Simulating and Analysing Basic Security Attacks in Wireless Sensor Networks using QualNet

Ayaz Hassan Moon[1] N.A.Shah[2] Ummer Iqbal[1] Adil Ayub[1]

[1] National Institute of Electronics and Information Technology,(NIELIT) Srinagar/Jammu
[2] Deptt. Of Electronics & Instrumentation Tech. University of Kashmir, Srinagar.

***Abstract* - Sensor nodes are resource constraint devices and are thus vulnerable to a variety of attacks, which can compromise the security of an entire Wireless Sensor Network. Some of these attacks can be launched by a laptop class adversary equipped with relatively powerful resources. In this paper, we simulate and analyse Black Hole and DoS by Hello Flooding attack in Wireless Sensor Networks. A generic WSN model has been created in QualNet and necessary changes have been done in the code library to simulate the attacks. Various parameters like throughput, packets dropped, end to end delay have been recorded and the analysis has been carried out to understand the impact of these attacks.**

Keywords: WSN Security, DoS attack, Black Hole Attack, Simulation of attacks in QualNet.

I. INTRODUCTION

WSN's consist of battery-operated sensor devices with computing, data processing, and communicating components. Irrespective of the ways, the sensors are deployed i.e., either in a controlled environment or in an uncontrolled environment, security for sensor networks becomes extremely important.

One of the fundamental goals for Wireless Sensor Networks[1] (WSNs) is to collect information from the physical world. Although a number of proposals have been reported concerning security[2] in WSNs, provisioning security remains critical and challenging task. However the end-to-end delivery is not guaranteed due to the scarcity of resources. A Sensor Network being broadcast in nature is subject to variety of attacks[3][4] that can compromise the network security[5][6][7]. Some of the common attacks launched against WSN are *Black Hole, DoS, Wormhole, Sybil attack etc*. Most of these attacks result in Denial of Service[8] for which the network has been created.

In this paper, two basic attacks namely Black Hole attack and DoS by Hello Flooding in AODV[9] have been simulated using QualNet and their impact on the network services has been analysed under different scenarios.

Black Hole Attack

In one of the forms of Black Hole[10] attack, the malicious node absorbs all the incoming traffic not intended for it. As a result of which, the node does not route or forward the messages intended for other nodes in the network. This attack has a considerable effect on various Quality of Service parameters[11] like throughput, number of packets received, delay etc. The position of the Black Hole nodes have a significant impact on the network. The severity of the attack will be felt more if the malicious node happens to be in the vicinity of the base station.

DoS by Hello Flooding

Denial of Service (DoS) is a class of attack wherein the objective of the attack is to make network resources unavailable to its intended users. One of the most common way to perform this attack is to flood the network with unsolicited, overwhelming flux of packets, thereby saturating the bandwidth and depleting the target system resources. DoS attack by flooding in AODV[12] can be carried out in various ways like Route Request (RREQ) flood[13], Hello messages flood. The simulation of DoS by Hello Flooding has been carried out and analysed.

II. METHODOLOGY

The flowchart of the processes adopted in QualNet[14] has been represented in Fig. 1.

978-0-7695-5013-8/13 $31.00 © 2013 IEEE
DOI 10.1109/ICMIRA.2013.20

In general, a simulation study in QualNet comprises the following phases:

•The first phase is to create and prepare the simulation scenario based on the system description and metrics of interest.

•The second phase is to execute, visualize, and analyze the created scenario and collect simulation results. Simulation results can include scenario animations, runtime statistics, final statistics, and output traces.

•The third phase is to analyze the simulation results. Typically, users may need to adjust the scenarios based on the collected simulation results. All these processes are done by QualNet Graphical User Interface (GUI). The GUI consists of the following tools.

•**QualNet Architect** — A graphical experiment design and visualization tool which has two modes: Design mode, for designing experiments, and Visualize mode, for running and visualizing experiments.

•**QualNet Analyser** — A graphical statistics analysing tool.
•**QualNet Packet Tracer** — A graphical tool to display and analyse packet traces.
•**QualNet File Editor** — A text editing tool.

