Enhanced DSR protocol for Detection and Removal of Selective Black Hole Attack in MANET

Mr.Rahul Vasant Chavan [1], Prof.M S.Chaudhari[2]

[1] *Department of Computer Engineering, Sinhgad Institue of Technology Lonavala, Pune, India.*

[2] *Department of Computer Engineering, Sinhgad Institue of Technology Lonavala, Pune, India.*

---***---

Abstract

Black hole attack on a MANET refers to an attack by a malicious node, which forcibly acquires the route from a source to a destination by the falsification of sequence number and hop count of the routing message. A selective black hole is a node that can optionally and alternately perform a black hole attack or perform as a normal node. In this paper, several IDS (intrusion detection system) nodes are deployed in MANETs in order to detect and prevent selective black hole attacks. We proposed an Intrusion Detection System (IDS) where the IDS nodes are set in promiscuous mode only when required, to detect the abnormal difference in the number of data packets being forwarded by a node. When any anomaly is detected, the nearby IDS node broadcast the block message, informing all nodes on the network to cooperatively isolate the malicious node from the network. The proposed technique employs Glomosim to validate the effectiveness of proposed intrusion detection system. This study employs ns3 to validate the effect of the proposed IDS deployment, as IDS nodes can rapidly block a malicious node.

Key Words: MANETs (Mobile ad hoc networks), Black hole attack, Selective black hole attack, Intrusion detection system (IDS),ns3.

1. INTRODUCTION:

In a wireless mobile ad hoc network (MANET), there are no Basic network devices, such as routers or access points; data transfer among nodes is realized by means of multiple hops, and rather than just serving as a single terminal, every mobile node acts as a router to establish a route. When a source node intends to transfer data to a destination node, packets are transferred through the intermediate nodes, thus, searching for and quickly establishing a route from a source to a destination node is an important issue for MANETs. The currently available routing protocols are mainly categorized into two types. So following is the types [1].

1. Proactive routing protocols

2. Reactive routing protocols

In Proactive routing protocols every node proactively searches for routes to other nodes, and periodically exchanges routing messages, in order to keep the formation in the routing table up-to-date and correct. Due to limitation in power and Bandwidth of MANET nodes, frequent transmission of routing messages would lead to congestion of the network. Proactive routing protocol it is mainly divided in to two types, following is [2].

- DSDV
- OLSR.

DSDV is nothing but then, it is Destination Sequenced Distance Vector routing protocol. The Second type is OLSR; it is nothing but the Optimization link state routing protocol In Reactive Routing Protocol, a route is searched and established only when two nodes intend to transfer data; and therefore, it is also called an on-demand routing protocol, such as.

- AODV (Ad hoc On-Demand Distance Vector)
- DSR (Dynamic Source Routing)

A source node generally Broadcasts a route request message to the entire network by means of flooding, in order to search for and establish a route to the destination node. The AODV is the most popular routing protocol and has been extensively discussed in research papers; therefore, this study deploys and evaluates the proposed IDSs on DSR and AODV-based MANETs [3].

MANETs are generally used for communication during natural disasters, on the battlefield, and business conferences, which illustrate the importance of guaranteed safety of data transfer between two nodes, thus, more secure routing protocols have been recently proposed. Most secure routing protocols are designed to prevent hazards to safety properties, such as:

(1) Identity authentication and non-repudiation

(2) Availability of resources

(3) Confidentiality and privacy.

DSR has two main functionalities: Route discovery and Route maintenance. The explanation of these two phases is given below. In Route Discovery phase is to establish a route by flooding Route Request (RREQ) packets in the network. The destination node, on receiving a RREQ packet, responds by sending a Route Reply (RREP) packet back to the source by reversing the route information stored in the RREQ Packet. On receiving the RREQ, any intermediate node can send the RREP back to the source node if it has the route to reach the destination. Route maintenance phase, the link breaks are handled. A link break occurs when any intermediate node which involves in the packet forwarding process moves out of the transmission range of its upstream neighbor [5].

2. RELATED WORK

- “Prevention of co-operative black hole attack in MANET ”
- **Author**-Tamilselvan, Sankaranarayanan VJ.

