An Approach to Locate Nasty Node and to Prevent Selective Dropping in WSN

Dharmendra Mishra
Oriental University, Indore

Sunil Patel
Oriental University, Indore

ABSTRACT
The fast growth in wireless communication and digital electronics has led to the development of low-cost and low-power sensor nodes that are small in size and may communicate over short distances. Sensor nodes are deployed in hostile environment in large number, which makes their physical protection against tampering difficult or more prone to be compromised by an adversary force. By doing that, an adversary can modify the behavior of the compromised nodes and launch routing misbehavior attacks. One most common type of such attacks is gray hole attack. Adhoc On Demand Distance Vector (AODV) in its pure form does not have any mechanism to deal with such type of attack. In this paper, we simulate gray hole attack on AODV routing protocol and evaluate AODV's performance by considering different metrics and scenarios. NS2 simulator has been used to conduct simulation of gray hole attack. Our simulation results show the influence of gray hole attack on the performance of AODV which suffers from decreased delivery ratio and increased packet loss. Furthermore, some countermeasures against gray hole attack are also provided.

Keywords
Wireless Sensor Networks, Security, and Gray Hole Attack/Selective Forwarding Attack, AODV, NS-2

1. INTRODUCTION
The AODV routing protocol is a popular reactive routing protocol in wireless networks, but AODV routing protocol designed for better performance of the network not for security of node, secure protocols are generally designed to have features such as authentication, integrity, confidentiality and non-repudiation. For security purpose AODV have vulnerabilities and it is easily manipulate by malicious node to destroy its network routing. The open nature of wireless medium also makes it easy for outsider attackers to interfere and interrupt the legitimate traffic. This concept classifies the attacks into two broad categories, namely Passive and Active attacks. In Passive attack, the adversary only eavesdrop upon the packets content, while packets may get dropped or altered on way in case of Active attacks. One of the widely known attacks is the Gray Hole Attack. It is the variation of Black-hole attack. Black- hole attack is one of the security threat in which the traffic is redirected to such a node that actually does not exist in the network and that node drops the entire packet. But in Gray-Hole attack, nodes will drop the packets selectively. The complete study observes that, AODV is a insecure routing protocol and does not incorporate any mechanism to detect and prevent communication from malicious affect.

The main purposes are following as:

1. Analyze and simulate the AODV protocol in WSN.
2. Analyze and simulate the impact of Gray-hole attack on AODV in detail for various scenarios.
3. Propose a technique for detection of malicious node under Gray-hole attack in AODV.
4. Propose a technique for prevention of malicious node under Gray-hole attack in AODV and analyze its performance.
5. Simulate and analyze its performance of modified AODV and compare with the normal AODV.

In short, major concern with AODV is:-

Insecure Routing, Packet Dropping, Security

2. LITERATURE SURVEY
Preeti Sharma et al. [1] presented a simulation study of a wireless sensor network to analyze the effects of selective forwarding attacks. The scenarios considered are no attack and attacks on nodes. The simulation tool OPNET 14.5 is used effectively for detailed analysis. The scenarios considered are mainly taken from the literature. The Simulation results show that the impact of selective forwarding attacks on performance of WSN can become quite significant. In case there is an attack the performance degradation is more severe. From this analysis we can conclude that packet dropping due to some network errors and selective forwarding attacks are affecting the network to different extent.

Aproova Joshi et al. [2] performance of LEACH protocol is evaluated with Selective Forwarding Attack using Network Simulator-2 by the Authors. It is observed that how Packet Delivery is affected, when number of malicious nodes increases. It is clear from the number of malicious nodes vs Packet Delivery Ratio graph that as number of malicious nodes increases packet delivery ratio decreases.

K. Ioannis and T. Dimitriou [3] defined a Distributed Intrusion Detection Scheme (IDS) for sensor networks based on watchdogs for selective forwarding and sinkhole attacks. They have adopted specification based rules and cooperative decision making techniques to create IDS with low false positives and false negative alarms. Neighbor monitoring is used for detecting selective forwarding attack in sensor networks. Watchdog approach is used by neighboring nodes which can easily monitor the behavior of a node to see whether it forwards correctly the packets it receives. By adopting specification-based approach, they define which norms are going to be used to describe normal operation. These specifications for detecting black-hole and selective forwarding attacks can simply be a rule on the number of messages being dropped by a node. Each of the watchdog nodes will apply that rule for itself to produce an intrusion alert. The naive approach would be to increment a counter every time a packet is dropped and produce an alert when this value reaches a threshold.