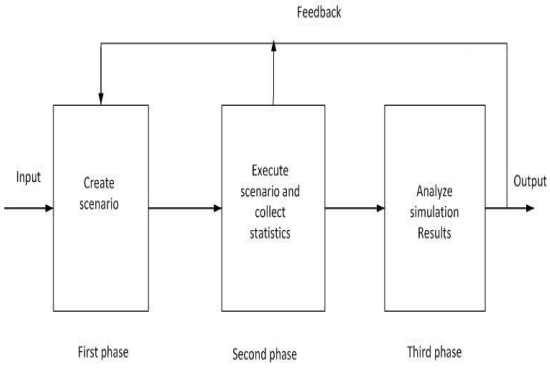

Fig. 1. QualNet Process Flow

Two scenarios have been created in the QualNet; one for simulating Black Hole Attack (Scenario 1) and the other for DoS by Hello Flooding (Scenario2).

A. Scenario1 (*Black Hole Attack*)

The Scenario1 that has been created by QualNet Architect is shown in Fig. 2.

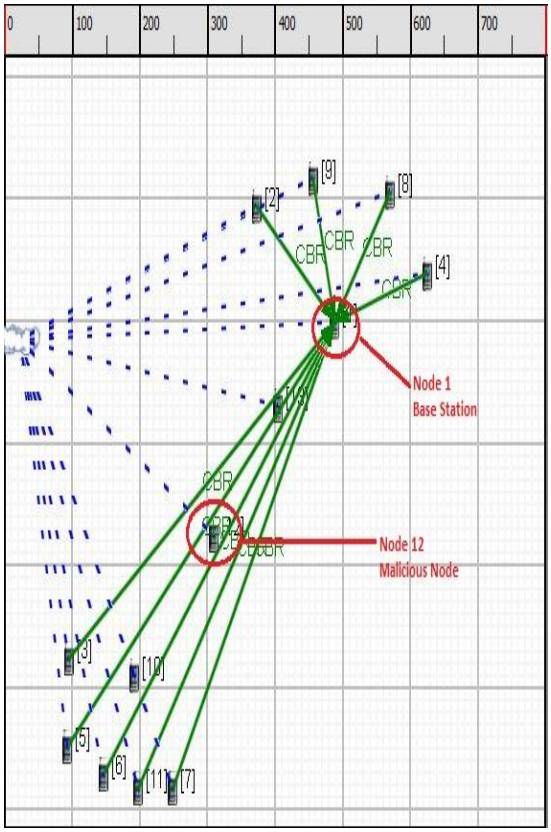

Fig. 2. Scenario 1 for simulation of Black Hole attack

There are 13 sensor nodes that have been deployed onto the QualNet Architect and the nodes are identified as node1 until node 13. Node 1 is the base station or the sink that collects all the data from the sensor nodes and subsequently sends out the data to the outside network (internet). Nodes 10, 12, and 13 are the routers (FFD) that relay data from the far-away sensor nodes to the base station or the sink. The remaining nodes, node2, node4, node8 and node9 are the sensor nodes that can directly communicate with the base station in a single hop communication.

In this scenario, Node12 has been programmed to act as a malicious node that initiates the Black Hole attack in the network.

B. Scenario2 (*DoS by Hello Flooding Attack*)

The Scenario2 created in the QualNet Architect is shown in Fig. 3. This scenario represents the DoS by Hello Flooding attack on a WSN.

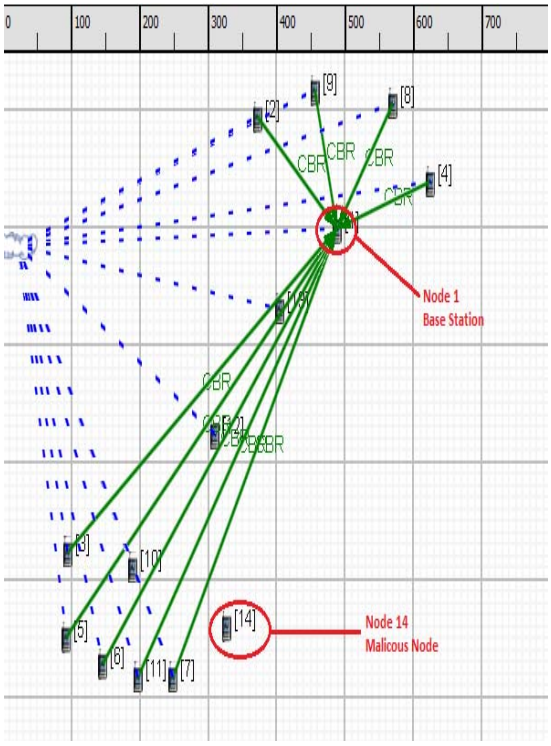

Fig. 3. Scenario2 for simulation of DoS by Hello Flooding Attack

This scenario is quite similar to the Scenario1 except for the addition of node14 which is programmed as a malicious node. This malicious node is responsible for sending unsolicited Hello messages used for flooding the network. This will result in network clogging, thereby degrading the Quality of Service.

