INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

PREVENTIVE MEASURES FOR BLACKHOLE ATTACKS IN WIRELESS SENSOR NETWORK

PALLAVI A. DHANDE, PROF. GAURAV D. GULHANE, DR. H. R. DESHMUKH

CSE Department, DRGIT&R, Amravati, Maharashtra, India

Accepted Date: 15/03/2016; Published Date: 01/05/2016

Abstract*:* Wireless sensor networks are vulnerable against various types of external and internal attacks being limited by computation resources, smaller memory capacity, limited battery life, processing power & lack of tamper resistant packaging. The black hole attack is one of the well-known security threats in wireless sensor networks. . In this paper, we analyze the behavior of wireless network with or without black hole attack with different parameters. Hence from all these result we can conclude that any black hole in the network can degrade the performance of the network. The intruders utilize the loophole to carry out their malicious behaviors because the route discovery process is necessary and inevitable

Keywords: Wireless Sensor Network, routing protocols, End to End delay, Packet Delivery Ratio, black hole attack, NS2.

Corresponding Author: MS. PALLAVI A. DHANDE

Access Online On:

www.ijpret.com

How to Cite This Article:

Pallavi A. Dhande, IJPRET, 2016; Volume 4(9): 1720-1729

PAPER-QR CODE

INTRODUCTION

Sensor networks [16][17][18] are highly distributed networks of small, lightweight wireless nodes, installed in large numbers to monitor the environment or system by the measurement of physical parameters such as temperature, pressure, or humidityThe sensor nodes are similar to that of a computer with a processing unit, limited computational power, limited memory, sensors, a communication device and a power source in form of a battery. In a typical application, a WSN is scattered in a region where it is meant to collect data through its sensor nodes. . Building sensors have been made possible by the recent advances in micro-electromechanical systems (MEMS) technology. The applications of sensor networks are endless, limited only by the human imagination [16] [17] [18]. In this paper an overview on various WSN attacks are mentioned with a special mention on black hole attack. Performance evaluation is done for black hole attack in WSN environment. Also proved that network performance decreases in presence of black hole attack. Network performance measure by considering parameters average end to end delay, Packet Delivery Fraction (PDF) and Throughput. The rest of the Paper is as follows: Section 2 gives literature review followed by section 3 in which black hole attacks in WSN are highlighted. In section 4 and 5 analyzed and discussed, followed by conclusion in section 6.

LITERATURE SURVEY

In paper [1] a comprehensive security model is presented for tailoring the needs of sensor networks. The authors outline the security properties that must be considered when designing a secure sensor networks. The various challenges for sensor networks are also discussed. In paper [2] various types of attacks on WSN and their respective countermeasure are shown. The role of a cNode is to analyze traffic and to send back a warning to the cluster head if any abnormal traffic is detected. The authors present the development of trust mechanisms along with short summarization of classical trust methodologies emphasizing the challenges of trust scheme in WSNs. In paper [3] novel approaches proposed for detecting Denial of Service (DoS) attacks in cluster-based sensor networks. This method is based on the election of controller nodes called cNodes which observe and report DoS attack activities.

In paper [5] an efficient technique that uses multiple base stations deployed in the network to counter the impact of black holes on data transmission is proposed. Paper [6] explains two alterations to the Lightweight Medium Access Control (LMAC) protocol are proposed and evaluated.The proposed dynamic solution improves the network lifetime by minimizing the energy consumption for each sensor node and can improve security by preventing attacks.

Initially, the algorithm explains taxonomy of security and reliability for cluster head election and clustering in WSNs. In paper [4] the review of the state-of-art of clustering protocols in WSNs with special concentrate on security and reliability issues.They propose countermeasures against typical attacks and show how they improve the discussed protocols.

First one is the Data Packet Separation Slot Size Randomization (DSSSR); and the second is Round Robin (RR) slot size assignment. The paper proves that (DS-SSR) is better in terms of Energy efficient denial of service link layer jamming attacks. This paper also explains that use of RR scheme directly affects system throughput for using countermeasure against energy efficient jamming. In paper [8] authors have focused on security of Wireless Sensor Network, security being fundamental to the acceptance. In paper [9] vulnerability of the network to black hole attack is discussed. The use of intelligent agents called Honeypots is done to detect these attacks. In paper [7] a protocol for establishing the security mechanism of wireless sensor networks and devising a scheme for preventing Denial of Service attacks is proposed. The protocol not only defends the network against Denial of Service attacks but also maintains confidentiality, integrity and authenticity of data transmitted between sensor nodes.

