SIMULATING AND ANALYZING RREQ FLOODING ATTACK IN WIRELESS SENSOR NETWORKS

Ayaz Hassan Moon
National Institute of Electronics and Information Technology ,Srinagar, J & K.

Ummer Iqbal
National Institute of Electronics and Information Technology ,Srinagar, J & K.

G. Mohiuddin Bhat
Department of Electronics and Instrumentation Technology, University of Kashmir, Srinagar, J & K.

Zaffar Iqbal
National Institute of Electronics and Information Technology, Srinagar, J & K.

***Abstract*—Broadcast nature of Wireless Sensor Networks subjects them to assortment of various attacks.. Denial of service is the most common class of attack launched against wireless sensor networks. To mitigate these attacks it gets imperative to comprehend their circumstances and end results. In this paper, we simulate and analyze DOS attacks by RREQ flooding. The study is based on a generic WSN model made in qualnet . The code library has been changed to simulate RREQ Flooding attack in the WSN simulation model specified. The impact of this attack on different network parameters like throughput, packet drop, end to end delay, energy consumption has been discussed in detail**

Keywords— Wireless Sensor Network (WSN), Route Request (RREQ), Route Reply (RREP), Denial of Service (DoS).

I. INTRODUCTION

Wireless sensor networks consist of large number of sensor nodes having limited resources of battery, processing power, storage capacity. These sensor nodes have to operate in complex harsh environments autonomously without any human intervention. One of the fundamental objectives for WSN is to collect data from the physical world in a secured environment [1]. Broadcast nature of WSN attracts various types of threats that exhaust the node resources [2] [3]. These attacks significantly affect the quality of service parameters like throughput, delay, energy consumption [4]. Limited resources of WSN nodes makes security a critical design issue. One of the commonly encountered security attacks in WSN is DoS attack. Denial of Service (DoS) is a class of attack wherein the objective is to make network resources unavailable to its intended users[5]. One of the most common ways to perform this attack is flooding the network with unsolicited, overwhelming flux of packets, thereby saturating the bandwidth and depleting the target system resources. Based upon the routing protocol used, WSN nodes send various types of control packets to ensure a connected topology. In case of AODV routing protocol, control packets involve HELLO, RREQ and RREP packets [6]. Hello packets are broadcasted by a node to know its immediate neighbours. RREQ packets are used in AODV protocol to find a route to destination [7]. When a node receives such RREQ packet, it broadcasts it to its neighbours and this procedure continues until the route to destination is obtained. When a node knows the path, it sends RREP back to the source[8]. Thus, a path is established for actual data communication. In this paper, we present DoS attack in AODV protocol by RREQ flooding and its impact on the quality of service parameters. When a malicious node receives such a packet, it generates multiple Route Request packets exhausting limited bandwidth and resources of the sensor nodes which in turn severely affects the network performance. Moreover, the RREQ packets continuously flooded by the malicious node result in the neighbour node not being able to process other packets. Thus functioning of the legitimate node is disrupted further degrading the network operation.

II. METHODOLGY

Simulation study in Qualnet consists of three stages [9]. In the first stage, a simulation model is created based on the domain and application parameters. Qualnet architect is used for creating simulation models. In second stage, results are collected based on various parameters which are configurable. In the final stage, analysis of these parameters is done to deduce results and inferences. A wireless sensor network scenario is created in qualnet architect which consists of the fixed sensor nodes and also few malicious nodes. A simulation model for analysing the effect of RREQ flooding is shown in Fig 1. This scenario consists of two nodes with IDs 2, 5 that are programmed to act as malicious nodes, and twelve legitimate sensor nodes among which node IDs 4, 8, 9 are Reduced Functional Devices (RFDs) and the remaining nodes are Full Function Devices (FFDs). In this scenario, node 1 is configured to act as sink which collects data from all the sensor nodes. The necessary modifications were made in the qualnet GUI (.prt file) and the WSN code library. The source code of the AODV routing protocol has been modified to incorporate RREQ flooding attack. The modified GUI is shown in Fig 2. When any node in the network wants to communicate to other nodes, it broadcasts route request (RREQ) packets to its neighbours. The malicious node also receives such a packet if it is in the range of sending node.