C*. QualNet GUI and Code Changes*

The necessary modifications have been made in the QualNet GUI (.prt file) and the WSN code library . The code of routing protocol AODV used in the scenario has been modified to incorporate Black Hole attack and DoS by Hello Flooding Attack. The changes incorporated in the GUI result in the inclusion of additional parameters viz. Black Hole and DoS by Hello Flooding not originally available in the QualNet Property menu.

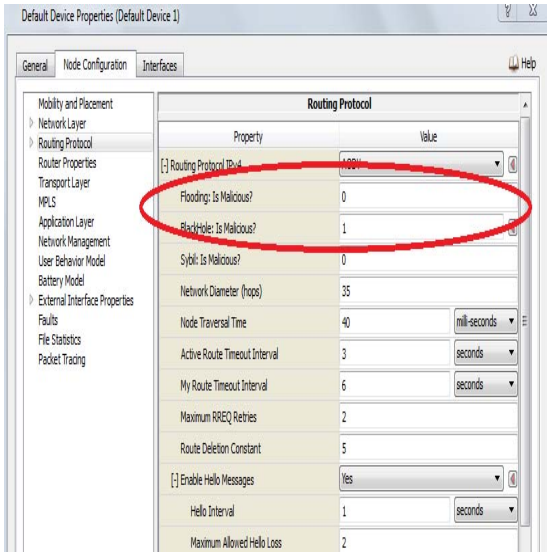

Fig. 4. QualNet GUI changes

DoS by Hello Flooding property and Black Hole property can be set/unset in the property menu of a node to exhibit malicious behaviour.

D. Configured Parameters

In both the scenarios, the configured parameters are as below:

1. Radio/Physical Layer

    a. Energy Model Specification : **MicaZ**
    b. Battery Model : **None**
    c. Radio Type: **IEEE 802.15.4**
    d. Modulation Scheme: **O-QPSK**
    e. Packet Reception Model: **PHY802.15.4**
    f. **Reception Model**
    g. Transmission Power: **0dBm**
    h. CCA Mode: **Carrier Sense**

2. MAC Protocol

Black Hole Attack Scenario

Node	Device Type	Mode
1	FFD	PAN Coordinator
10,12,13	FFD	coordinator
2,3,4,5,6, 7,8,9 & 11	RFD	——

DoS by Hello Flooding Attack Scenario

Node	Device Type	Mode
1	FFD	PAN Coordinator
10,12,13, & 14	FFD	coordinator
2,3,4,5,6, 7,8,9 & 11	RFD	——

3. Network Protocol: IPV4
   a. Network Protocol: **IPV4**
   b. Routing Protocol for IPV4: **AODV**

The distance between the sink/base station and the nodes is tabulated in Table 1. The location of each sensor node is determined and defined in terms of coordinates (X_i, Y_i). The distance D between each sensor node is determined by using the Pythagoras theorem.

$$D = \sqrt{Xi^2 + Yi^2}$$

Where ,

X_i is the difference between coordinate X of the sensor nodes and the sink node

Y_i is the difference between coordinate Y of the sensor nodes and the sink node

Coordinate (Xi, Yi)		**Distance D (meters)**
Sink Node	**Sensor Node**	
[1] (488.41 , 498.86)	**[2]** (372.43 , 593.93)	**149.96**
	[3] (94.83 , 223.17)	**480.53**
	[4] (625.30 , 538.79)	**142.59**
	[5] (92.93 , 150.92)	**526.75**
	[6] (146.17 , 128.10)	**504.57**
	[7] (248.84 , 116.69)	**451.05**
	[8] (570.17 , 605.34)	**134.24**
	[9] (456.08 , 616.75)	**122.24**
	[10] (191.80 , 209.86)	**414.12**
	[11] (197.50 , 116.69)	**480.29**
	[12] (309.68 , 323.94)	**250.08**
	[13] (404.75 , 430.42)	**108.08**

Table1. Distance between nodes

E. *QualNet Animator*

When the configuration and placement of nodes is completed in the Architect mode, click **RUN** in the runtime toolbar to begin the simulation of the scenario. There are various controls for the simulation like speed, zoom in and zoom out , pause, stop and pan. These controls can be used for closely monitoring the node broadcasts and communications flow.

