"An Opinion Trust Based Detection and Prevention Method for Defending Black-hole and Gray-hole Attacks in Wireless Sensor Networks"

Mitali Khandelwal[1], Sachin Upadhyay[2]

PG Scholar, Computer Science Engineering, Alpine Institute of Technology, Ujjain, India [1]
Assistant Professor, Computer Science Engineering, Alpine Institute of Technology, Ujjain, India [2]

***Abstract* - In a Wireless Sensor Network (WSN), Security is a key challenge due to its dynamic topology, open wireless medium, lack of centralized infrastructure, intermittent connectivity, resource constrained sensor nodes. The security of a wireless sensor network is compromised because of the random deployment of sensor nodes in open environment, memory limitations, power limitations and unattended nature. These weak entities make WSN easily mutual aid by an adversary to device abundant attacks resulting in disastrous consequences. Black Hole and Gray-hole attacks are of them wherein it exploits a trustworthiness of a network by promising routing of data packets to the destination knowing that it has a shortest path but in reality it drops all packets as well as selectively drops the packets, and consequently threatens reliability. In order to accomplish secure packet transmission, an efficient and opinion trust based secure protocol is proposed to defend against Gray-hole and Black Hole attacks. The Simulation results signify that the proposed protocol performs satisfactorily in secure routing and is strong against both Gray-hole and Black Hole attacks in a dynamic environment.**

Keywords: ***Wireless Sensor Network, AODV, RREQ, RREP, NS2, Black-hole, Gray-hole***

1. Introduction

Wireless Sensor Network consists of a large number of small and low cost sensor nodes which are randomly deployed in an area. The sensor nodes have computational capability to carry out simple computations and transmit the required information [1]. These nodes transmit information to the sink node that aggregates the entire information received from other nodes and generates a summary data to be transmitted to another network. These sensor nodes can collectively monitor physical and environmental conditions like pressure, temperature, humidity and sound vibrations. Such features ensure a wide range of applications for wireless sensor network such as military, medical, industrial, disaster relief operations, environmental monitoring, traffic surveillance, agriculture, infrastructure monitoring [1, 2]. Since the majority of sensor nodes are deployed in hostile environment, they are susceptible to various attacks that are caused by malicious or compromised nodes in the network. The malicious nodes can alter the normal behavior of the network, tamper with the node's hardware and software, transmit false information, or drop the required information. Hence, security of wireless sensor network becomes a critical issue.

1.1 Major Design Challenges

WSNs have many constraints from which new challenges stand out. The extreme resource limitations of sensor nodes and unreliable communication medium in unattended environments make it very difficult to directly employ the existing security approaches on a sensor platform due to the complexity of the algorithms [3] [4] [5] [6]. Indeed, the understanding of these challenges within WSNs provides a basis for further works on sensor networks security.

1.1.1 Very Limited Resources

WSNs pose unique challenges because of the strict resource constraints on each individual sensor. Embedded devices with very limited resource must implement complex, distributed, ad-hoc networking protocols. Size reduction of sensor nodes is essential to cut costs and create more applications. As physical size decreases, so does energy capacity. The underlying energy constraints end up creating computational and storage limitations that lead to a new set of design issues. For example, Zigbex sensor type HBE has an 8-bit, 7.372 MHz ATmega128L RISC MCU with only 4 Kb SRAM, 128 Kb flash memories and 512 Kb flash storage [5]. With such limitations, the software built for the sensor must also be quite small.

1.1.2 Unreliable Communication

Due to the wireless medium that is inherently broadcast in nature, packets may get damaged due to channel errors and conflict will occur, or dropped at highly congested nodes in the network. As well, an attacker can launch Denial-of-Service (DoS) attacks without much effort, etc. Furthermore,

the multi-hop routing, network congestion and node processing can lead to greater latency in the network, thus making it difficult to achieve synchronization among sensor nodes. The synchronization issues can be critical to sensor security where the security mechanism relies on critical event reports and cryptographic key distribution.

1.1.3 Unattended Operations

Sensors nodes interact closely with their physical environments, process and fuse data, and eventually create new knowledge that must be presented to an end-user. These tiny nodes are often deployed in open, large-scale and even hostile areas. Potential issues range from accidental node failure to physical capture. Getting secure data in harsh environment from physical wireless sensors to an end-user is not a simple task due to these severe constraints.

