Analysis of Flooding Attacks on Wireless Sensor Network

Kapil Mangla[1], Ravinder Kumar[2], Vinit Bhargava[3]

[1]*Asst. Proff at SCET Palwal Affiliated to MDU, Rohtak (Haryana), India.*
[2]*M.Tech Scholar at SCET Palwal Affiliated to MDU, Rohtak (Haryana), India.*
[3]*Asst. Proff at IET, Alwar, Affiliated to RTU, Kota (Rajsthan), India.*
[1]kapilm@satyaedu.org, [2]Ravi31045@gmail.com, [3]er.bhargava.vinit@gmail.com

Abstract: **Wireless sensor network have emerged as an important application of the ad-hoc networks paradigm, such as for monitoring physical environment. These sensor networks have limitations of system resources like battery power, communication range and processing capability. Low processing power and wireless connectivity make such networks vulnerable to various types of network attacks. One of them is hello flood attack, in which an adversary, which is not a legal node in the network, can flood hello request to any legitimate node and break the security of WSN.**

Flooding attack occurs in the network. It suddenly decreases the overall performance of the wireless sensor networks. In this paper flooding attack on wireless sensor network is analyzed. The performance of WSN under flooding attack on various network parameters is deeply studied.

Keywords: WSN, Flooding Attacks, signal strength.

1. INTRODUCTION

Wireless sensor networks are a particular type of ad hoc network, in which the nodes are 'smart sensors'. Sensors are small devices equipped with advanced sensing functionalities (for monitoring temperature, pressure, acoustics etc.), a small processor, and a short-range wireless transceiver [1]

However, while the routing strategies and wireless sensor network modeling are getting much preference, the security issues are yet to receive extensive focus. Security is a broadly used term encompassing the characteristics of authentication, integrity, privacy, non-repudiation, and anti-playback. The more the dependency on the information provided by the networks has been increased, the more the risk of secure transmission of information over the networks has increased. Here, explore the security issues and challenges for wireless sensor networks and discuss the crucial parameters that require extensive investigations. [2][3]

2. ATTACKS ON SENSOR NETWORKS

Most sensor network routing protocols are quite simple, and for this reason are sometimes even more susceptible to network attacks as compared to general ad-hoc routing protocols. Most network layer attacks against sensor networks fall into one of the following category. [2]

2.1 Flooding Attack:

Many protocols require nodes to broadcast HELLO packets to announce themselves to their neighbors, and a node receiving such a packet may assume that it is within (normal) radio range of the sender. This assumption may be false: a laptop-class attacker broadcasting routing or other information with large enough transmission power could convince every node in the network that the adversary is its neighbor. For example, an adversary advertising a very high-quality route to the base station to every node in the network could cause a large number of nodes to attempt to use this route, but those nodes sufficiently far away from the adversary would be sending packets into oblivion. The network is left in a state of confusion. A node realizing the link to the adversary is false could be left with few options, all its neighbors might be attempting to forward packets to the adversary as well.[4][5]

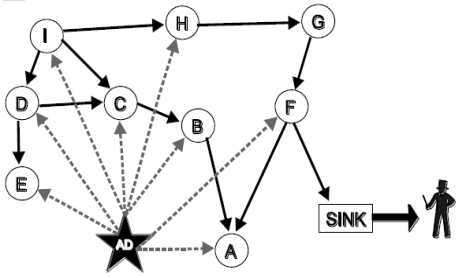

Fig 2.1 Flooding Attacks

2.2 Efficient Flooding in Wireless Sensor Networks Secured with Neighborhood Keys:

Network flooding is a fundamental communication primitive for Wireless Sensor Networks (WSN). Flooding is used for disseminating code updates and parameter changes. It affects the operation of all deployed node in WSN. When flooding occurs each node, typically, broadcasts the flooding packet once. The costs for flooding, however, can become significant if neighborhood keys are used for communication, since, instead of a single broadcast, a node is required to perform several unicast transmissions. For flooding code updates (a common operation in WSN, since they are physically inaccessible) the naive support of broadcasting through multiple unicast transmission can be very costly. They formulate the problem of deciding if it is possible to achieve 100% network coverage by a flooding packet,

when each node cleverly chooses one of its keys to unicast the broadcast message. [6]

3. MOTIVATION OF THE WORK

In wireless sensor network, there are so many challenges. The main challenges are how to provide maximum lifetime to network and how to provide secure communication to network. As sensor network totally rely on battery power, the main aim for maximizing lifetime of network is to conserve battery power or energy with some security considerations.

There are various attacks on wireless sensor network. Attacks mainly classified into two parts, active attack and passive attack. Passive attacks are very difficult to detect in comparison with active attacks.