The Honeypots generate dummy Route Request (RREQ) packets to detect and prevent black hole attackers. In paper [10] a requirement based Intrusion Detection System for WSN is proposed. This paper [11] reviews the design and implementation of a novel defence strategy designed to work alongside existing Denial of Service (DoS) counter measures. The previous approaches were generic and were not capable of filtering out all attack traffic, instead a small amount of attack traffic reached the attackers intended victim. This small level of attack traffic posed a significant threat to the limited resources of WSN. The proposed scheme tries to optimize the local information (information collected by watch dogs) into global information (decision taken by cluster head) in order to compensate the communication pattern in network. In paper [12] authors have developed algorithm to contest with Black hole attack by using co-operation with neighbours who claim to have a route to destination. The simulation results show that the proposed protocol provides better security and also better performance in terms of packet delivery than the conventional AODV in the presence of Black holes with minimal additional delay and Overhead. In paper [13] the denial-of-sleep attack, which targets a battery powered device's energy supply is studied. The survey of denial-of-service threats is updated with current threats and countermeasures.

In paper [14] the security related issues and challenges in wireless sensor networks are investigated. They concluded that most of the attacks against security in wireless sensor

networks are caused by the insertion of false information by the compromised nodes within the network. In paper [15] all known security issues in wireless sensor networks are documented along with the research direction towards counter measures of these threats.

BLACK HOLE ATTACK IN WSN

Black hole attacks occur when an intruder captures and reprograms a set of nodes in the network to block the packets they receive instead of forwarding them towards the base station. The network performance parameters i.e. throughput and end- to- end delay are affected in the presence of black hole nodes; throughput becomes very less and end- to- end delay increases. As a result any information that enters in the black hole region is captured. Black hole attacks are easy to constitute and they are capable of undermining network effectiveness by partitioning the network, such that important event information do not reach the base stations.

Black hole attack in WSN is carried out as:

Normal Flow of Packets

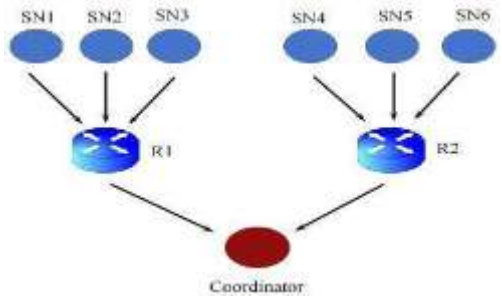

Fig 1: Normal flow of Packets

Figure 1 shows normal flow of packets. In this scenario we have 6 sensor nodes (i.e. SN1, SN2, ---- SN6), two router nodes (R1, R2) and a coordinator. The sensor nodes sense any physical phenomenon, convert this into information and send this sensed and processed information to router node R1 and R2. Sensor nodes SN1, SN2 and SN3 are reporting to router R1 and SN4, SN5 and SN6 are reporting to router R2. The router R1 and R2 further sends data to Coordinator node.

Black Hole Attacking Scenario

Figure 2 shows blackhole attacking scenario. In this scenario we have 6 sensor nodes (i.e. SN1, SN2, --- -SN6), two router nodes (R1, R2) and a coordinator. The sensor nodes sense any physical phenomenon, convert this into information and send this sensed and processed information to router node R1 and R2. Sensor nodes SN1, SN2 and SN3 are reporting to router R1 and SN4, SN5 and SN6 are reporting to router R2. The router R1 send data to coordinator node. But router R2 is a Blackhole attacker and absorbs all the traffic coming to it without sending it further to coordinator. Router R2, the blackhole node is represented by a black background here. Due to the consumption of all the packets by the Blackhole attacker, R2 here, the delay increases and throughput decreases thus degrading in the performance of network.

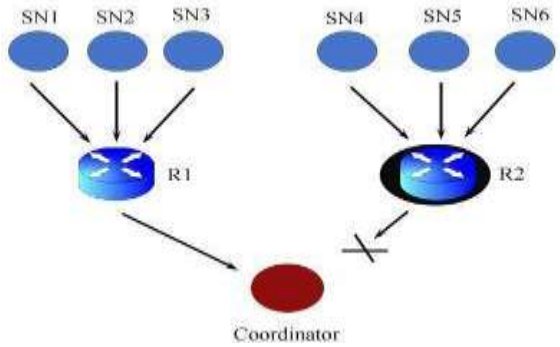

Fig 2 : Black Hole Attacking Scenario

Analysis And Discussion

In this scenario, all the three routing protocols are evaluated in different number of nodes, keeping other factors fixed and performance evaluated based on the three performance metrics which are Packet Delivery Fraction, End-to-End Delay and throughput. Table 4 list the simulation parameters applied in the experiments.