B. Lee et al. [4] have proposed a resilient packet-forwarding scheme using Neighbor Watch System (NWS) against maliciously packet-dropping nodes in sensor networks. This

scheme basically employs single-path data forwarding, which consumes less power than multi-path schemes. The packet is forwarded along the single-path towards the base station; however, the scheme uses multi-path data forwarding at the location where NWS detects relaying nodes' misbehavior. The watch node around a malicious node can find that after receiving, the malicious node do not transmit to other nodes or transmit to a node that does not exist in its neighbor list, and then the watch node must retransmit the package.

Wazir Zada Khan et al. [5] explained the systematic analyses of the Selective Forwarding attack and its all existing defenses in sensor networks. The main objective of this research paper is to give an overview for all those researchers and developers who used to propose different techniques to counter Selective Forwarding attack. The developers may make this paper a source when developing techniques for detecting and defending against selective forwarding attack as this paper covers all the drawbacks of existing countermeasures for selective forwarding attack.

S.Sharmila & G. Umamaheshwari [6] mentions that malicious node is detected based on the acknowledgement and energy level of the node.From the simulations, byte overhead is 0.39 percentages and detection accuracy is 80% are observed and thus increasing the network throughput. These results show that the packets can be forwarded without any selective packet drop by minimizing the malicious nodes in the network. The further enhancement of the proposed scheme is to improve the success rate to 100% with various mobility and receiver sensitivity of the node.

Literature survey is given in tabular form in below Table 1.

In the table I have given the brief result of different research done on Selective forwarding attack.

Table 2 Comparative Study of Gray Hole Attack Approach

Technique	Nodes	Simulator Protocol	Attack Scenario Result	Result after attack Prevention
1.Node location[1] Topology table of network is used to obtain physical location of node	30	OPENET	**Throughput** 7 Kbps **Packet Dropped** 50.0	**Throughput** 70 Kbps **Packet Dropped** 7.0
2. Leach Protocol [2] In the method the detection of malicious node is done by calculating packet dropping by cluster head.	100	NS-2 LEACH	**Packet Delivery** 0.95 **Throughput** Not Taken in parameter	**Packet Delivery** 0.98 **Throughput** Not Taken in parameter
3.Local Monitoring Technique [4] In this proposed method local monitoring technique is used to defense Gray Hole Attack	06	NS-2 AODV	**Packet Delivery Ratio** **0.46** **Throughput** Not Taken in parameter	**Packet Delivery Ratio** **0.95** **Throughput** Not Taken in parameter
4.Performance of AODV Gray Hole Attack [5] Influence of Gray Hole attack on performance of AODV	10 20 30	NS-2 AODV -	**Packet Delivery** 10 Node-31 20 Node-21 30 Node-10 **Packet Drop** 10 Node-69 20 Node-79 30 Node-90 **Throughput** Not Taken in parameter	**Packet Delivery** Not Taken in parameter **Packet Drop** Not Taken in parameter **Throughput** Not Taken in parameter

Throughput in Kbps

3. OBJECTIVES

1. Simulate WSN topology & Scenarios in NS-2 environment.
2. Simulate vulnerable WSN with possibility of Gray-hole attack.
3. Implement the AODV routing protocol with proposed preventive strategy.
4. Compare and observed the performance of Normal AODV & modified AODV.

The purpose of this study is to detect Gray-hole attack in the WSN. Application of WSN such as military battle field is used to transmit the confidential data via wireless medium. Wireless Sensor Network is also used in national security applications such as monitoring and tracking the borders, nuclear attacks detection etc. The data in WSN applications is very important and due to the hostile environment of applications, Wireless Sensor Network needs security mechanism.

4. METHODOLOGY

1. The work for the research starts with studying the theoretical aspects of the AODV routing protocol.
2. AODV routing protocol is then implemented in ns2 on different scenarios.
3. Performance evaluation of AODV protocol under normal is done.
4. Theoretical aspects of security issues and their impacts on routing are studied**.**
5. Simulation of AODV under various attacks is done to analyze the impact on performance metrics when malicious nodes are inserted in the network scenario.
6. Analyze the impact of Gray-hole attack on various performance metrics for AODV.
7. Implement the proposed technique in AODV for detection and prevention of Gray-hole attack.
8. Analyze the performance metrics for modified AODV under Gray-hole attack.
9. Compare the performance parameters for AODV under normal condition, Gray-hole attack and Preventive Gray-hole attack.

In short, following steps have been taken to detect and prevent Gray-hole attack.
Creation of normal node scenario
Deployment of Gray-hole Attack
Deployment of IDS mechanism to detect and prevent Gray-hole attack.