This reception of RREQ packet by malicious node serves as trigger for it to launch RREQ flooding attack. This is done by creating duplicate packets of this received RREQ packet and the multiple copies are forwarded to other nodes, which in turn forwards them again. As a result, there occurs congestion in the network and the legitimate nodes exhaust its resources uselessly, which degrades the overall network performance [10].The simulation parameters considered are listed in Table I:

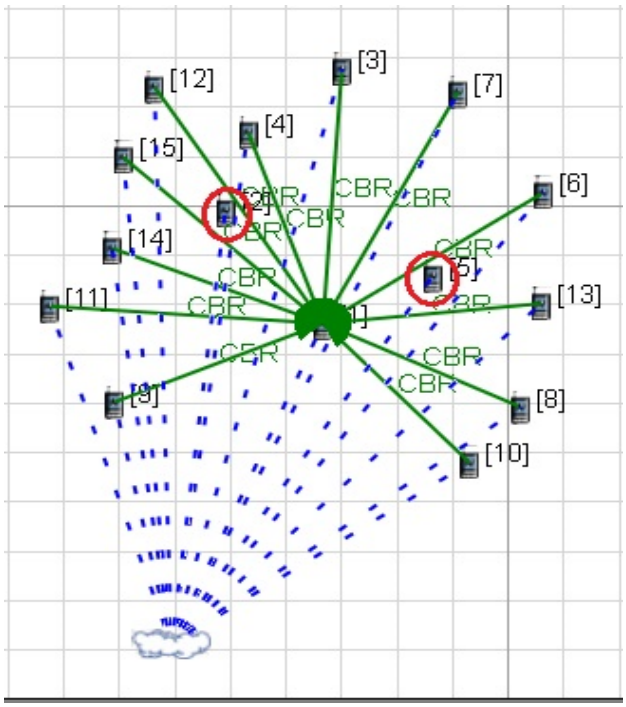

Fig. 1. Deployment Scenario

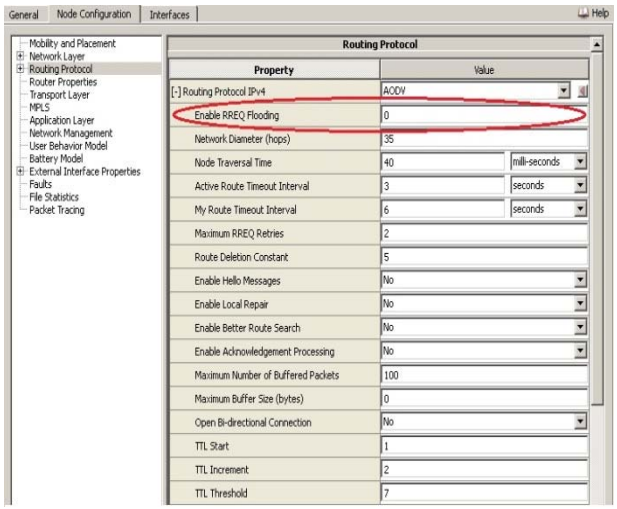

Fig. 2. Changed qualnet GUI

TABLE I: SIMULATION PARAMETERS

Number of legitimate Nodes	12
Energy Model	MicaZ
Battery Model	Linear
Radio Type	802.15.4
Transmission Power	0 dbm
Routing Protocol	AODV
Number of Malicious Nodes	2
Deployment Area	1000 x 1000

III. RESULTS AND DISCUSSION

In this section, we present the results of simulation and then discuss them briefly.

A. RREQ packets initiated

RREQ packets are initiated by a node when it needs to find a route to destination. Malicious node upon reception of RREQ packet generates multiple unsolicited RREQ packets to disrupt normal network operation. Fig 3 indicates approximately 100 % increase in RREQ packets generated by various nodes which would result in Heavy network congestion.