Table 1 : NS2 set up table

Parameter	***Value***
Number of Nodes	10 to 90 (varying)
Pause Time	2 Seconds
Simulation time	180 seconds
Traffic type	CBR
Data Payload	512 bytes/packet
Mobility Model	Random Way Point Algorithm

Packet Delivery Ratio (PDR) : ∑ Number of packet receive / ∑ Number of packet send The greater value of packet delivery ratio means the better performance of the protocol.The ratio of the number of delivered data packet to the destination. This illustrates the level of delivered data to the destination.

End-to-end Delay: the average time taken by a data packet to arrive in the destination. It also includes the delay caused by route discovery process and the queue in data packet transmission. Only the data packets that successfully delivered to destinations that counted.

∑ (arrive time – send time) / ∑ Number of connections

The lower value of end to end delay means the better performance of the protocol.

Throughput: throughput is the ratio of no of packet send to the no of packet received in a given amount of time.

RESULT

Packet Delivery Ratio

It is the ratio of the data packets delivered to the destinations to those generated by the constant bit rate (CBR) sources is known as Packet Delivery Fraction (PDF). Fig. 4 shows the PDF of the AOMDV and Black hole models for varying number of nodes. The PDF is always low in the black hole model as compared to the AOMDV model. The number of dropped packets in the black hole model is greater than that in the AOMDV model. The black hole model does the packet drop by allowing communication through it.

Table 2: PDF in AOMDV Vs. PDF in Black Hole

Nodes	PDR	PDR Blackhole
10	77.4613	73.4047
20	89.2206	83.5232
30	87.7165	85.3236
40	87.2835	78.0994
50	85.1413	87.1923

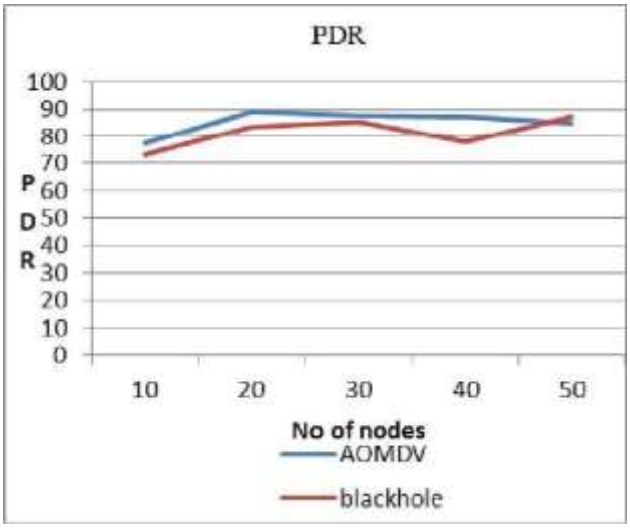

Fig 3 : PDF with or without Black hole in AOMDV

Average End-to-End Delay

Average end-to-end delay includes all possible delays due to buffering during route discovery latency, queuing at the interface queue, retransmission delays at the MAC, and propagation and transfer times of data packets. Table shows the end-to-end delay incurred in sending the data from the source node to sink node in the AOMDV and black hole models. The end-to-end delay is higher in the black hole model as compared to the AOMDV model.

Table 3: Delay in AOMDV Vs. PDF in Black Hole

Node	E2edelay	E2EDelay Blackhole
10	0.00340795	0.00612434
20	0.00895958	0.0132625
30	0.0060726	0.0125268
40	0.0129921	0.0144254
50	0.00467113	0.00927064

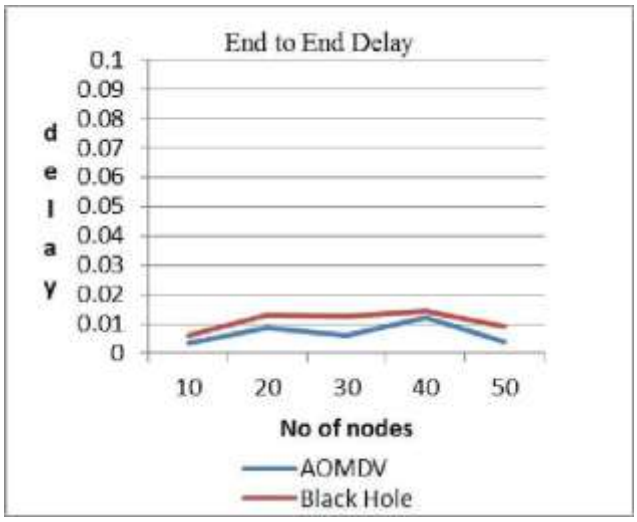

Figure 4 : Delay with or without Black hole in AOMDV

Throughput

Throughput is the amount of data transferred from one place to another or processed in a specified amount of time. Data transfer rates for disk drives and networks are measured in terms of throughput. Typically, throughputs are measured in kbps, Mbps and Gbps.