5. SOLUTION DOMAIN

One of the objectives of this thesis work is to reduce the effects of Gray-hole attack on the performance of on demand reactive routing protocol, AODV. Gray-hole attack adversely affects the performance of AODV routing protocol. An adaptive technique is presented in the research work which is based on the on demand AODV routing protocol. The basic idea behind the proposed technique is based on Intrusion Detection System.

In the proposed work, every AODV node executes an IDS mechanism, i.e. each node in the network has an IDS agent in-built in the form of module with AODV routing protocol. IDS module estimates the suspicious value called count of a node according to the numbers of RREQ and RREP packets transmitted or forwarded from the node. When a suspicious value for a neighboring node exceeds a threshold, then that node is isolated from the network as other nodes do not forward packets through the suspected malicious node.

6. PROPOSED ALGORITHM

In this section the proposed mechanism for defending against Gray- hole attack is presented. The mechanism modifies the AODV protocol by introducing three concepts,

1. Broadcast RREP packet,
2. Data Routing Information, count
3. Reliability checking of a route

Broadcast RREP packet

This paper proposes the intrusion detection for AODV by verifying the RREP packets. The RREP packets are normally unicast to the source node by any intermediate node having the route to the destination. In order to detect Gray-hole attack, RREP packets are monitored. In the proposed modification of AODV routing protocol the RREP sent by intermediate nodes or the destination node is broadcasted. Broadcasting of the RREP packet is helpful for other nodes in the network so they can maintain a list of RREP packets and collect the routing information about the usability and trust of routes.

Data Routing Information

In the proposed scheme, each and every node maintains a broadcast route-reply list. Each node also maintains an additional data routing information (DRI) field, count corresponding to each route-reply entry in broadcast RREP list. Value of count is incremented whenever a node receives a RREP packet from its neighbor node except for first time, when the route in entered in the route-reply list.

Reliability Checking of a Route

The proposed scheme relies on reliable nodes (nodes through which source has routed data previously and knows them to be trustworthy) to transfer data packets. In the modification the source node broadcasts a RREQ message to discover a reliable route to the destination. The intermediate node that generates the reply broadcasts the RREP packet. Upon receiving the RREP message from the intermediate node other nodes along with the source node check their own route reply list to see whether the RREP is a trustful route or not. If the node has received this route in RREP packet earlier through some other node before, then this RREP is trustful. If this route reply exists in the list then its corresponding count is incremented and it starts routing data through this route but if the route corresponding to the RREP is not available in route-reply list, then the route is not trusted and a new entry corresponding to the RREP received is made in its RREP LIST with count zero.

BEGIN

Setting Parameters -

Set Channel – Wireless

Set Link – Mac/802_15_4

Set Queue Length – 50

Set Packet Length – 512 Bytes

Set Traffic Pattern – CBR

Set Transport Agent – UDP

Set Nodes – 100/500/1000

Set Duration – 100 Sec/200 Sec/1500 Sec

Gray Node Deployment -

Broadcast RREQ in network

Receive Acknowledgement

Update Routing table with neighbour IDs, Dropping selective packets from front or tail in queue

Mechanism to detect Nasty Node Intrusion -

Broadcast RREQ to All Neighbours, Wait for Reply Acknowledgement

Create route reply list;

Set count == -1;

first received packet count discarded due for rtable creation;

Create list()

{

Set neighbour id == received id;

Set count == packet.RREP;

}

RREP Packet use to create list {} with RREP count and associate id of RREP Sender;

if (Receive packet type == RREP)

count ++;

Increment count value when receive RREP packet;

Reliability Checking of a Route;

If (count > 0)

{

Check route reply exist in table;

If (rrep.route == rtable.route)

If RREP route is existed than route is trustful;

End if

If (rrep.route != rtable.route)

route from RREP not in route-reply list then route is not trustful ;

End if

End if

}

End If

Create new entry to the RREP received is made in its RREP LIST with count zero;

END

In Below Fig.1 Flow Chart of proposed algorithm is given

Flow chart of Algorithm used:

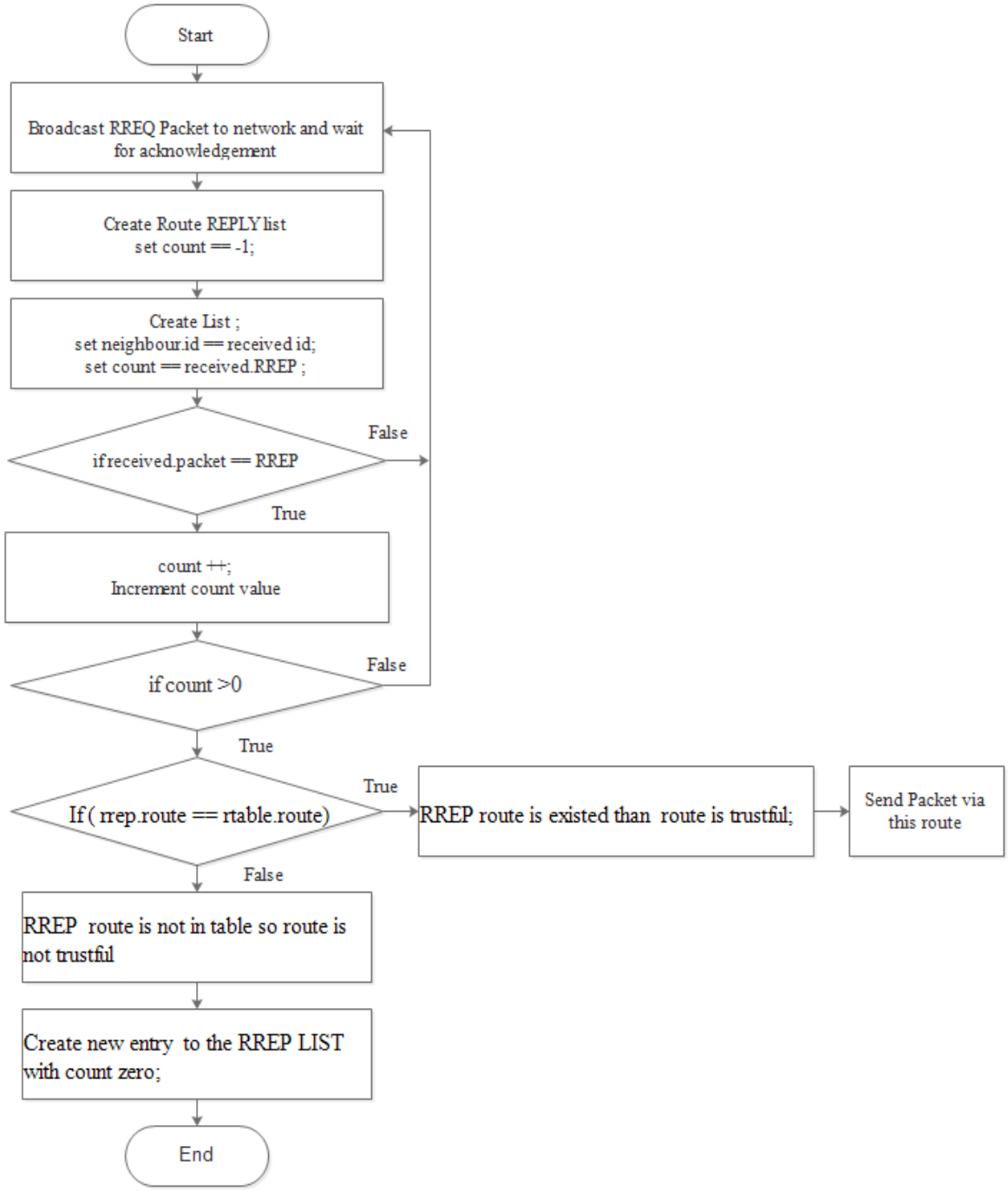

Fig .1 Flowchart of Proposed Algorithm

7. SIMULATION SETUP

Simulation is the replication of essential features of some system or process in order to study the characteristics or performance of the system. This research work requires a network simulator as the proposed work is based on WSN. In this work, Network Simulator (NS- 2) software version 2.35 (NS2.35) is used due to its open source simplicity and free availability. Network Simulator (NS) is a simulation tool developed and maintained by researchers at Berkeley. It is discrete event and object oriented simulator developed for networking research. It provides substantial support for simulation of TCP, routing, and multicast protocols over both wired and wireless networks. NS-2 is written in C++ and Object Tool Command Language (OTCL). User uses the scripting language OTcl for defining the network and other feature like traffic or routing protocols, agents etc. The OTcl script written by user is used by ns during the simulations. The result of the simulations is provided in an output trace file. NS2 also provide an animation tool called Network Animator (NAM) to visualize the packet traces.

Some important component of NS2 simulation is followed as;

1. Tool Command Language

2. Trace File

3. Network Animator

4. AWK Programming

The simulation configuration for mobile nodes consists of many network components and simulation parameters that are shown in the Table 1 in detail.