F. *QualNet Analyzer*

Upon completion of the simulation, various statistics are generated and the graphical metric result can be collected by clicking on the **Analyzer** button.

III. RESULTS AND ANALYSIS

A. Black Hole Attack

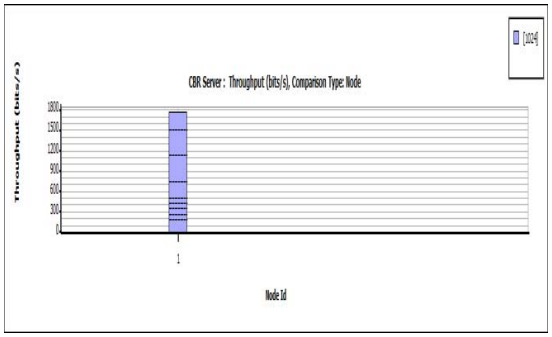

Fig. 5. Throughput_No Attack

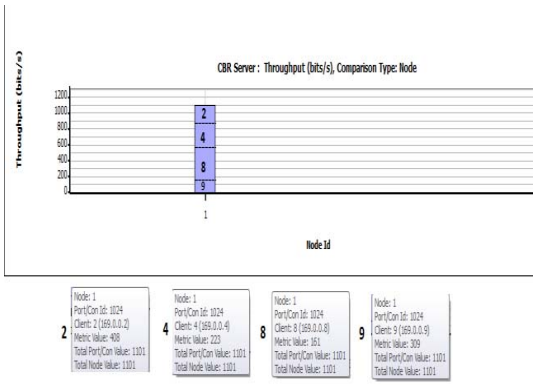

Fig. 6. Black Hole Attack

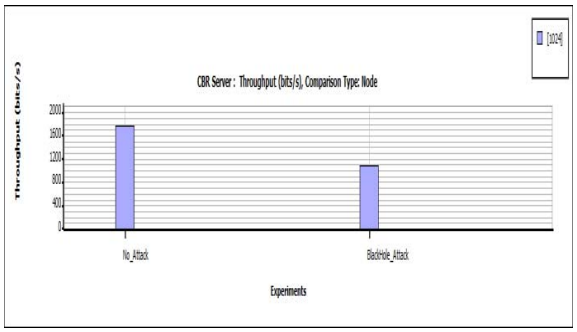

Fig. 7. CBR Server throughput comparison of Normal (No Attack) and Black Hole Attack Scenario

Throughput:

Fig 1. shows the CBR Server throughput at node 1 in case of a normal (No Attack) scenario. The throughput at node 1 consists of data from all the nodes.

Fig2. shows the CBR Server throughput at node 1 in case of a Black Hole attack scenario. The throughput at node 1 consists of data from nodes 2, 4, 8 and 9 only. This is because the data from nodes 3, 5, 6, 7 and 11 are not forwarded by the node 12 which acts as a Black Hole node.

As shown in Fig 3. , the throughput in Black Hole attack scenario is less than the throughput in the normal (no attack) scenario. This is due to the malicious behaviour of node 12 (which is a black node) that does not forward any data , rather drops all the traffic that it receives. As a result, the base node (node 1) does not receive any data from nodes 3, 5,6,7 and 11.