This Paper addresses that, it is an enhancement of the Basic AODV routing protocol, which will be able to avoid multiple black holes acting in the group. We present a technique to identify multiple black holes cooperating with each other and a solution to discover a safe route avoiding cooperative black hole attack [2]

- “Detecting Black hole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method.”
- **Author**-Satoshi Kurosawa, Hidehisa Nakayama.

In this paper, we have analyzed the black hole attack and introduced the feature in order to define the normal state of the network [3].

- Prevention of selective black hole attacks on mobile ad hoc Networks through intrusion detection systems
- **Author**-Ming-Yang Su.

This paper addresses that, to detect and separate malicious nodes, which selectively perform black hole attacks by deploying IDSs in MANETs (mobile ad hoc networks). All IDS nodes perform an ABM (AntiBlackhole Mechanism), which estimates the suspicious value of a node, according to the amount of abnormal difference between RREQs and RREPs transmitted from the node [4].

- “An Acknowledgment-Based Approach for the Detection of Routing Misbehaviour in MANETs ”
- Kejun Liu, Jing Deng, Member

We study routing misbehavior in MANETs (Mobile Ad Hoc Networks) in this paper. In general, routing protocols for MANETs are designed based on the assumption that all participating nodes are fully cooperative. However, due to the open structure and scarcely available battery-based energy, node misbehavior may exist. One such routing misbehavior is that some selfish nodes will participate in the route discovery and maintenance processes but refuse to forward data packets. In this paper, we propose the 2ACK scheme that serves as an add-on technique for routing schemes to detect routing misbehavior and to mitigate their adverse effect. The main idea of the 2ACK scheme is to send two-hop acknowledgment packets in the opposite direction of the routing path [6].

3. MOTIVATION

As per the brief literature survey the main limitation of existing system is Intermediate Node Some time acts as Normal node some time acts as Malicious node .so at the time of transmitting packets the existing system do not follows any criteria to find out malicious behavior of each and every intermediate nodes, it is very difficult to find out malicious behavior of each every intermediate nodes in mobile ad hoc networks. So in proposed system we are trying to provide security to each node with the help of IDS system. so with the help of IDS system we provide secure packet transmission to each user in MANET.

4. SELECTIVE BLACK HOLE ATTACK

4.1. System Architecture

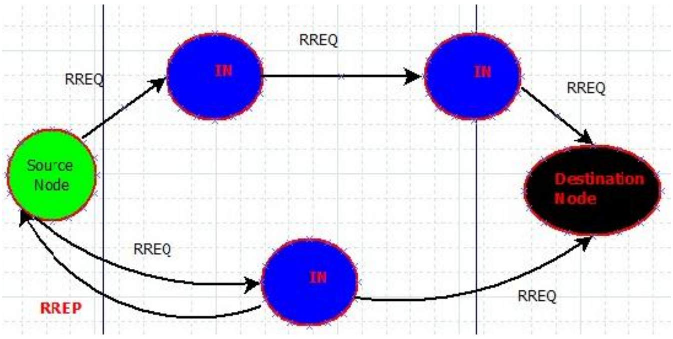

Fig. 4.1. System Architecture

Above diagram explains, after establishing a connection in between source to destination. Source Sends RREQ message to the destination with the help of intermediate nodes. After getting RREQ message to the destination that will send first RREP message back to the source node. Source node simply thinks that this is our trusted path, we can send or transmits packet to the destination with taking help of that intermediate node [1].

After that source node starts to sends packets on that path simulteneously, but source node simply sends packets on that path without think our packets is sends to the destination or not. At one time one intermediate node in the connection, he will forwards some packets to the neighbor node or some packets drops at that location.beacause this IN acts as Malicious node, this attack is called as Black Hole Attack. Selective Black Hole Attack is nothing but ,IN simultaneously drops all the packets at location of that malicious node. so how to provide security to that connection, how to perform a secure packet transmission, how to maintain DRI table entries.etc this problems occurs in Existing system. [1].