Simulation ParametersTable .1

Channel	Channel/Wireless
Propagation	Propagation/Two Ray
Network Interface	Phy/Wireless Phy
Platform	Ubuntu 15.04
NS Version	Ns-allinone-2.35
MAC	Mac/802_15_4
Interface Queue	Queue/ Drop tail / Pri
Link Layer	LL
Antenna	Antenna/Omni Antenna
Interface Queue Length	50
No. of Nodes	1,00,50,01,000
Simulation area size	750*550
Traffic Pattern	CBR Sessions
CBR Packet Size	512 bytes
Simulation Duration	100 Sec,200 Sec,1500

In below Fig 2, Fig 3, & Fig 4 shows the type of scenario used in our research work.

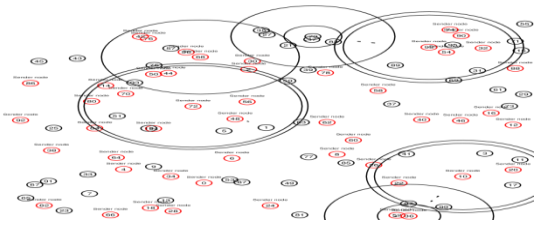

Fig .2 Simulation Scenario 1 with 100 nodes in WSN

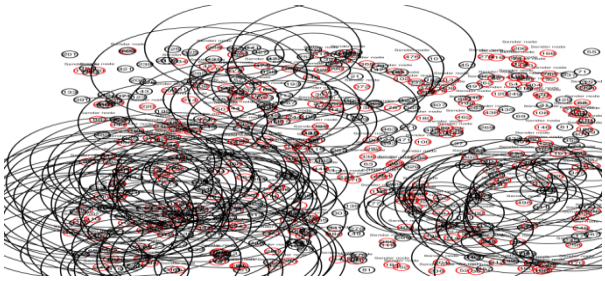

Fig-3 Simulation Scenario 2 with 500 nodes in WSN

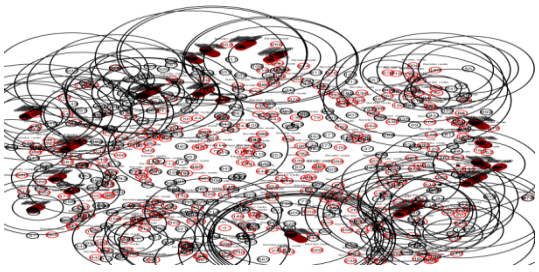

Fig-4 Simulation Scenario 3 with 1000 nodes in WSN

The following metrics are used in this work for comparing the performance of AODV under attacks and Modified AODV routing protocols.

1. Throughput
2. Packet Delivery Ratio
3. Packet Drop Ratio

8. THROUGHPUT

Throughput is the amount of data transferred successfully on a communication network or network link over the period of time. Throughput is calculated in bytes/sec or bits/second (bps).

$$Throughput = \frac{Total\ No.\ of\ Received\ Packets\ at\ Destination}{Total\ Simulation\ Time}$$

In the research paper we have focused on comparison of throughput of 100, 500 and 1000 Node scenario in the simulation time of 100, 200 and 1500 Secs.

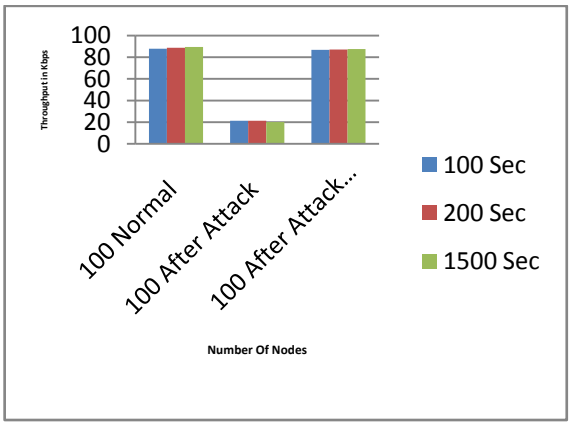

Fig .5 Comparison of Throughput in 100 node network in Simulation Time of 100 Sec, 200 Sec & 1500 Sec

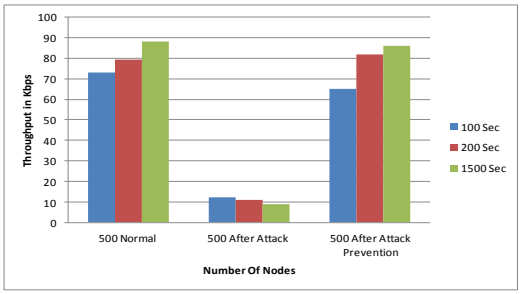

Fig 6 Comparison of Throughput in 500 nodes network in Simulation Time of 100 Sec, 200 Sec & 1500 Sec