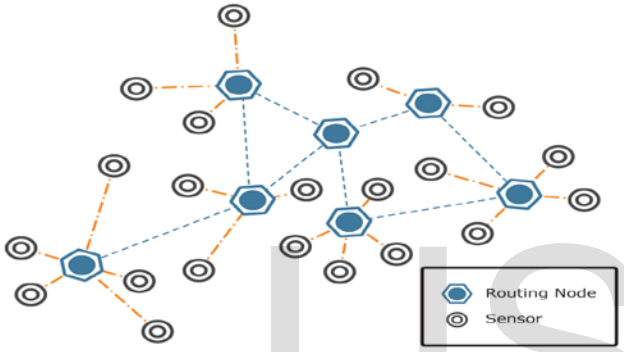


Figure 1 Wireless Sensor Networks [7]

A wireless sensor network consists of many tiny sensor nodes, each equipped with a radio transceiver, a microprocessor and a number of sensors. These nodes are capable of independently forming a network through which sensor readings can be propagated. Each node has an autonomous processing capacity; data can be processed as they pass through the network [7].

The remainder of paper is organized as follows. Section 2 describes related work and Section 3 is short note about Gray hole and Black hole Attack. In Section 4, proposed scheme is discussed for making WSN free from the malicious attack. Implementation of the proposed scheme is covered in Section 5 and Result Section is 6. Finally conclusion and future directions are given in Section 7.

2. Literature Survey

Numerous Researchers have worked on multiple detection and prevention of wormhole attacks in wireless sensor network, based on the detection mechanism, the existing techniques of detecting and preventing wormhole attacks can be illustrate in this section.

Patel and Dadhaniya [8] proposed a 3-step host based Intrusion detection technique in which each node acted as IDS node. It detects a malicious node based on sequence number generated by it. If sequence number generated by replying node is greater than the sequence number generated by source node, then the replying node is considered as malicious node and the messages sent by it are also blocked, by transmitting node id to all other nodes. The simulation results of the paper showed that there was an increase in PDR and average throughput.

Deng et al. [9] presented a solution for solving problem of Black Hole Attack. In this technique, along with the RREP message, information regarding the neighbor of replying node is also asked and when RREP message reaches source, source instead of sending message immediately sends another message to neighbor of replying node asking whether the intermediate node which is replying for RREQ message really has path to destination or not. But it had limitation that it increased the message overhead so it can be used to verify identity of node which is under doubt of being malicious and it also assumed that Black hole nodes cannot work in group.

Raj and Swadas [10] proposed a method DPRAODV to detect black hole node based on RREP sequence number and threshold value. If the value of RREP sequence number comes out to be greater than the threshold value then the node sending this RREP will be considered as malicious. Further this malicious node is isolated from network by sending a control message ALARM to all other nodes and a list of blacklisted nodes is created. The simulation results showed that there was an increase in packet delivery ratio but also an increase in routing overhead and delay in message delivery.

Mistry et al. [11] did a modification in working of source node by the addition of new function for storing RREP messages for some specified time, a table which stores these RREP messages, a timer and Malicious node id for detecting black hole node and to keep record of all malicious nodes present in network. This technique discards the RREP message stored in table which has highest value of destination sequence number and node sending this RREP will be considered as malicious and its identity will be stored as malicious id. This method leads to an increase in memory and time overhead but increase in packet delivery ratio compensated for that overhead.

Guori Li [12] with his colleagues uses sequential mesh test based scheme. The Cluster head node detects the nasty node based on the sequential mesh test method after receiving the report from the nodes. In the scheme it extracts small samples from the networking nodes instead of doing test on whole network in advance. In the sequential mesh test method, the test decides whether to continue the test or to hold after final conclusion.

Xin with his colleagues [13] uses light weight defense schemes for the detection of Gray Hole attack. He uses the neighbor node as monitoring nodes and resends the dropped packets again to the nodes associated with that node.

Brown and Xiaojiang [14] uses heterogeneous sensor network (HSN) for detection of selective forwarding attack. In the

HSN model consist of high end large Sensor Node (H-Sensors) and Low end (L-Sensors). After deployment of all Sensor nodes, a cluster formation takes place with H-Sensors as Cluster Head.