Active attacks are again classify into attacks on routing protocol, fabrication, dos, modification, impersonation, eavesdropping. Here considering only attacks on routing protocol, which are as follows Sybil attacks, wormhole attack, sinkhole, flooding attack. In this paper, considering Flooding attack and will analyze the flooding attack with various performance parameters.

3.1 Objectives of Proposed Research Work:

- To study and analyze the effect of flooding attack in wireless sensor network.
- To study and analyze the performance of wireless sensor network.
- To study and analyze the effect of flooding in wireless sensor network.

3.2Performance parameters:-

- Packet Delivery Ratio
- Received Packets

3.3Simulation Environment:-

In the research, NS2 is used to simulate a virtual environment, as each run of the simulator accepts as input that describes the exact effect of each node and the exact time at which each change in node origination or cluster head organization is to occur and its varying with the distance of cluster head, no of nodes and data gathering rate. [7]

4. RESULT AND ANALYSIS

In this Section, the experimented and simulated work results are presented and then through graph does an analysis of the result obtained.

The effect of Flooding and hello flood attack is analyzed. Effect of flooding attack is analyzed with number of nodes varies and also analyzed the impact on Packet Delivery Ratio and Received packet is analyzed. The number of nodes is as 10, 30, 50, 70, 90 and 110.

It analyzed the effect of flooding and hello flood attack at varies number of nodes and analyzed overall performance of network when flooding attack occurs.

4.1Simulation Result:

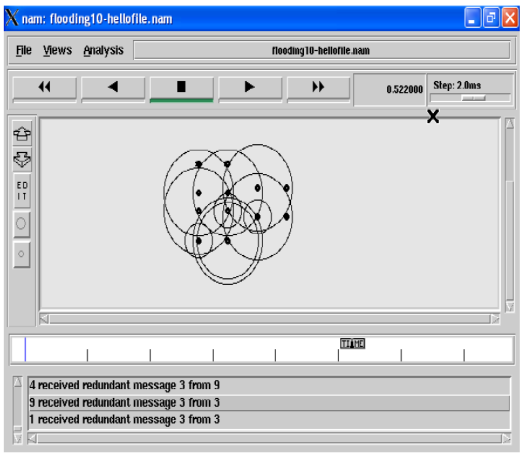

Figure 4.1 Output of Flooding10-hellofile

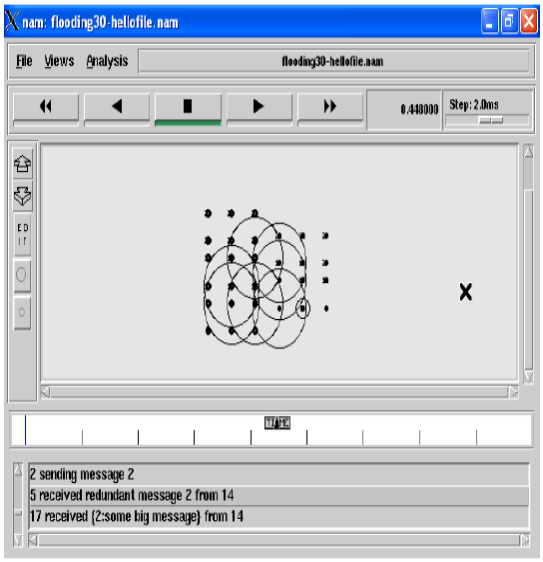

Figure 4.2 Output of Flooding30-hellofile

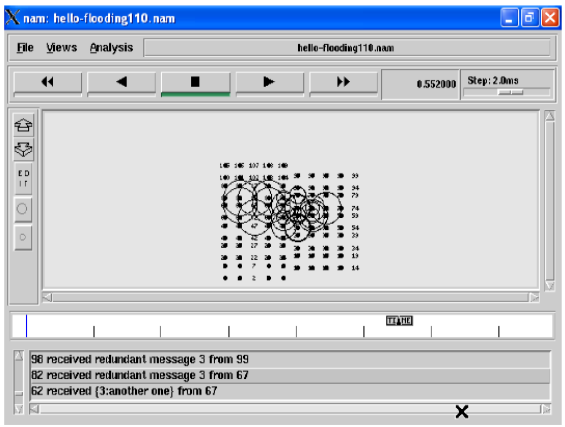

Figure 4.2 Output of Flooding110-hellofile

4.2 Analysis of Flooding Attack on Packet Delivery Ratio with different number of nodes:

Packet delivery ratio is the ratio of the number of delivered data packet to the destination. This illustrates the level of delivered data to the destination. The greater

value of packet delivery ratio means the better performance of the protocol.
Formula used to calculate packet delivery ratio.
Σ Number of packet receive / Σ (dropped Packet + received Packet)