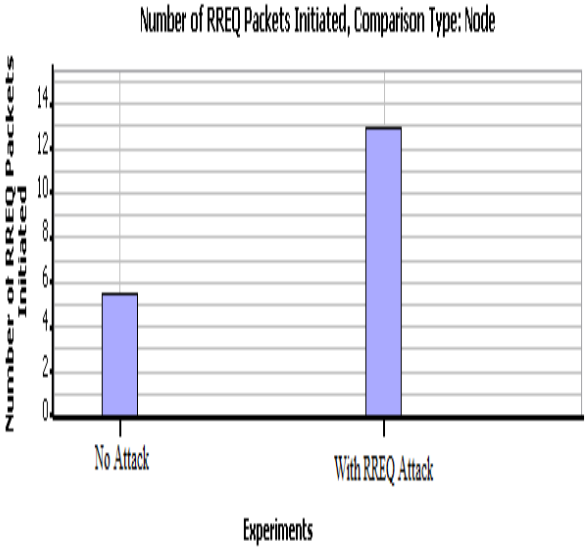

Fig. 3.

Fig. 3: RREQ packets initiated Comparison

B. Energy consumption

This metric is of utmost importance in wireless sensor networks which directly influences the lifetime of the nodes and the network too. Transmitting 1 bit data consumes energy equivalent to computational energy cost of over 800 bits. This implies that the no of transmissions in WSN need to be curtailed as much as possible. The simulation indicates that the Malicious node triggers a surge of RREQ packets to flood the network. This causes the neighbouring nodes to process unnecessary packets which can lead to energy exhaustion and reduce the lifetime of the network. Moreover, flooded RREQ packets may further be broadcasted by the receiving nodes causing a chain reaction of unsolicited broadcast. This unwanted energy intensive task severely depletes further the battery resource of sensor nodes. The Fig 4 shows energy comparison between normal network operation and the network under RREQ flooding attack signifying an increase of nearly 24% in the energy consumption of a node.

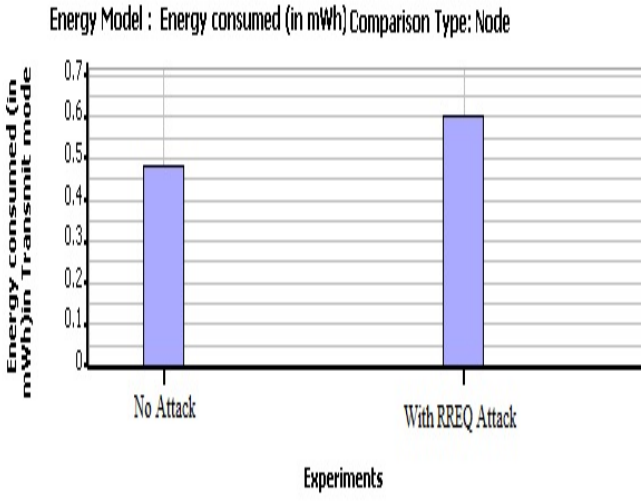

Fig. 4: Energy Consumed Comparison

C. . End- to-End delay

The flooding of unwanted RREQ packets wastes the limited bandwidth available to sensor nodes. The large amount of traffic generated causes severe congestion in the network resulting in increased end to end delay. Fig 5 shows average end-to-end delay comparison between normal and RREQ attack scenario. It clearly depicts that the delay is increased by 66% in RREQ attack scenario.

D. Buffer overflow

Sensor nodes have limited buffer capacity. Unsolicited traffic and undesired packets being sent to sensor nodes exhausts this restricted resource quickly. As a result, the valid sensor nodes are unable to process the normal desired packets. Fig 6 below represents the buffer utilization comparison which can result in dropping of data packets to the extent of 100 % in a given RREQ flooding scenario.