No. of Data Packets Forwarded:

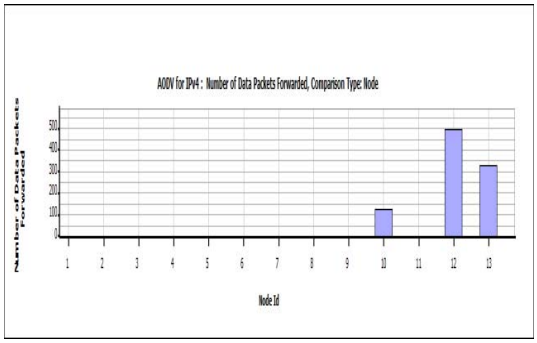

Fig. 8. No. of Data Packets Forwarded in Normal (No Attack) Scenario

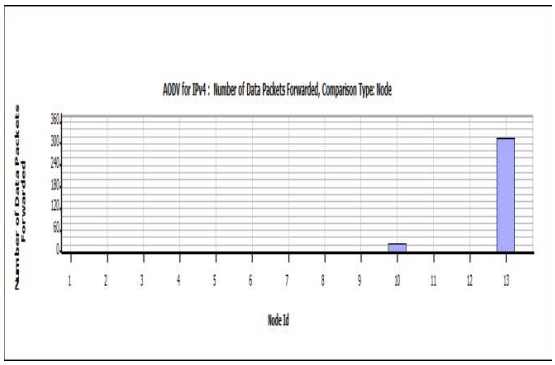

Fig. 9. No. of Data Packets Forwarded in Black Hole Attack scenario

Fig 4. shows the number of data packets forwarded by the FFD devices in normal scenario. In this scenario, nodes 10, 12 and 13 take part in data

forwarding. But in Black Hole attack scenario reflected in Fig 5., node12 is the malicious node and does not forward any packets that it receives.

Average End To End Delay:

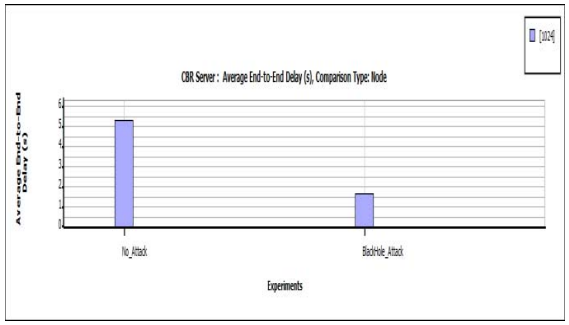

Fig. 10. Average End to End Delay

Fig 6., reveals that there is a decrease in the end to end delay in case of Black Hole attack which is often misleading. This is due to the instantaneous reply generated by the malicious node as it does not check the routing table for appropriate routing decision as would have been done in normal scenario by an FFD.

No. of Data Packets Dropped for no Route:

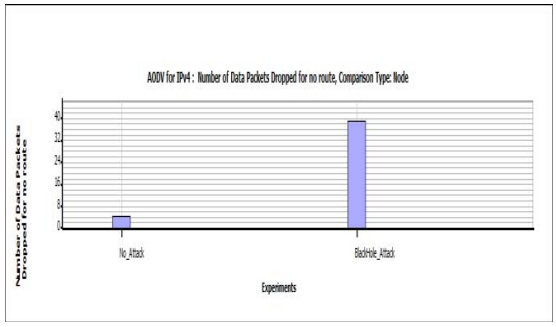

Fig. 11. No. of Data Packets Dropped for no Route

As can be observed from Fig 7., the number of data packets dropped in Black Hole attack scenario is large as compared to the normal scenario. This is because the malicious node 12 simply drops all the incoming packets and does not forward any packet.

No. of Route Reply (RREP) Packets Initiated:

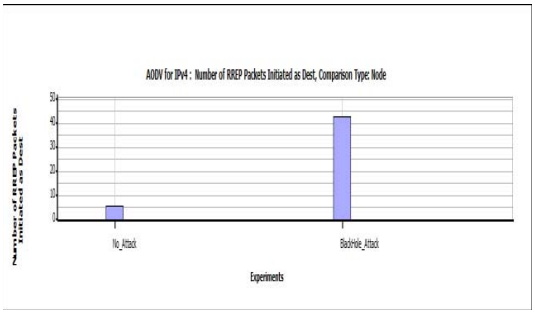

Fig. 12. No of RREP Packets Initiated.

From Fig 8., It can be observed that the number of RREP packets initiated in Black Hole attack scenario is large than the normal scenario without attack. This is because of the nature of the malicious node that sends route replies immediately as it receives any RREQ.