Sophia Kaplantzis [15] uses centralized intrusion detection system based technique on SVM (Support Vector Machines), and sliding windows. Here Sophia uses the intrusion detection at the Sink Node, so the energy of nodes is also saved. She proposed that this is the best method for detecting the Gray Hole attack without utilizing the energy of the sensing node.

3. Black-hole and Gray-hole Attacks

3.1 Black-hole Attack

Black hole attack is a routing layer attack in which data is revolves from other node. The transmission of packets on multiple nodes and dropping of packets is mostly occurring on routing layer. Routing protocol is targeted by the attack. The busy DOS attack is black hole attack. Black hole attack is difficult to detect; it is mostly found in temporary networks like virtual/wireless mesh networks [16].

In black hole attack, the sender node receive reply message from fault node and make smallest way to receiver node. Fault node sends reply message after authorized node to sender node and then sender become confuse in two replies. On that way, Fault node become sender node and whole data received by it. In this, the data packets fully dropped by sender node.

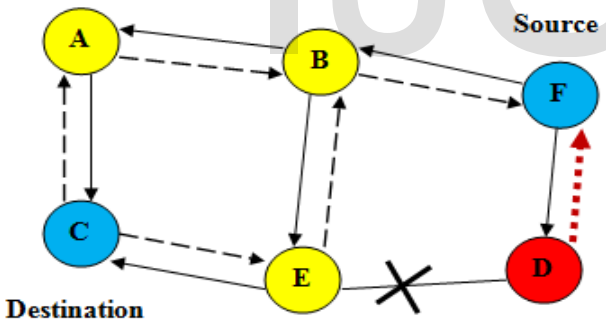


Figure 2 Black hole Attacks

In Black whole attack, using routing protocol to an attacker promotes itself as the shortest path to the objective device [17]. An attacker watches the routes appeal in an overflow based routing protocol. When the attacker receives an application for a route to the purpose node, it forms a reply for connecting of actually short route. If the naughty respond reaches to the initial node, previous to the reply from the authentic node, a false route gets formed. Once the malicious device joins the network itself among the converse nodes, it is forceful to do the whole thing during the packets passing through them. It can crash the packets between them to implement a denial-of-service attack, or on the beforehand use its situation over the route is the first step of man-in-the-middle attack [18].

3.2 Gray-hole Attack

Gray hole is a node that can switch from behaving correctly to behaving like a black hole that is it is actually an attacker and it will act as a normal node. So we can't identify easily the attacker since it behaves as a normal node. Every node maintains a routing table that stores the next hop node information which is a route packet to destination node [19]. If a source node is in need to route a packet to the destination node it uses a specific route and it will be checked in the routing table whether it is available or not. If a node initiates a route discovery process by broadcasting Route Request (RREQ) message to its neighbor, by receiving the route request message the intermediate nodes will update their routing tables for reverse route to the source [20]. A route reply message is sent back to the source node when the RREQ query reaches either to the destination node or to any other node which has a current route to destination.

The gray-hole attack has two phases:

Phase 1: A malicious node exploits the AODV protocol to advertise itself as having a valid route to destination node, with the intention of interrupting packets of spurious route.

Phase 2: In this phase, the nodes has been dropped the interrupted packets with a certain probability and the detection of gray-hole attack is a difficult process. Normally in the gray-hole attacks the attacker behaves maliciously for the time until the packets are dropped and then switch to their normal behavior [21]. Both normal node and attacker are same. Due to this behavior it is very hard to find out in the network to figure out such kind of attack. The other name for Gray-hole attack is node misbehaving attack.

4. Proposed System

The proposed work is intended to find an adoptable security algorithm formulation by which the wireless sensor network becomes secure.

4.1 Methodology

The proposed security model is a trust based security framework and promises to provide a secure communication model. Therefore the following security solution is required to implement.

1. To provide efficiency during the route discovery this process is taken place
2. Obtain some essential network parameters that help to design the attribute based rules to improve the performance during the attack.
3. Design of a opinion based trust based Model that helps to identify the Black-hole and Gray-hole attacks in networks

4.2 Proposed Algorithm

Table 1 Proposed Algorithm for Attacks Prevention

Algorithm for Black-hole and Gray-hole Attack

1: Initialize the Network, with N nodes where $N = 1, 2, 3, \ldots\ldots$,, in ideal condition.

