Mitigating Selective Blackhole Attacker By Using Divergence Metric Based Advanced Intrusion Detection System

H.Shaleena M.C.A, M.phil[1], A.Prakash, M.C.A, M.Sc(IT), M.Phil, Master(Ph.D) ,[2]

[1] *Research Scholar, Department of Computer Science, Hindusthan College of Arts and Science, Coimbatore, Tamilnadu, India*

[2] *Assistant professor, Department of Computer Science, Hindusthan College of Arts and Science, Coimbatore.*

Abstract— **A mobile adhoc network is a group of mobile nodes that does not have the permanent infrastructure. Providing a route from source to destination is a primary problem in MANET because of the random movement of the nodes. An adversary node generates a Blackhole attack and acquire the route from source to destination. We suggest Intrusion detection system which executes Anti-black hole mechanism for detecting the black hole attack. This mechanism calculates the suspicious value of the nodes based on the irregular dissimilarity between the routing messages transmitted from the node. When there is an increase in suspicious value than the threshold value, an intrusion detection system will transmit a block message, inform to all nodes on the network. This intrusion detection system is only identifies the black hole attacks when they occur constantly. But in this system it does not perceive when the node behaves an attacker occasionally. So in order to conquer this trouble, we provide an innovative approach called advanced intrusion detection method which is identifying the selective black hole attack even it is abnormally behaving rarely. This can be accomplished by including the computation divergence of every node behavior. The divergence distribution precisely discover out even very small divergence of normal behavior. In the advanced intrusion detection method we utilize kulback liebler divergence to compute the divergence in node's behavior.**

Keywords—**MANETs, Selective black hole attack, Intrusion detection system (IDS), Kulback liebler divergence**

I. INTRODUCTION

Typically the mobile adhoc networks are used in military applications, commercial applications that demonstrate the safety of the information is an important dilemma. The data is transmitted by means of multiple hops in the mobile adhoc networks The data send from source to destination by using the intermediate nodes. Because of the irregular movement of the nodes in the mobile adhoc networks, an attacker simply discover route from source to destination. This is an important problem in mobile adhoc networks.

Confidentiality, integrity and availability of the system resources are the major concerns in the development and exploitation of network based computer systems. Improvement in computer infrastructure have elevate the vulnerability of these systems to security threats, attacks and intrusions. Intrusion Detection is the process of identifying, avoiding and possibly answering to the attack and intrusions in a network based computer systems. A black hole attack is an attack that can be happened by the malicious node which identify the route from source to destination. This black hole attack can inspect the route by changing the hop count and the sequence number of the routing message and drop the data. So, in order to conquer this trouble we use intrusion detection systems to recognize and avoid the selective black hole attacks. To perform the function of anti-black hole mechanism the IDS nodes are set in sniff mode. By using this mechanism, to compute a suspicious value of a node according to the irregular difference between the routing messages transmitted from the node. An IDS will broadcast a block message, initiate to all nodes on the network, asking them to coactively separate the malicious node, when a suspicious value of a node surpasses a threshold value.

In the mobile adhoc networks sometimes nodes behave like an attacker rarely. But in the existing intrusion detection system, it capable to identify only the regular occurrence of the black hole attacks. So, in order to rectify this problem we propose an innovative approach called advanced intrusion detection method. This system able to detect the black hole attacks even if they occur infrequently. By including the computation of divergence of each node action, the detection of uncommon occurrence of the black hole attack is accomplished. The divergence distribution faithfully realizes even a very small difference of normal behavior. The proposed advanced intrusion detection method we employ kulback libeler divergence to compute the divergence in node's behavior.

II. LITERATURE REVIEW

Satoshi Kurosawa et.al [1] proposed an anomaly detection scheme using the dynamic training method for detecting the black hole attacks. Because in a Blackhole attack, a malicious node personalizes a destination node by sending a spoofed

route reply packet to a source node that initiates a route discovery. So, it easily drops the data from the node. We utilize a reactive routing protocol known as Ad hoc On-demand Distance Vector (AODV) routing for analysis of the effect of the Blackhole attack when the destination sequence number is changed through simulation. The destination number may change that depends on the traffic involving in the destination. So, depending on the increased amount of destination sequence the effect of the Blackhole attack may also change. Then, we have chosen the features in order to describe the normal state from the characteristic of Blackhole attack. For accurate detection of the Blackhole attack we use a new training method for updating the training data in every given time interval and adaptively defining the normal state according to the changing network environment.