B. DoS By Hello Flooding

Throughput:

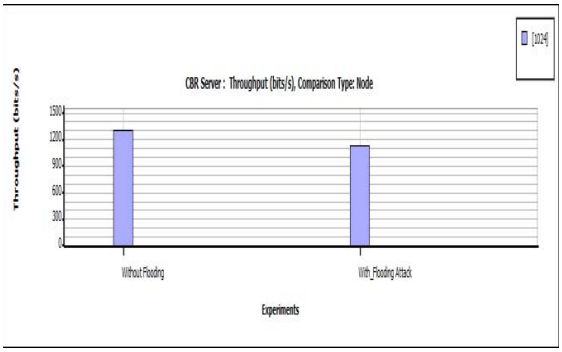

Fig. 13. CBR Server Throughput

Fig 9., Shows the server side throughput for both normal and flooding attacks scenario. It shows that throughput in DoS by Hello Flooding attack scenario is less than that in normal scenario. The reason is that the network gets congested by the flooding attack by the malicious node (node 14). The sensor nodes do not find the free channels for transmission of data, hence less number of packets reach the destination sink i.e., node 1.

Number of Data Packets Dropped due to Buffer Overflow:

Fig. 14. Number of Data Packets Dropped due to Buffer Overflow

From Fig 10, we observe that the number of data packets dropped for buffer overflow is greater in DoS by Hello Flooding attack scenario as compared to the normal scenario. The data packets generated by the nodes are stored in buffer till the node finds the carrier (channel) free. Because of the behaviour of the malicious node, the medium is busy for most of the time. This leads to the accumulation of packets in the limited sized buffer and this finally leads to the buffer overflow.

Number of Hello Messages sent:

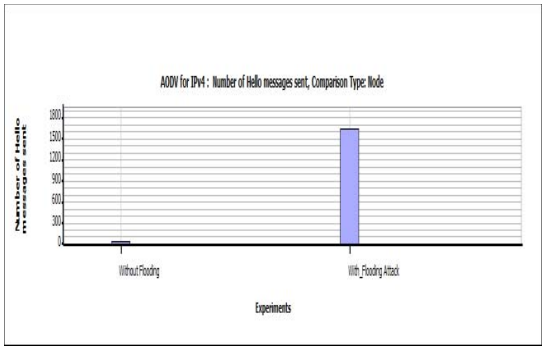

Fig. 15. No. of Hello Messages Sent

From Fig 11, we can observe that the number of hello messages sent in the DoS by Hello Flooding scenario is much large than in the normal scenario. The reason is that in flooding scenario, node 14 (malicious node) has the nature of sending large number of hello messages.

Number of Data Packets Sent as Source:

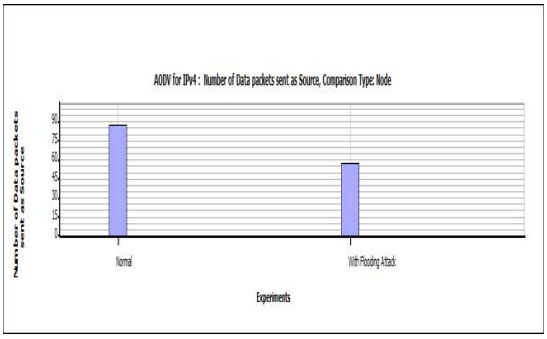

Fig. 16. No of Data Packets Sent As Source

Fig 12, shows that the number of data packets sent DoS by Hello Flooding scenario is less. This is because the CCA mode is carrier sense i.e., a node first senses the channel whether it is available for transmission of packets. But due to flooding attack carried out by node 14, the hello packets flood the network, thereby clogging the network and utilizing most of the bandwidth. Thus the nodes are deprived from sending out their data packets.

Number of Data Packets Received:

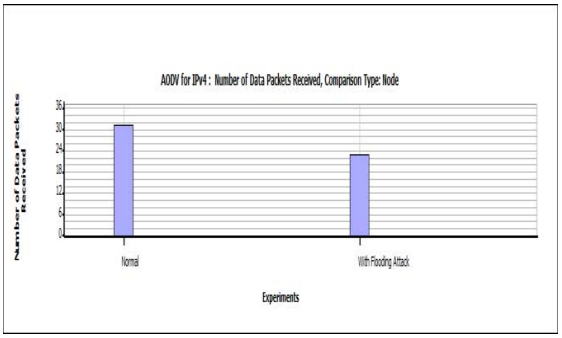

Fig. 17. No. of Data Packets Received

Fig 13, represents the number of data packets received in normal and DoS by Hello Flooding attack scenarios. As is clear from the figure, the number of data packets received in flooding attack is less than the number of packets received in the normal scenario. Due to flooding attack by node 14, node 10 is also affected. Since all the nodes send data through node 10, so under flooding attack, it is not able to receive the packets and hence cannot further forward the packets to node 12 and subsequently to node 1.