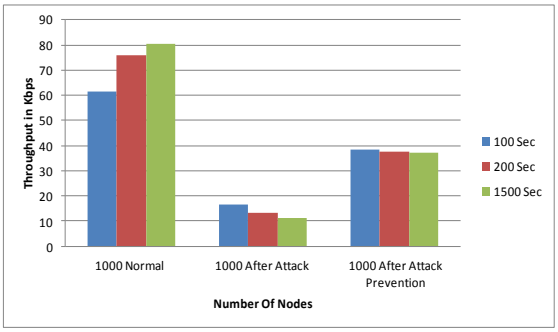

Fig 7 Comparison of Throughput in 1000 nodes network in Simulation Time of 100 Sec, 200 Sec & 1500 Sec

Description: Result shown in above graphs describe that before Gray Hole Attack throughput is high and after Gray Hole Attack, it decrease and after prevention throughput is restore with some difference due to routing path change and routing packet delivery .in 100,500 & 1000 nodes network throughput in 500 nodes network have high throughput after prevention of Gray Hole Attack because of new routing path and low routing overhead. In Scenario of 1000 Nodes throughput which is recovered after prevention of attack is less if we compared to the throughput which we have received in 100 Node and 500 node scenario this is due to scalability of the algorithm, which shows that algorithm having limitation in 1000 Node Scenario.

9. PACKET DELIVERY RATIO

It is the ratio of the number of data packets received by the destination node to the number of data packets sent by the source node. It can be calculated in terms of percentage (%).

$$Packet\ Delivery\ Ratio = \frac{No.\ of\ Received\ Packets}{No.\ of\ Sent\ Packets}$$

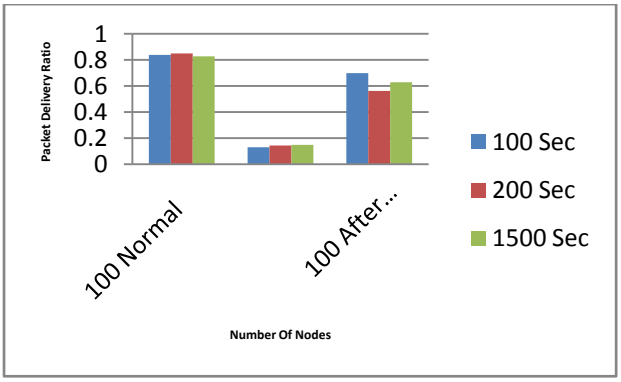

Fig .8 Comparison of Packet Delivery Ratio in 100 nodes network in Simulation Time 100 Sec, 200 Sec & 1500 Sec

Description: Result had shown on Graph for packet delivery ration of 100 Node in simulation time of 100 Sec, 200 Sec and 1500 Sec. As per graph and the results we received on simulation that packet delivery ratio is good in normal scenario while it gets worst during gray hole attack on network. But after prevention of network we again able to recovered the network and received good packet delivery ratio in network.

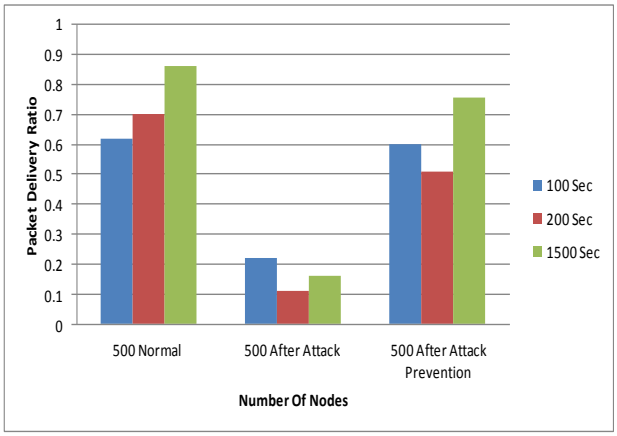

Fig .9 Comparison of Packet Delivery Ratio in 500 nodes network in Simulation Time 100 Sec, 200 Sec & 1500 Sec

Description: Result had shown on Graph for packet delivery ration of 500 Node in simulation time of 100 Sec 200 Sec and 1500 Sec. As per graph and the results we received on simulation that packet delivery ratio is good in normal scenario while it gets worst during gray hole attack on network. But after prevention of network we again able to recovered the network and received good packet delivery ratio in network.