4.2. High Level Design

In proposed System, we are going to propose IDS system for providing security to each and every node in mobile adhoc networks. So IDS is nothing but the it is Intrusion Detection System. Intrusion detection is an important technology in business sector as well as an active area of research. It is an important tool for information security. A Network Intrusion Detection System is used to monitor networks for attacks or intrusions and report these intrusions to the administrator in order to take evasive action.

Today computers are part of networked; distributed systems that may span multiple buildings sometimes located thousands of miles apart. The network of such a system is a pathway for communication between the computers in the Mobile ad-hoc networks. The network is also a pathway for intrusion.

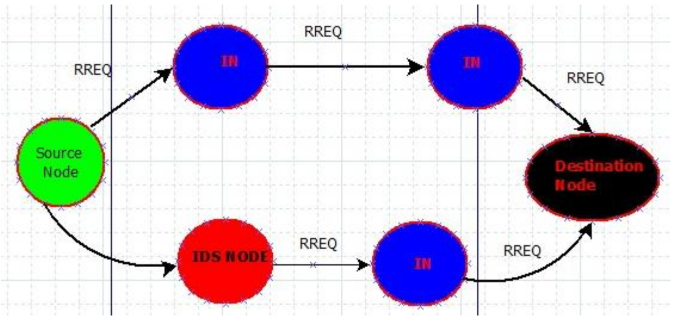

Fig. 4.2 Proposed Architecture

Above diagram depicts proposed solution on Selective black hole attack in mobile adhoc networks. An intrusion detection system (IDS) is composed of hardware and software elements that work together to find unexpected events that may indicate an attack will happen, is happening, or has happened. Note that we must think in all three tenses; some products warn in advance that an attack may take place, some warn as they notice an attack in progress, and some warn when they notice the after-effects of the attack. The goal of an intrusion detection system is to provide an indication of a potential or real attack. An attack or intrusion is a transient event, whereas vulnerability represents an exposure, which carries the potential for an attack or intrusion.

5. PROPOSED ALGORITHM

1. Create topology.

2. Select source node.

3. Path discovery.

- Send RREQ packet along with destination node id.

– Destination reply with RREP packet.

– After validation path will selected as per different Parameters.

4. Data forwarding.

– Data sent by source.

– If path exist data forwarded to next hop.

– Else Path discovery algorithm started again.

– Maintains trust value for each send and receive Packet.

5. Gray Hole attack.

– Generates fake RREQ and RREP packet.

– Get packet attracted to malicious node.

– On time basis packets are get dropped by malicious Node.

6. Malicious node detection.

– Source creates different block of same packet. Forwards packet one by one.

-First it checks the trust values for nodes in path.

- It starts validating node which is very less Trust value to most trust value.

– Also source inform destination about number of Blocks it sending and to inform it uses different path.

– Destination calculates probability of packet received.

– IF PD >= TP L it starts Malicious node detection Algorithm.

.

*It validates current path node by trusting on neighbor and checks how much packets it receives and how much packets it forwarded. If different in count then it sets flag to suspected node.

6. SET THEORY

- Let S represent our proposed system
- S={I, O, Su, Fa, Ø }
- Where,

I = Input, O = Output, Fa= Failure,
Su = Success

- I is input, I={CE, RD, RM,PT, ɗ }

Where,

- CE = Connection Establishment, RD = Rout Discovery, RM = Route Maintenance, PT = Packet Transmission, ɗ = Threshold value

- O is output, O = {PD}
- Where, PD = Probability of Packets Received at the Destination Side.
- Su is success, Su = ST
- Where Su= Successful Transmission
- RT = Routing Table (RT)
  Input = Update
  Output = Count Data Packets
  Failure = No Packet Loss.
- Ø is an constraints of the system,
- Ø = {PD, MN}
- Where, PD = Probability Of Packets Received at the Destination Node
- MN = Malicious Node

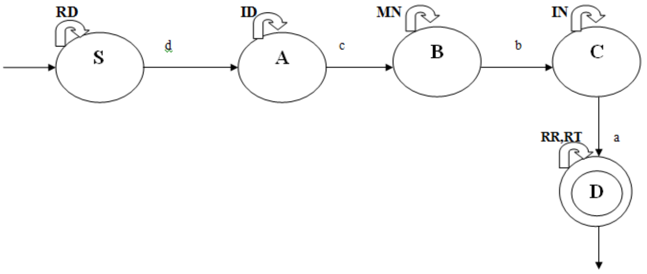

Fig: Deterministic Finite Automata (DFA)

- Where, RD = Route Discovery, ID=Intrusion Detection, MN =Malicious Node,
  IN = Intermediate Node, RR=Route Reply,
  RT= Routing Table.