Table 4: Throughput in AOMDV Vs. PDF in Black Hole

Node	Throughput AOMDV	Throughput Blackhole
10	29.89	29.72
20	35.79	35.41
30	36.41	32.76
40	34.50	34.12
50	35.11	34.23

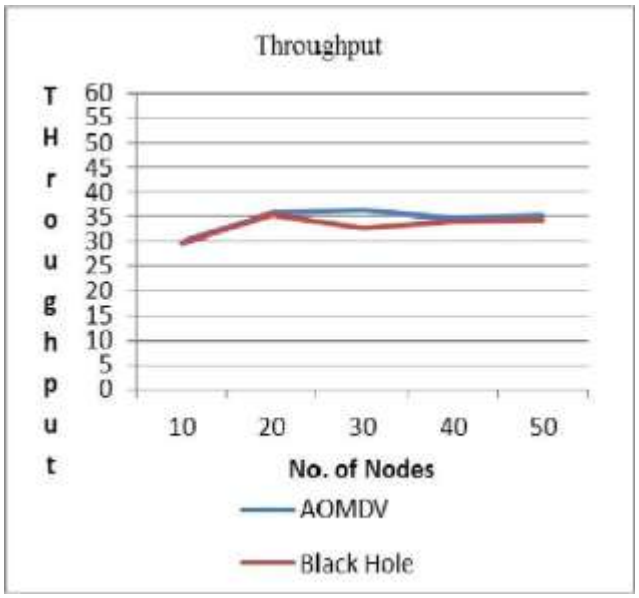

Figure 5 : Throughput with or without Black hole in AOMDV

CONCLUSION

After simulation we reach to conclusion that simulation of these two scenarios AOMDV and AOMDV with black hole attack, black hole affects the performance of network. Hence performance of the network under black hole attack is affected hence we have to develop an effective mechanism which can keep black hole nodes a side and improve the performance under black hole attack. Different preventive techniques are developed but these techniques are not work in all condition. So we need to develop a digital signature based cryptosystem model which can keep nodes in the network authentic and allow safe transmission of data within the network. The packet delivery ratio decreases, average end to end delay increases and system throughput also decreases after adding black hole attack in AOMDV protocol.

REFERENCES

1. Asmae Blilat, Anas Bouayad, Nour el houda Chaoui, Mohammed El Ghazi, “Wireless Sensor Network: Security challenges”, IEEE National Days of Network Security and Systems (JNS2) 2012.
2. M . Guechari, L. Mokdad, S. Tan, “Dynamic solution for detecting Denial of Service attacks in wireless sensor networks”, IEEE International Conference on Communications (ICC) 2012.
3. Weerasinghe H, Fu H (2007) Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation. Paper presented at the Future Generation Communication and Networking, Jeju-Island, Korea, 6-8 December 2007

4. Peter Schaffer, Karoly Farkas, Adam Horvath, Tamas Holczer, Levente Buttyan, "Survey Secure and reliable clustering in wireless sensor networks: A critical survey", ACM, Computer Networks: The International Journal of Computer and Telecommunications Networking, July, 2012.
5. Satyajayant Misra, Kabi Bhattarai, Guoliang Xue, "BAMBi: Blackhole Attacks Mitigation with Multiple Base Stations in Wireless Sensor Networks", IEEE International Conference on Communications (ICC) 2011.
6. Ahmed R. Mahmood , Hussein H. Aly , Mohamed N. El-Derini, "Defending Against Energy Efficient Link Layer Jamming Denial of Service Attack in Wireless Sensor Networks", IEEE 9th IEEE/ACS International Conference on Computer Systems and Applications (AICCSA) 2011.
7. R. Nanda, P. Venkata Krishna, "A self-enforcing and flexible security protocol for preventing Denial of Service attacks in wireless sensor networks", IEEE Recent Advances in Intelligent Computational Systems (RAICS) 2011.
8. Hero Modares, Rosli Salleh, Amirhossein Moravejosharieh," Overview of Security Issues in Wireless Sensor Networks", ACM 3rd International Conference on Computational Intelligence, Modelling & Simulation (CIMSIM '11), 2011.
9. Anoosha Prathapani , Lakshmi Santhananr , Dharma P. Agrawal, "Intelligent Honeypot Agent for Blackhole Attack Detection in Wireless Mesh Networks", IEEE 6th International Conference on Mobile Adhoc and Sensor System (MASS) 2009.