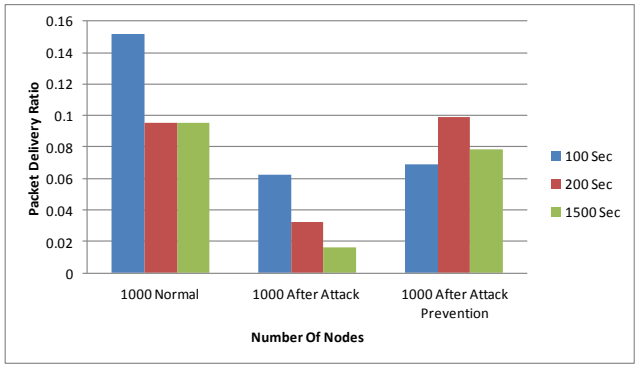

Fig .10 Comparison of Packet Delivery Ratio in 1000 nodes network in Simulation Time 100 Sec, 200 Sec & 1500 Sec

Description: Result shown in above graph describe the PDR for 1000 Node scenario for different simulation time, we found that packet delivery ratio and the recovery of packets are less as compared to packets which we have achieved in normal scenario. The reason behind this is that this is the limitation of Algorithm that it will not give better recovery in the 1000 Node Scenario.

10. PACKET DROP RATIO

The ratio of the number of packets received at the destination and the number of packets sent by the source. In a network system the packet delivery ratio of the flow at any given instance is calculated as,

$$Packet\ Drop\ Ratio = \frac{Total\ No.\ of\ Sent\ Packets - Total\ No.\ of\ Received\ Packets}{Total\ No.\ of\ Sent\ Packets}$$

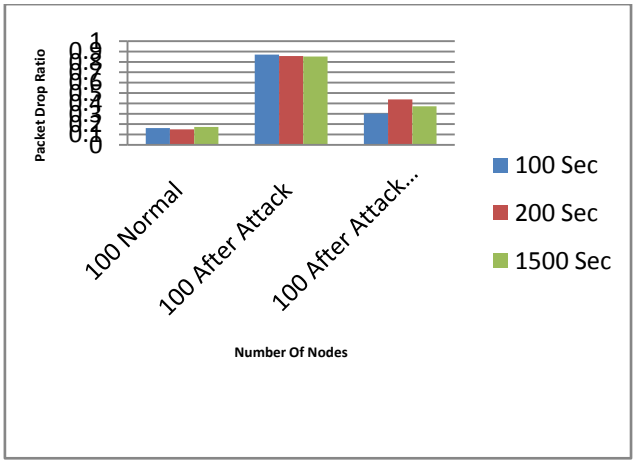

Fig- 11 Comparison of Packet Delivery Ratio in 100 nodes network in Simulation Time 100 Sec, 200 Sec & 1500 Sec

Description: Result shown on the above graph shows that the packet drop ratio in the normal scenario on network is very less but when the network is affected by Gray hole attack the drop ratio goes very high, due selective forwarding attack on

the network, but after prevention of attack, we are able to recovered the network in the satisfactory condition.

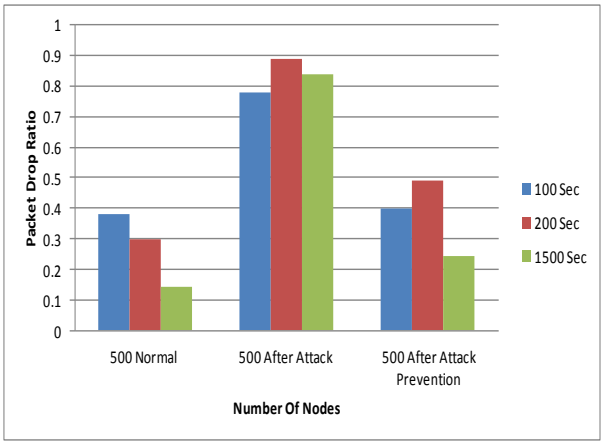

Fig- 12 Comparison of Packet Delivery Ratio in 500 nodes network in Simulation Time 100 Sec, 200 Sec & 1500 Sec

Description: Result shown on the above graph for the scenario of 500 nodes in the different simulation time of 100 200 Sec and 1500 Sec shows that the packet drop ratio in the normal scenario on network is very less but when the network is affected by Gray hole attack the drop ratio goes very high, due the selective forwarding attack on the network, but after prevention of attack, we are able to recovered the network in the satisfactory condition.