6.1 Deterministic Finite State Automata

A deterministic finite automata M is a 5-tuple, (Q, Σ, Ø, q0, F) consisting of

- a finite set of states (Q)={S,A, B, C, D}
- a finite set of input symbols called the alphabet (Σ)={a,b,c,d,e}
- a transition function (ɗ : Q×Σ- Q)={RD, ID,MN,IN,RR}
- a start state (q0 ε Q)= S
- a set of accept states (F proper subset of Q)= D
- Where, S-Source Node, D- Destination Node

- A, B, C -Intermediate Node, St- states, Alp-alphabets.
- Derivation (d) is defined by below transition table.

St/Trns	S	ID	MN	IN	DN
A	d	∅	∅	∅	∅
B	∅	c	∅	∅	∅
C	∅	∅	∅	∅	∅
D	∅	∅	∅	a	∅

Fig: Transition Table

7. MULTIPLEXER LOGIC

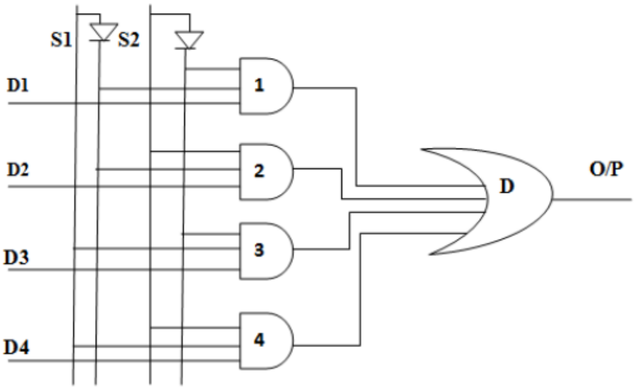

Fig.: Multiplexer Logic

In this Section, Where S1 & S2=Select Lines, D_0 to D_n=Data Packets. The multiplexer logic is use to show the flow of data from one module to another module using logic gates.

8. RESULT AND ANALYSIS

Proposed system validate the detection and isolation efficiency of the proposed method against gray hole nodes. In an area 1000×1000m,50 normal nodes executing the EDSR(Enhanced DSR)routing protocol were randomly distributed and a couple of malicious nodes, selectively performing gray hole attack, are randomly located along with several fixed IDS nodes.

Results of EDSR system is following below,

1.Packet delivery ratio with varying number of IDS nodes.

Below figure shows the PDR of our scheme in presence of five gray hole nodes. First the packet delivery ratio is obtained with nine IDS nodes that cover the entire network region. Then the number of IDS nodes reduced to four which are not sufficient to cover the entire network area. As the number of IDS nodes reduced, Some of the gray hole nodes remain undetected, which results in less packet delivery ratio as compared to Existing system.