2: Initialize Route Discovery by Source Node N_s

3: N_s sends RREQ Packets to Destination N_d

4: Wait Until all Route Replies not received

5: Calculate Packet Delivery Ratio

$$Packet\ Delivery\ Ratio = \frac{Total\ Delivered\ Packet}{Total\ Sent\ Packet}$$

6: Calculate Average PDR Value for each Node

$$\emptyset_{PDR} = \frac{1}{N}\sum_{i=1}^{N} PDR\ i$$

7: $\boldsymbol{If}(Current\_Node\_\emptyset_{PDR} < 30\%)$ {

$trusty_{node}[i] = trusty_{node} - 1$

}

8: ***else***

{

$trusty_{node}[i] = trusty_{node} + 1$

}

9: $\boldsymbol{if}$ $(Reply\_node\_sequence\_same)$ {

$trusty_{node}[i] = trusty_{node} - 1$

}

10: ***else***

{

$trusty_{node}[i] = trusty_{node} + 1$

}

11: $\boldsymbol{if}(trusty_{node} < 0)$ {

This node is not good set as Malicious

$my\_opinio\_for\_node = 0$

}

12: ***else***

{

This is Normal Node

$my\_opinio\_for\_node = 1$

}

13: ***end process***

Description: For detecting the packet dropping attack we used opinion based technique who first find out its neighbor's reply or any destination for a sample time, and store the sequence number as along with the destination number and the neighbor IP also neighbor's node find out the Packet Delivery Ratio (PDR) of each node .In starting time (0.0) all nodes having same trust which is 0 , for making own decision the current node will compare the PDR of its neighbor node and assign to the node. If the current node receiving the reply with the same sequence but the destination not same, so that may be a malicious reply so again down the trust for that node.

Now to make the final decision for that node by the node, will depend on trustworthiness of node for communication with any nodes. The current node will ask for its all neighbor node for their own opinion and include their own opinion and make final decision select or not as next hop . and final decision make by counting number of grater opinion if he find more 1 in opinion make as trusted node and safe for working and if find more 0's the mark as malicious find some other next hop if the count is same than we will processed for this node as safe.

5. Implementation

The simulation is being implemented in the Network simulator [22]. Protocol used here is AODV.

Table 2 Simulation Scenarios

Parameters	*Values*
Antenna Model	Omni Antenna
Dimension	1000 X 1000
Radio-Propagation	Two Ray Ground
Channel Type	Wireless Channel
Traffic Model	CBR
Routing Protocol	AODV
Mobility Model	Random Waypoint

5.1 For Black-hole Attack

Simulation using Proposed Routing Method: In this phase, of proposed secure routing method is simulated when attack prevention is established. Therefore the second simulation is prepared which is demonstrated in figure 3. In this simulation screen the green nodes demonstrate as normal legitimate node in network. The given simulation is developed using the

IJSER

proposed secure routing technique. When the proposed method is deployed network performance is improve and large number of packet is delivered to the destination. Communication is happened between source node 9 and destination node 18.

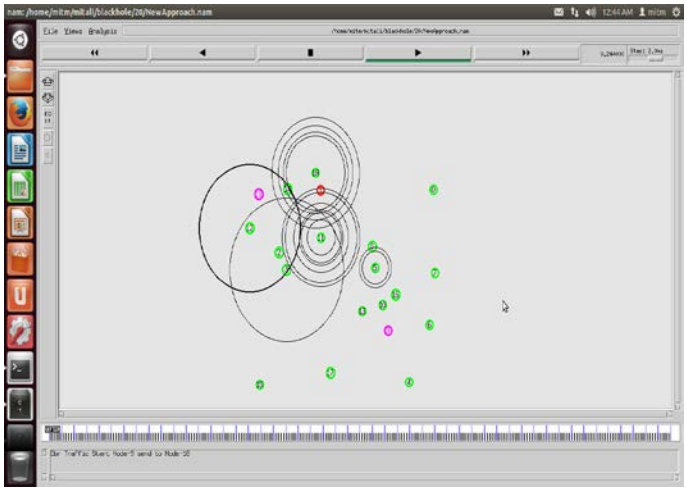


Figure 3 Proposed Routing under Black hole Attack Prevention

5.2 For Gray-hole Attack

Simulation using the Proposed Secure Routing Technique: In this simulation scenario the proposed routing technique which is developed with the help of AODV routing modifications are implemented with the Wireless Sensor Network. Additionally a similar kind of attacker node on the network is deployed. The deployed attacker is normalized using the technique and their performance is estimated on the basis of the network trace files. Additionally the measured performance is compared with the traditional AODV performance under attack conditions. The figure 4 demonstrates the simulation screen of the proposed secure routing technique for Gray-hole Attack prevention.