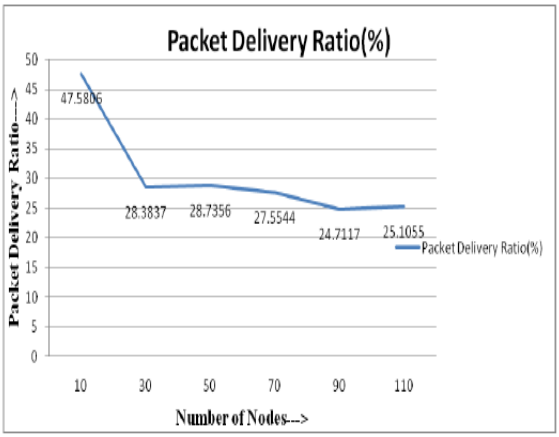

Figure 4.4 Graph Packet Delivery ratios

4.3 Analysis of Hello Flood Attack on Received Packets with different number of nodes
Received packet means number of packet actually received by receiver. To calculate the number of received packet following formula to be used. The greater value of received packets means the better performance of the network.
Number of packet received = Number of packet send – Packet lost.

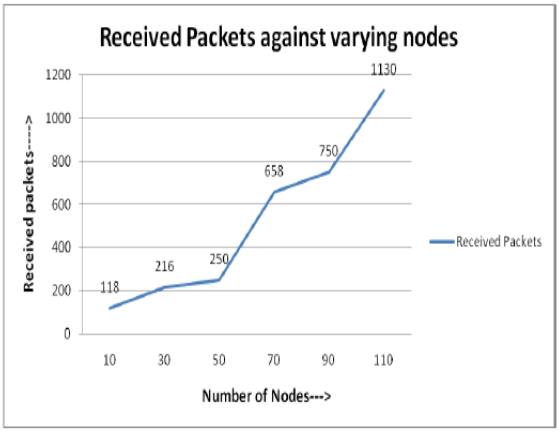

Figure 4.5 Graph of Received packet with different number of nodes

4.4 Result Analysis at a Glance:
Table 4.1 present all simulation result at a glance. In this table packet delivery ratio, received packets with varies number of nodes are presented.

Number of Nodes	Packet Delivery Ratio(PDR)	Received packet
10	47.5806	118
30	28.3837	216
50	28.7356	250
70	27.5544	658
90	24.7117	750
110	25.1055	1130

Table 4.1 Simulation Result at a Glance

CONCLUSION AND FUTURE WORK

5.1 Conclusion
In this work the clearly stipulated objective in the beginning of the dissertation has been accomplished. In this work, impact of hello flood attack has been analyzed on packet delivery ratio, received packet, dropped packet and average throughput with varying number of nodes. In this work simulation results have been carried out by using network simulator (NS2), which clearly demonstrates that when hello flooding attack occurs it decreases the performance of the wireless sensor network. Result also shows that more number of nodes in a wireless sensor network, more decreases overall performance of the wireless sensor network.

5.2 Future work
Hello packets plays an important role for establishing connection among nodes in wireless sensor network though these hello packets may be also used as an attack on network resulting in failure in data transmission in wsn. In this dissertation the network performance under hello flood attack on various parameters is lightened. The proposed work can be used for overcoming from the effect of hello flood attack on wsn.

REFERENCES

[1] Luis E. Palafox, J. Antonio Garcia-Macias,(2008) Security in Wireless Sensor Networks, IGI Global, Chapter 34.
[2] Alok Ranjan Prusty, ―The Network and Security Analysis for Wireless Sensor Network: A Survey‖, (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (3) , 2012,4028 – 4037 ISSN:0975-9646.
[3] Undercoffer, J., Avancha, S., Joshi, A., and Pinkston, J.―Security for Sensor Networks‖, CADIP Research Symposium, 2002.
[4] John Paul Walters, Zhengqiang Liang, Weisong Shi, Vipin Chaudhary,‖ Wireless Sensor Network Security: A Survey‖, Security in Distributed, Grid, and Pervasive Computing Yang Xiao Auerbach Publications, CRC Press 2006.
[5] Dr. Jens-peter kaps,‖ secure routing in wireless sensor networks‖, srividya shanmugham, scholarly paper, march 2009.
[6] Amin Hassanzadeh, Radu Stoleru, Jianer Chen, ‖Efficient Flooding in Wireless Sensor Networks Secured with Neighborhood Keys‖, 2011 IEEE 7th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob).
[7] NAM: Network Animator, http://www.isi.edu/nsnam/nam/.
[8] Cygwin user‘s Guide, http://www.cygwin.com.
[9] M. Greis, ‖Tutorial for the network simulator NS‖, http://www.isi.edu/nsnam/ns/tutorial/index.html.