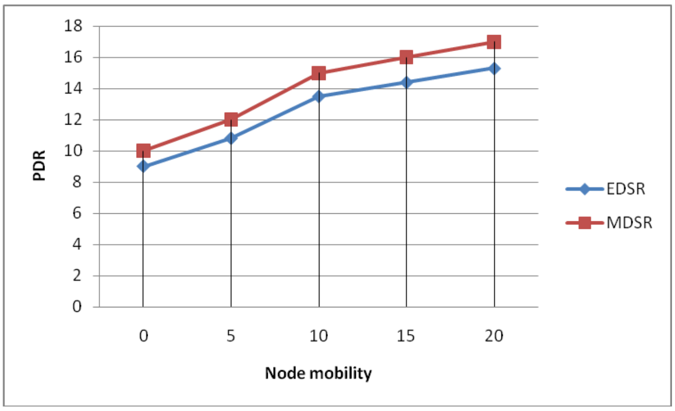

Fig: Packet Delivery Ratio

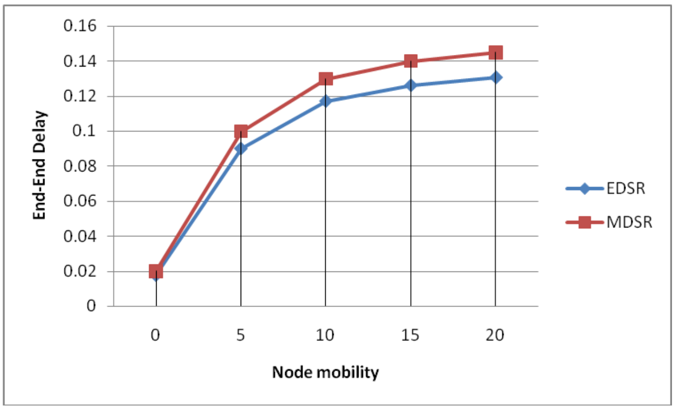

Fig: End-to-End Delay

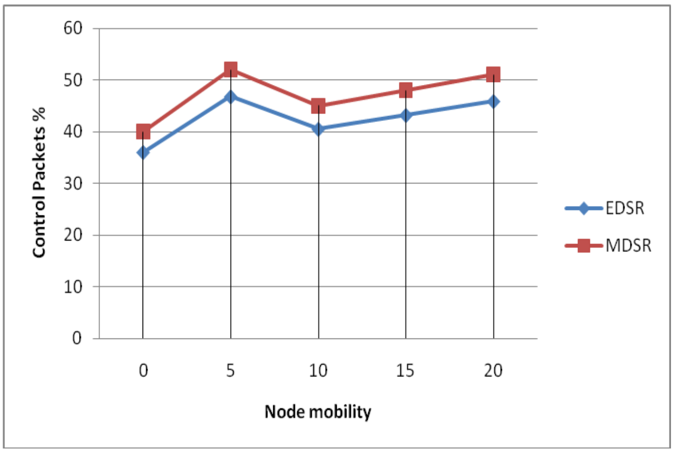

Fig: Control Packet Overhead

9. CONCLUSIONS

In the Proposed solution, we will try to convert Black hole node in to normal node, which selectively Perform black hole attacks by deploying IDSs System in MANETs (mobile ad hoc networks). All IDS nodes Going to define malicious behavior in MANET, which estimates the Packet Threshold Value of a node, According to the amount of abnormal difference between RREQs and RREPs transmitted from the node. The simulation results show that the percentage of data packet loss in our proposed work is better than DSR in presence of multiple Black hole nodes.

REFERENCES

[1] *M. Mohanapriya, Iango Krishnamurthy."Modified DSR protocol for detection and removal of selective black hole attack in MANET". Computers and Electrical Engineering 2014.*

[2]J. *Tamilselvan Latha,."Prevention of co-operative black Hole attack in MANET".J Networks 2008;3(5):1320*.

[3] *R.A. Raja Mahmood, A.I. Khan,and "A Survey on Detecting Black Hole Attack in AODV-based Mobile Ad Hoc Networks", in: Proc. of the International Symposium on High Capacity Optical Networks and Enabling Technologies (HONET),pp. 16, 2007*.

[4] *Ming-Yang Su. "Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems". Comput Commun 2010.*

[5] *Cheng Bo-Chao, Tseng Ryh-Yuh. "A context adaptive intrusion detection system for MANET". Comput Commun 2011; 34:3108*.

[6] *Robert Mitchell, Ing-Ray Chen "A survey of intrusion detection in wireless network applications" 42 (2014) 123.*

[7] *Li-Chin Huang and Min-Shiang Hwang "Study of Intrusion Detection Systems".*

[8]*Luo Junhai, Fan Mingyu, Ye Danxia." Black hole attack prevention based on authentication mechanism". In: Proc. of the IEEE Singapore international conference on communication systems (ICCSs), 2008. p. 173.*

[9] *J. Lou, M. Fan, and D. ye, "Black hole Attack Prevention Based on Authentication Mechanism", International Conference on Communication System, pp. 173-177, 2008.*