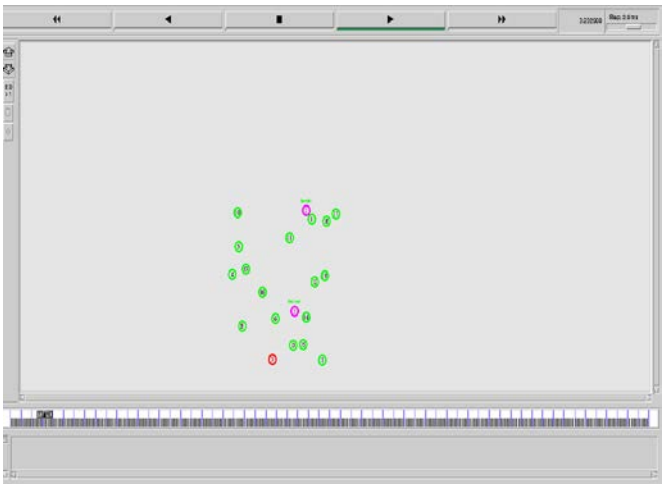


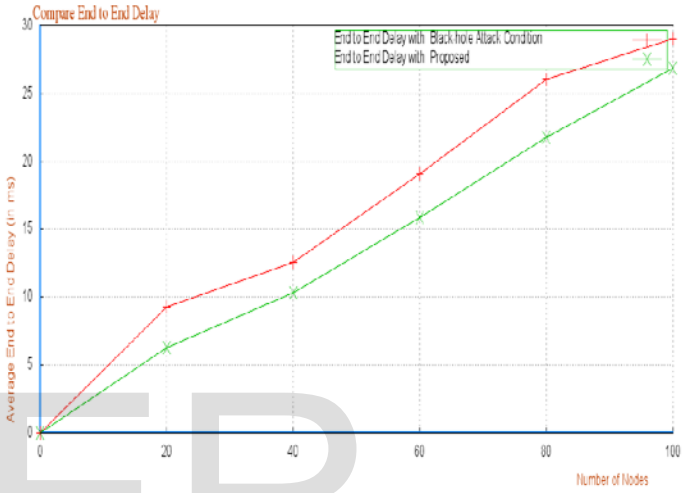
Figure 4 Proposed Method under Gray-hole attack Prevention

6. Result Analysis

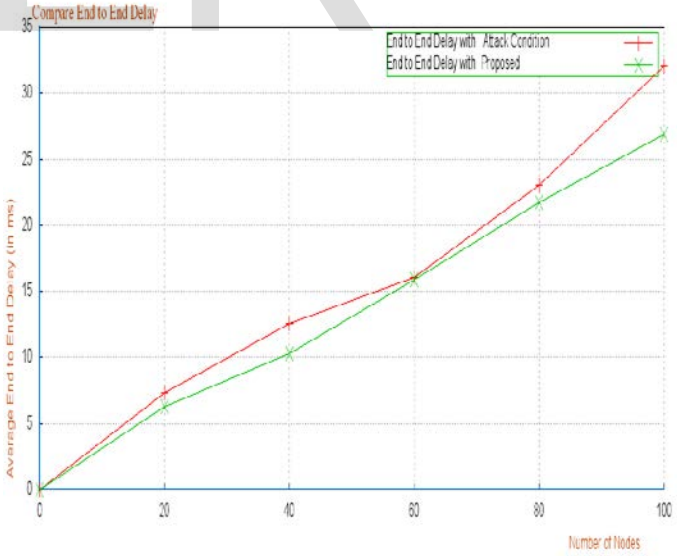
6.1 End to End delay

End to end day on network refers to the time taken, for a packet to be transmitted across a network from source to destination device, this delay is calculated using the below given formula.