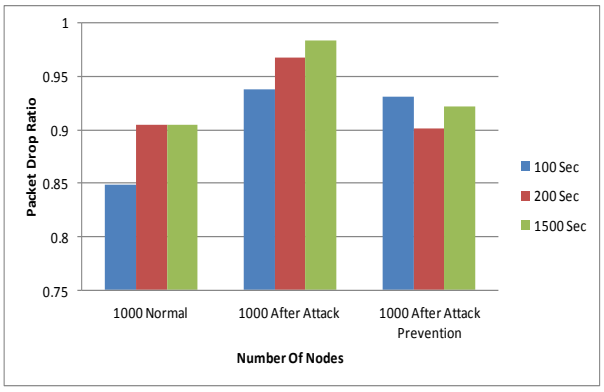

Fig- 12 Comparison of Packet Delivery Ratio in 1000 nodes network in Simulation Time 100 Sec, 200 Sec & 1500 Sec

Description: Result shown in above graph describe the Packet Drop Ratio for 1000 Node scenario for different simulation time, we found that packet drop ratio and the recovery of packets are less as compared to packets which we have achieved in normal scenario. The reason behind this is that this is the limitation of Algorithm that it will not give better recovery in the 1000 Node Scenario.

11. RESULT ANALYSIS

After taking the implementation and other details from the simulation environment, this work had applied some of the policies and designed algorithm on the code of the AODV protocol for detection and prevention of Gray Hole attack in WSN. Proposed technique is implemented and simulated and result is shown in graph using different colors for making the comparison easy and complete. At the end, graph shows the effectiveness and efficiency of the suggested approach on different parameters such a throughput and packet delivery ratio. In all the parameters the suggested approach is performing well. Thus the work is capable of detecting attack on time and with less resource.

12. CONCLUSION

This research work carried out the detailed study and analysis of AODV routing protocols and security issues and attacks in WSN theoretically and through simulation. This research work carried out the study of routing protocols and various security threats. This research work proposed IDS based detection technique to identify malicious node(s) into Wireless Sensor networks. NS-2 simulator has been used to simulate and evaluate the performance of proposed system. Simulation of security strategies provides the facility to select a good security solution for routing protocols and gives the knowledge how to use these schemes in hostile and compromised environments. Simulation results show that packet delivery ratio becomes very less in case of malicious attack. And after implementation of proposed algorithm the packet delivery of the packets recovered satisfactory. Proposed system will not only avoid malicious circumstances but prevent genuine node from packet dropping.

In the complete analysis it is observed that the proposed algorithm performed betters in Gray-hole attack. Still, a scope of improvement is observed and expected to improve the throughput, packet delivery of the packets throughout the network and improves the security of the packets also.

13. FUTURE WORK

Wireless network are subjected to attack due to their scalability and openness and broadcast nature. Today is generation of wireless network, wireless network evolving and next generation network are wireless. so security issue is major concern for wireless network. Gray Hole attack is not limited to wireless network, it have different problems and concepts that remain unaddressed can be performed in the future. The concept like identity management with the help of this approach can provide exact, timely analysis of intrusion of Selective Forwarding Attack attack in network & its successful detection with high accuracy of proposed scheme is embedded network simulator-2 for contribution and help in future research in open standard community. The source code of proposed scheme is embedded network simulator-2 for contribution and help in future research in open standard community

14. ACKNOWLEDGEMENT

The authors wish to acknowledge Oriental University, Indore for their support & motivation during this research. The Author would also like to thank anonymous referees for their many helpful comments, which have strengthened the paper. Author also like to give thanks to Dr. Dhruva Ghai, Dr. Deepak Sukheja and Asst. Prof. Sunil Patel for discussions in specific domain.

15. REFERENCES

[1] Preeti Sharma. Monika Saluja and Krishna Kumar Saluja″ A review of Selective Forwarding Attack in Wireless Sensor Networks.

[2] Aproova Joshi, Pragya Sanghi & Richa Agarwal Priyanka Sharma , “A Reserarch on Selective Forwarding Attack on Leach Network” IPASJ International Journal of Computer Science (IIJCS) ISSN 2321-5992 Vol. 2 Page No. 21-26 December 2006.

[3] K. Ioannis and T. Dimitriou, "Toward intrusion detection in sensor networks," in 13th European Wireless Conference, Page No.1-7 April 2007.

[4] B. Lee and Y.-H. Choi, A Resilient Packet-Forwarding Scheme against Maliciously Packet-Dropping Nodes in Sensor Networks, In Proceedings of the Fourth ACM Workshop on Security of Ad Hoc and Sensor Networks(SASN'06), Page No. 59-70, January 2006.

[5] Wazir Zada Khan,Yang Xiang,Mohammad Y Aalsalem & Quratulain Arshad "Comprehensive Study of Selective Forwaring Attack in Wireless Sensor Network" I.J. Computer Network and Information Security, Page No. 1-10 February 2011.

[6] S.Sharmila & G. Umamaheshwari "Defensive Mechanisms of Selective Forward Attack in Wireless Sensor networks" International Journal of Computer Applications (0975 8887)Vol 4 Page No. 43-49 February 2012.