divide all the n victim nodes into T group accordingly {g1,g2,.....,gt};
// Group testing will be done for each round on m groups using m different channels. Here testing can be done in asynchronous manner, the m group tested in parallel need not wait for each other to finish the testing, instead any finished test j will trigger the test j+m, i.e, the tests are conducted in m pipelines.
for i= 1 to [t/m] do
Conduct group testing in group gim+1,gim+2,gim+m in parallel;
If any node in group gj with j∉[im+1,im+m] detects jamming noises, finish the testing in this group and start testing on gj+m;
If no nodes in group gj sense jamming noises, while at least one other test in parallel detects jamming noises,
All the nodes in group gj resend more messages to set off possible hidden jammers;
If no jamming signals are detected till the end of the predefined round length (L)
Return a negative outcome for this group and start testing on gj+m;
end

VII. RESULTS& ANALYSIS

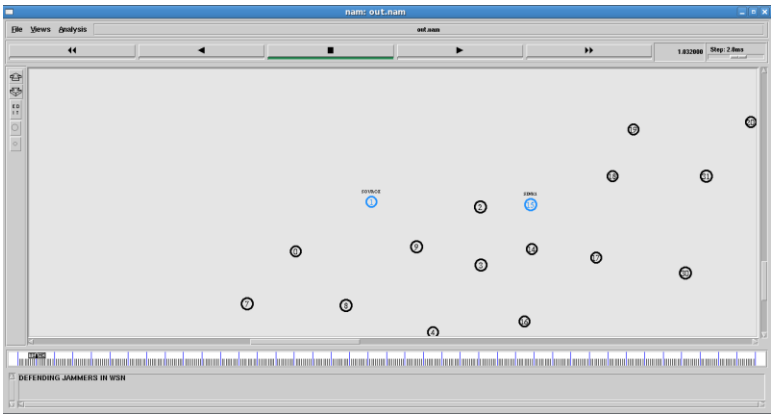


Fig 6.1: The above diagram represents environment for wireless sensor networks. Two or three sensor nodes gather collectively formed power efficient and autonomous network. Each and every node is assigned by an unique ID. Let us assume there are 50 nodes which are defined in network including clusters. The node ID 1 which acts as a source and the node ID 15 which acts as destination. The intermediate nodes help in transmitting data from source to destination.

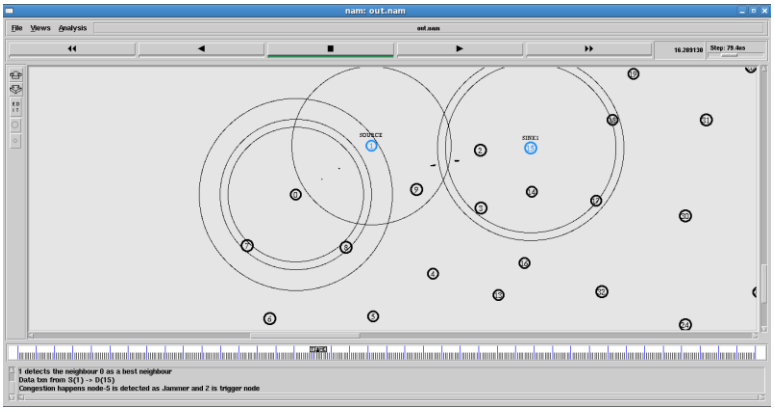


Fig 6.2: In the above figure the next step is choosing optimal path from several alternatives. The optimal path is chosen after considering two parameters 1) Energy efficiency 2) Security. Here, Source node 1 detects 0 as a best neighbour.

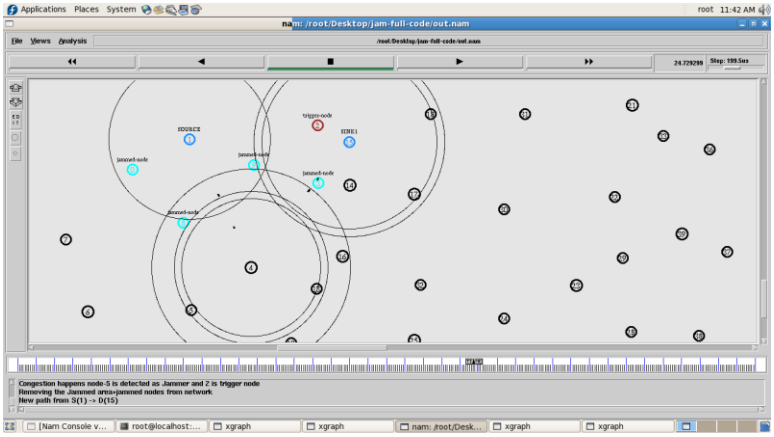


Fig 6.3:The remaining task is we are differentiating optimal and non optimalpaths.The node ID 5 acts as a jammer which is invoked by the trigger node which here is node ID 2. The jammer will detect jammed nodes and the trigger node and it avoids routing and it eliminates both the trigger node and the jammed nodes.