$$E2E\ Delay = Receiving\ Time - Sending\ Time$$



Graph 1 End to End Delay or Black-hole



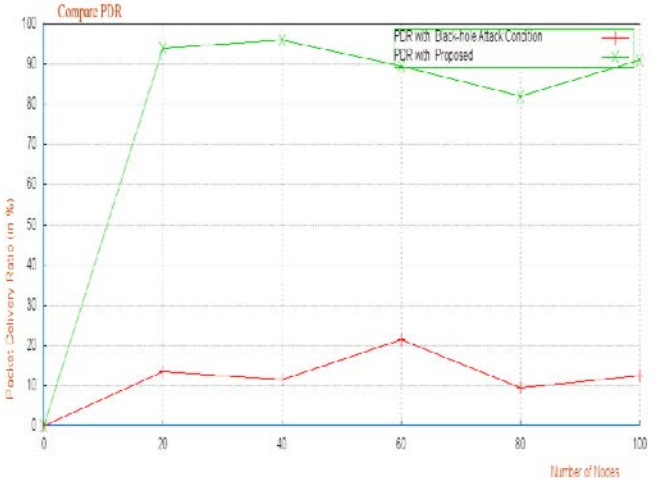
Graph 2 End to End Delay for Gray-hole Attack

6.2 Packet Delivery Ratio

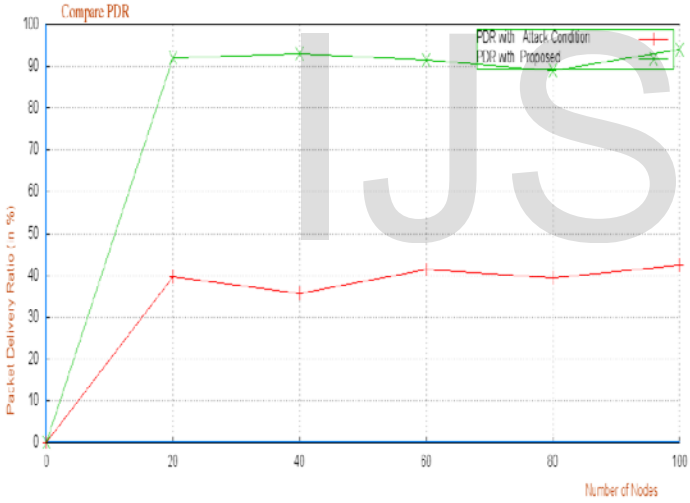
The performance parameter Packet delivery ratio sometimes termed as the PDR ratio provides information about the performance of any routing protocols by the successfully

delivered packets to the destination, where PDR can be estimated using the formula given:

$$Packet\ Delivery\ Ratio = \frac{Total\ Delivered\ Packets}{Total\ Sent\ Packets}$$



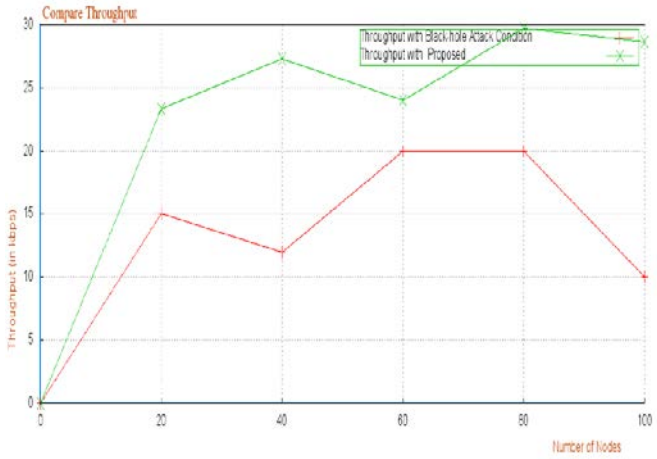
Graph 3 Packet Delivery Ratio for Black-hole