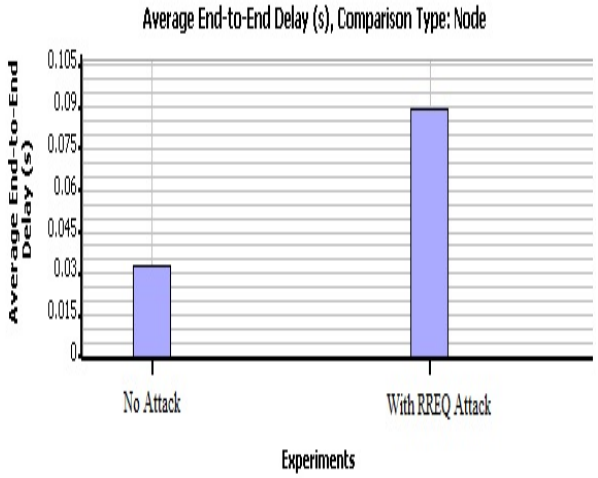

Fig. 5: End-to-End delay Comparison

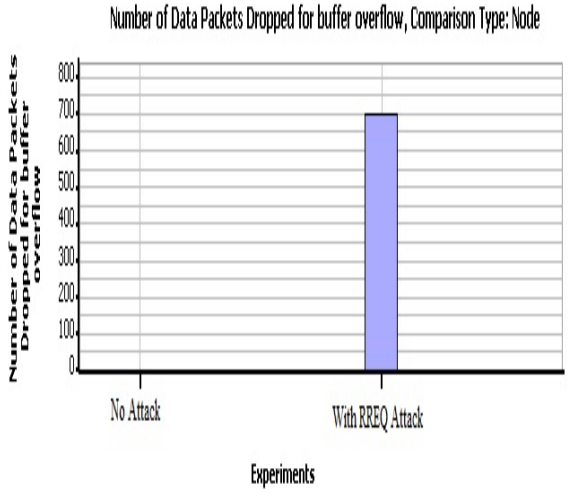

Fig. 6: Buffer Overflow Comparison

E. Throughput comparison

Throughput is defined as the average rate of successful message delivery over a communication channel. Fig 7 shows throughput comparison of the RREQ flooded network and the normal scenario.

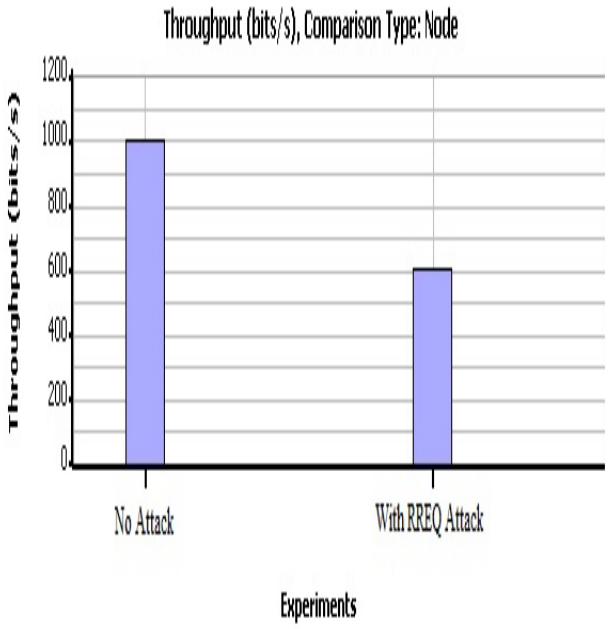

Fig. 7: Throughput Comparison

It evidently portrays that the throughput is less in RREQ flooded scenario than in the normal scenario. The reason being that the network gets congested due to unsolicited traffic. The attack wastes the communication bandwidth, overflows node buffers and denies processing of legitimate data by sensor nodes, as a result of which the throughput of the network gets reduced.

IV. CONCLUSION

Wireless sensor networks are often deployed in unattended environments where nodes are prone to a variety of attacks launched by intruders. The characteristics like limited processing capability, storage and battery restrictions attract various types of threats and restrict us in using high standard measures to reduce chances of attacks. In this paper, the impact of RREQ flooding attack on various network performance parameters like RREQ packets initiated, Energy consumption, End to End Delay , Buffer Overflow and throughput was analysed. RREQ flooding attack reduces the performance of the wireless sensor network because it exhausts the constrained resources of network quickly. This analysis would help in designing relevant security mechanisms to thwart RREQ flooding attack.

References

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

[2] Y. A. Huang and W. Lee, "Attack analysis and de-tection for ad hoc routing protocols," in The 7th In-ternational Symposium on Recent Advances in Intru-sion Detection (RAID'04), pp. 125-145, French Riv-iera, Sept. 2004.

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

[4] [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)

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

[6] Varsha Sahni, Pankaj Sharma, Jaspreet Kaur, Sohajdeep Singh," Scenario Based Analysis of AODV and DSR Protocols Under Mobility in Wireless Sensor Networks " , 2012 International Conference on Advances in Mobile Network, Communication and Its Applications

[7] 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

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

[9] QualNet Simulator Documentation. "QualNet 5.2 UsersGuide "Scalable Network Technologies, Inc., Los Angeles, CA 90045.

[10] [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)