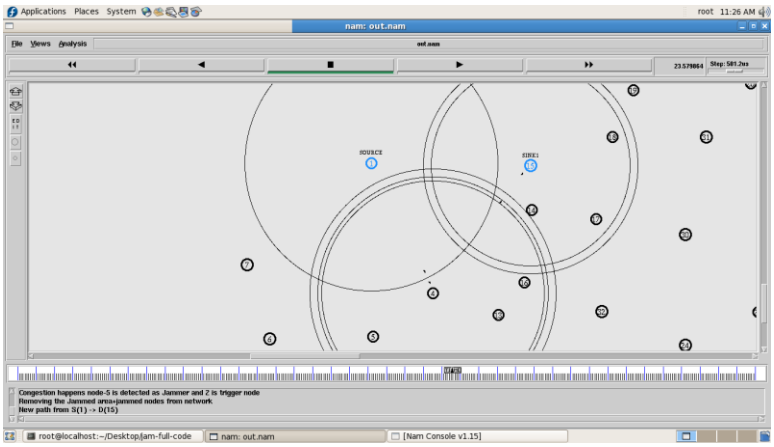
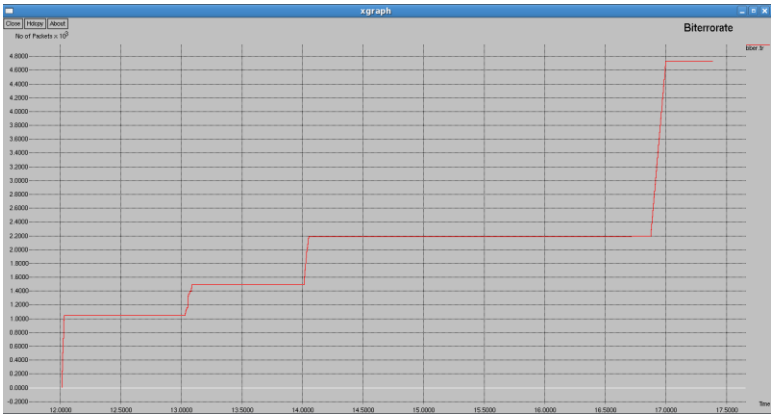
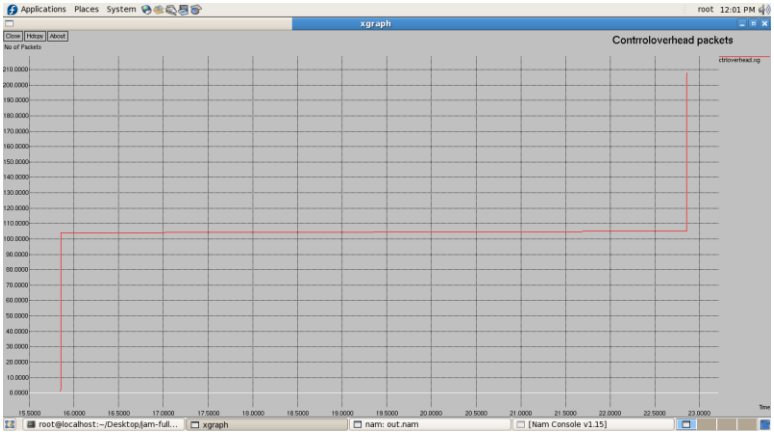


Fig 6.4: After taking considerable security measures it avoids non-optimal routing paths and it deletes untrusted nodes and it broadcasts to entire network with a secure path. Then it will select the optimal path to send data from source to destination.

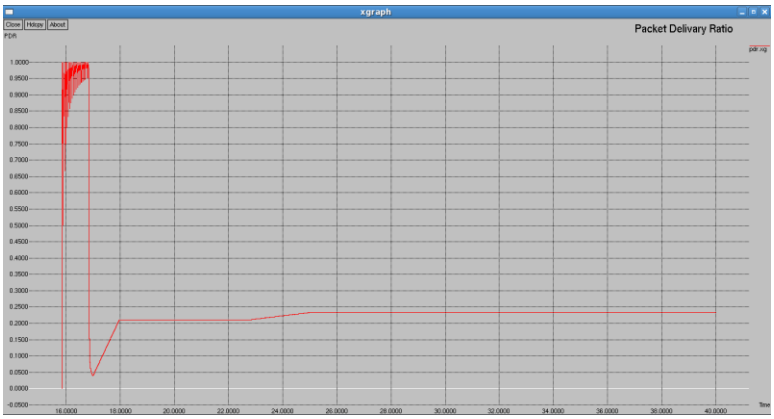
After implementing the above steps following parameters are achieved in our work.
Bit error rate