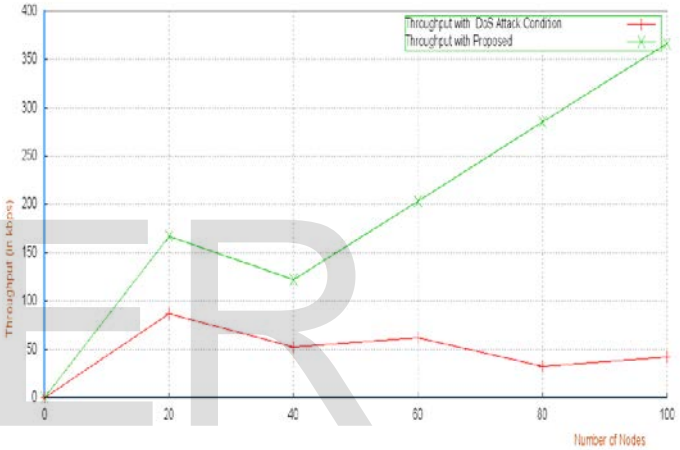
Graph 4 Compare Packet Delivery Ratios for Gray-hole

6.3 Throughput

Network throughput is the average rate of successful message delivery over a communication channel. This data may be delivered over a physical or logical link, or pass through a certain network node. The throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second or data packets per time slot.



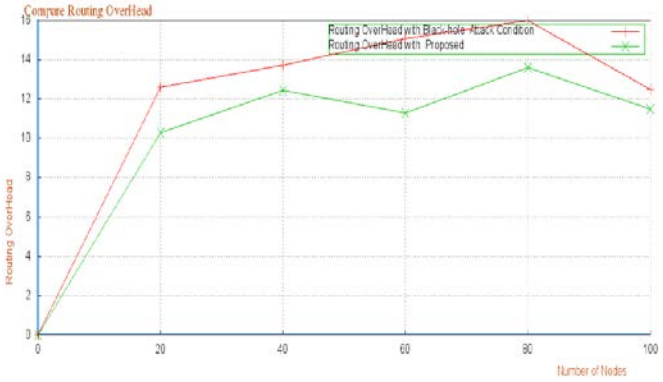
Graph 5 Throughput for Black-hole Attack



Graph 6 Throughputs under Gray-hole Attack

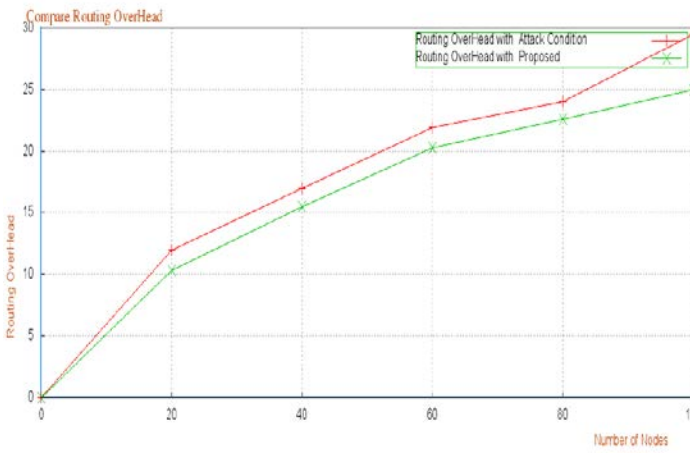
6.4 Routing Overhead

During the communication scenarios it is required to exchange the packets for different tracking and monitoring purpose. Therefore the additional injected packets in network is termed as the routing overhead of the network



Graph 7 Routing Overhead for Black-hole

IJSER



Graph 8 Compare Routing Overhead for Gray-hole Attack

7. Conclusion and Future Work

The Misbehavior of nodes have been caused severe damage and the whole network has been attacked in the network layer which is a Gray hole and Black hole attack in WSNs. Security is the most important feature for deployment in WSNs. As we seen and study different methods are proposed from different researchers, but all having drawbacks. Also sometimes happens that due to obstruction of the network false attacks came into existence. In the proposed technique, we have tried to give the better utilization of bandwidth, good packet delivery ratio and less end to end delay, network throughput which help us and also to new researchers to design networks which counter this type of attacks.

In near future the work is enhanced more with adding more parameters to distinguish more or different kinds of network attacks. The solution is based on Node Trust so untrustworthy behavior of the network can be analyzed by using parameter enhancement. The whole research work can be extended in the future in other protocol rather than AODV.

References

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless sensor networks: A survey, Computer Networks”, pp. 393- 422, 2000.