Total Packets Dropped from queue:

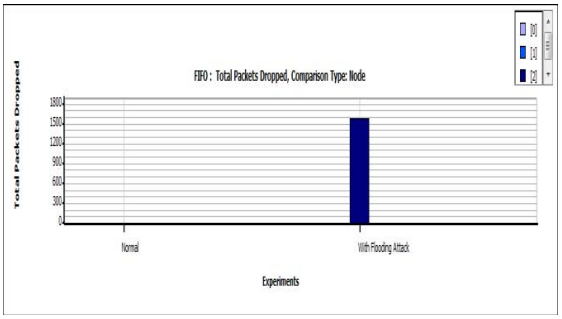

Fig. 18. Total Packets Dropped from queue

From Fig 14., it can be seen that the total packets dropped from FIFO queue is much larger in the DoS by Hello Flooding scenario. The reason is that due to unavailability of bandwidth the nodes

IV. CONCLUSION

In this study, an effort has been made to simulate two basic attacks usually encountered in a WSN scenario. The attacks have been simulated using QualNet Network Simulator. The simulator has been customised to design proper scenarios and to analyse the result. The analysis done would help in designing proper security safeguards against such attacks in the form of proper authentication keeping in mind the resource constraints attributed to WSN node.

ACKNOWLEDGEMENT

This work is supported by Deity, Govt. of India.

REFERENCES

[1]Waltenegus Dargie, Christian Poellabauer, "Fundamentals of Wireless Sensor Networks, Theory and Practice", Wiley and Sons.

[2] Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong, " Security in Wireless Sensor Networks: Issues and Challenges", Feb 20-22, 2006

[3] Y. A. Huang and W. Lee, "Attack analysis and detection for ad hoc routing protocols," in The 7th International Symposium on Recent Advances in Intrusion Detection (RAID'04), pp. 125-145, French Riviera, Sept. 2004.

[4] Adrian Perrig, John Stankovic, David Wagner.," Security in wireless sensor networks", communications of the ACM, vol 47,no. 6, pp 53-57, June 2004.

[5] Xiangqian Chen, Kia Makki, Kang Yen, and Niki Pissinou "Sensor Network Security: A Survey" IEEE Communications Surveys & Tutorials, Vol. 11, No. 2, Second Quarter 2009.

[6] D. Djenouri, L. Khelladi, and N. Badache, "A survey of security issues in mobile ad hoc and sensor networks," IEEE Commun. Surveys Tutorials, vol. 7, pp. 2-28, 2005.

[7] John Paul Walters., Zhengiang Liang, Weisong Shi and Vipin Chaudhary., "Wireless sensor network security : A Survey", Chapter 17, Security in distributed grid and pervasive computing 2001

[8] A. D. Wood and J. A. Stankovic, "Denial of Service in Sensor Networks," IEEE Computer, vol. 35, pp. 54-62, 2002.

[9] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto, "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method" International Journal of Network Security, Vol.5, No.3, PP.338–346, Nov. 2007

[10] Kai Xing, Shyaam Sundar Rajamadam Srinivasan, Manny Rivera, Jiang Li, Xiuzhen Cheng, "Attacks and Countermeasures in Sensor Networks: A Survey" 2005 Springer

[11] Faieza Hanum Yahaya, Yusnani Mohd Yussoff, Ruhani Ab. Rahman and Nur Hafizah Abidin, "Performance Analysis of Wireless Sensor Network" 2009 5th International colloquium on Signal Processing and Its Applications (CSPA)

[12]C. Perkins and E. Royer, "Ad-hoc on-demand distance vector routing," in MILCOM '97 panel on Ad Hoc Networks, 1997.

[13] Shishir K. Shandilya, Sunita Sahu," A Trust Based Security Scheme for RREQ Flooding Attack in MANET", International Journal of Computer Applications (0975 – 8887) Volume 5– No.12, August 2010

[14] QualNet Simulator Documentation. ”QualNet 5.2 UsersGuide “Scalable Network Technologies, Inc., Los Angeles, CA 90045