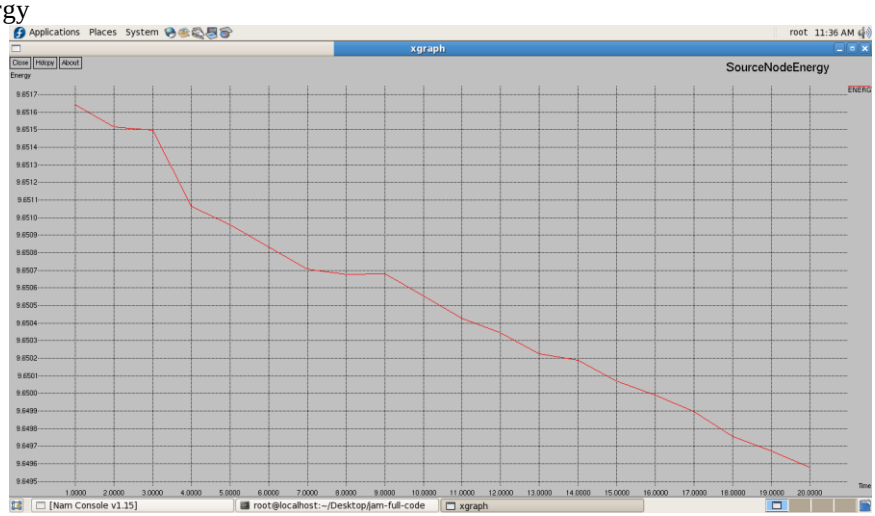
Control overhead packets



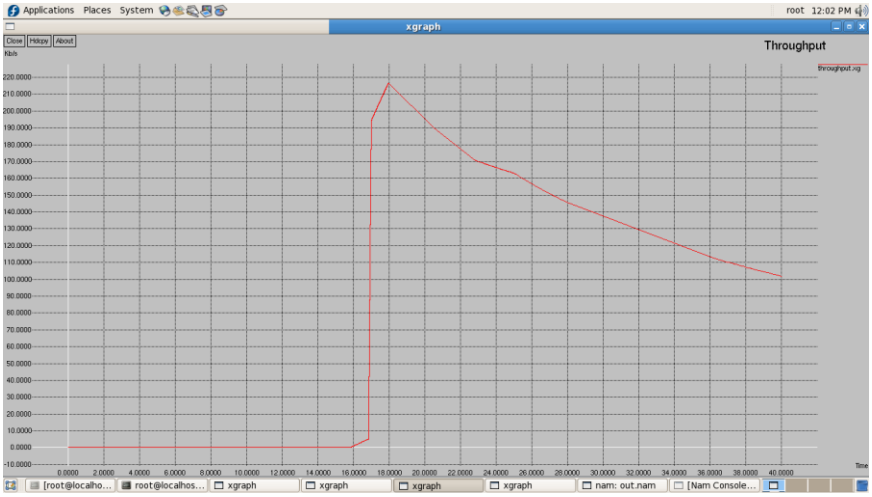
Packet Delivery Ratio



Source node energy



Throughput



VIII. CONCLUSION

In this paper, a novel trigger identification service for reactive jamming attack in wireless sensor network is introduced to achieve minimum time and message overhead. The status report message are transferred between the base station and all sensor nodes. For isolating reactive jammer in the network a trigger identification service is introduced, which requires all testing groups to schedule the trigger node detection algorithm using group testing after anomaly detection. By identifying the trigger nodes in the network, reactive jammers can be eliminated by making trigger nodes as only receivers. This detection scheme is thus well-suited for the protection of the sensor network against the reactive jammer. Furthermore, investigation into more stealthy and energy efficient jamming models with simulations indicates robustness of the present proposed scheme. The result can be stored in the network for further operations i.e. to perform best routing operation without jamming. This work achieves the elimination of attackers to maintain the soundness of wireless sensor networks.

REFERENCES

[1] G. Padmavathi,"A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks," vol. 4, no. 1, pp. 1–9, 2009.
[2] LV Bo,ZHANG Xiao-fa,WANG Chao ,YUAN Nai-chang," Study of Channelized Noise Frequencyspot Jamming Techniques",2008
[3] XI You-you,CHENGNai-ping, "Performance Analysis of Multi-tone Frequency Sweeping Jamming for Direct Sequence Spread Spectrum Systems",2011.
[4] Williams united state ," Multi-Directional Barrage Jamming System",1975.
[5] J. Schuerger, "Deceptive Jamming Modelling In Radar Sensor Networks," pp.1–7[6] W. Xu et al., "Channel Surfing and Spatial Retreats: Defenses Against Wireless Denial of Service," Proc. 2004 ACM Wksp. Wireless Security, 2004, pp. 80–89.
[6] W. Xu et al., "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks," MobiHoc '05: Proc. 6th ACM Int'l. Symp. Mobile Ad Hoc Net. and Comp., 2005, pp. 46–57.
[7] W. Xu et al., "Channel Surfing and Spatial Retreats: Defenses Against Wireless Denial of Service," Proc. 2004 ACM Wksp. Wireless Security, 2004, pp. 80–89.
[8] W. Xu et al., "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks," MobiHoc '05: Proc. 6th ACM Int'l. Symp. Mobile Ad Hoc Net. and Comp., 2005, pp. 46–57.
[9] Y. Law et al., "Link-Layer Jamming Attacks on S-Mac," Proc. 2nd Euro. Wksp. Wireless Sensor Networks, 2005, pp. 217–25.
[10] A. Wood and J. Stankovic, "Denial of Service in Sensor Networks," IEEE Comp., vol. 35, no. 10, Oct. 2002, pp. 54–62