[2] A.S.K. Pathan, H.W. Lee, C.S. Hong, “Security in Wireless Sensor Networks: Issues and Challenges”, Communications, IEEE Transaction, Feb 2006.

[3] E.Shi and A.Perrig, “Designing Secure Sensor Networks”, Wireless Communication Mag., Vol. 11, No. 6, pp.38-43, Dec 2004.

[4] Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Sean Hong, “Security in Wireless Sensor Networks: Issues and Challenges”, Proc. ICACT 2006, Volume 1, 20-22, pp. 1043-1048, Feb. 2006.

[5] Dr. G. Padmavathi, Mrs. D. Shanmugapriya, “A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks”, International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2, 2009.

[6] Shahnaz Saleem, Sana Ullah, Hyeong Seon Yoo, “on the Security Issues in Wireless Body Area Networks”, International Journal of Digital Content Technology and its Applications Vol. 3, No. 3, Sep. 2009

[7] “RELATED TECHNOLOGIES”, available online: http://www.purelink.ca/en/technologies/related-technologies.php

[8] N. Patel, A. Dadhaniya, "Detection of Black Hole Attack in MANET using Intrusion Detection System", International Journal of Advance Engineering and Research Development (IJAERD, Volume 1, Issue 5,May 2014.

[9] H. Deng, W. Li, and D.P. Agrawal, “Routing Security in Wireless Ad Hoc Network”, IEEE Communications Magazines, vol. 40, no. 10, October 2002.

[10] P.N. Raj, P.B. Swadas, “DPRAODV: A Dynamic Learning System against Black Hole Attack in AODV Based MANET”, IJCSI International Journal of Computer Science Issues, Vol. 2, pp 54-59 2009.

[11] N. Mistry, D.C. Jinwala, M. Zaveri, ”Improving AODV Protocol against Black hole Attacks”, in Proc. of the International Multi Conference of Engineer and Computer Science, Vol. 2, 2010.

[12] Gouri Li, Xiangdong Liu and Wang″ A Sequential Mesh Based Test based Selective Forwarding attack, detection schemes in wireless Sensor Nrtworks".

[13] Wang Xin-Sheng, Zhan Yong-Zhao, Xiang Shu-ming and Wang Liangmin, ″Lightweight defense scheme against selective forwarding attack in Wireless Sensor Networks" pg 226-232. Oct 2009.

[14] Jeremy Brown and Xiaojiang Du.″ Detection of Selective Forwarding Attack in Heterogeneous Network", In ICC pg 1583-1587, 2008.

[15] Sophia Kaplantzis, Alistair Shilton, Nallasamy mani, Y.Ahmad, Ekesnio Glu ″Detecting Selective Forwarding attack By using SVM. Intelligent Sensor Networks and Information’s, 3rd International Conference, pg 333-340.

[16] Rupinder Kaur and Parminder Singh, “REVIEW OF BLACK HOLE AND GREY HOLE ATTACK”, the International Journal of Multimedia & Its Applications (IJMA) Vol.6, No.6, December 2014.

[17] Fan-Hsun Tseng1, and Han-Chieh Chao, “A survey of black hole attacks in wireless mobile ad hoc networks”, Tseng et al. Human-centric Computing and Information Sciences 2011.

[18] Neetika Bhardwaj, Rajdeep Singh, “Detection and Avoidance of Black-hole Attack in AOMDV Protocol in MANETs”, International Journal of Application or Innovation in Engineering & Management (IJAIEM), PP. 376 – 383, Volume 3, Issue 5, May 2014.

[19] Vishnu K and Amos J Paul "Detection and removal of Cooperative Black/Gray hole attack in Mobile Ad-hoc Networks" IJCA Vol.1, No.22 Jan 2010.

[20] Megha Arya and Yogendra Kumar Jain, "Gary-hole attack and prevention in Mobile Ad-hoc Network" (IJCA), Volume 27, Number 10, Aug 2011

[21] Onkar V .Chandure, Prof V. T. Gaikwad " A Mechanism for recognition & Eradication of Gray Hole attack using AODV Routing Protocol in MANET" IJCSIT , Vol.2, No.6, Jul 2011.

[22] The Network Simulator. NS-2 [Online] http://www.isi.edu/nsnam/ns/

IJSER