Sanjay Ramaswamy et.al [2] proposed a method to recognize multiple black holes cooperating with each other and provide a resolution to determine a safe route avoiding cooperative black hole attack. By introducing the concept of data routing information(DRI) table and cross checking for identifying the multiple Blackhole attacks. By using two bits of additional information from the nodes responding to the RREQ of a source node S, we find multiple black hole nodes acting in cooperation. Every node in the network maintains the data routing information table. The first bit represents the "From" denotes that the information on routing data packet from the node. The second bit denotes that "Through" denotes that information on routing data through the node. When the source node broadcasts the route request packets to find a secure route to the destination. The intermediate node creating the route reply packet and to provide its next hop node. After receiving the route reply packet from intermediate nodes, the source node verifies its DRI table to see whether the intermediate node is reliable or not**.**

Jacquet p. et.al [3] suggested optimized link state routing protocol for mobile wireless networks. This protocol is based on the link state algorithm and it is table-driven in nature. The protocol achieves something to the stability of the link state algorithm. Since the proactive behaviour of the protocol, it has a benefit of routes instantaneously available when required. In the link state protocol, all the links with the neighboring nodes are declared and flooded in the entire network. For the mobile adhoc networks, Optimized link state routing protocol is an optimization of the link state protocol. Firstly, it minimizes the size of the control packets. In its place of all links, it confirmed only a subset of links with its neighbours who are its multipoint relay sectors. Secondly it decreases the flooding of this control traffic by using only the selected nodes called multipoint relays. Only the multipoint relays of a node retransmit its broadcast messages. This technique drastically minimizes the number of retransmissions in a broadcast nature.

Kimaya Sanzgiri et.al [4] suggested authenticated Routing for Ad hoc Networks (ARAN), employs public-key cryptographic mechanisms to conquer all familiar attacks. In this technique firstly identify the specific protocols that is Ad hoc On-Demand Distance Vector protocol and dynamic source routing protocol gives better performance but the problem is security. Secondly we explain and discriminate the diverse environments that make exploit of ad hoc routing and varied in their assumed pre-deployment and security requirements. At last, we use an Authenticated Routing protocol that recognize and prevent the malicious actions by third parties and nodes. This protocol provides authentication, message integrity, and no repudiation for routing in adhoc networks. Authenticated Routing for Ad hoc Networks consists of consists of a preliminary certification process followed by a route instantiation process that give assurance end-to- end authentication. The protocol is straightforward compared to most non-secured ad hoc routing protocols.

Charles E. Perkins et.al [5] proposed Adhoc On Demand Distance Vector Routing AODV a novel algorithm for the process of the adhoc networks. The main objective of the algorithm is to broadcast the data packets whenever required. AODV employs a broadcast route discovery mechanism as is also used in the Dynamic Source Routing algorithm. This method vigorously offers the route table entries at the intermediate nodes. By using the concept of destination sequence numbers, the routing information is maintained between the nodes. Every adhoc node sustains a monotonically growing sequence number counter which is used to displace stale cached routes.

Frank Kargl et.al [6] proposed secure Adhoc routing protocols to prevent the misbehavior of the nodes. Malicious nodes are trying to damage other nodes or sometimes the whole network. All nodes in the adhoc networks act as a router. Due to the node mobility in the adhoc networks, the topology must constantly change. In the adhoc networks to design the protection mechanism by classifying and structuring the lists of possible attacks. The selfish nodes crash all the route requests received from all other nodes and discard all the packets. Due to this type of attacks, the information is taken by unauthorized instance. However, most network applicants are mobile devices, they can easily be stolen. Thus an attacker can simply gain all data stored in a node. By using the secure routing protocol uses a common session key so that the routing messages can be confirmed in any node on their way between source and destination. The intermediate nodes do not require to execute any cryptographic operations.

Yes-Chun Hu et.al [7] proposed a new secure on-demand ad hoc network routing protocol, called Ariadne to prevent attackers or the compromised nodes. Ad hoc networks necessitate no fixed network infrastructure such as base stations or access points, and can be rapidly and economically set up as needed. By using one of the three schemes the Ariadne can authenticate the routing messages. A shared secret key is used between the all pairs of nodes. A shared secret keys between communicating nodes shared with digital

signatures. The pairwise shared keys evades the necessitate for harmonization, but at the cost of higher key setup overhead. Ariadne also necessitate that each node has an authentic component of the Route Discovery chain of every node initiating Route Discoveries. These keys can be set up in the similar method as a public key.

Semih Dokurer et.al [8] proposed a solution for the black hole attacks in the adhoc networks. A wireless adhoc network is a temporary network, the nodes in this network move randomly. In this type of network there is a large number of attacks and Blackhole attack is a vulnerable one. In this type of attack the malicious node creates the attacks in the nodes and drops all the data packets. By using the Ad-hoc On-Demand Distance Vector protocol to find the route between the source and the destination. When the source node broadcasts the route request packets to the neighboring nodes and identify the route by receiving the route reply packets. Sequence numbers are also used in the route reply messages and they provide as time stamps and permit nodes to evaluate how fresh their information on the other nodes. A Highest sequence number of the nodes are chosen to select a route over this node by the other nodes. So, the Blackhole node sends the route reply with the highest sequence number so source chosen as a route over the Blackhole node and this node drops all the data packets.

III. INTRUSION DETECTION SYSTEM AND KULBACK LIEBLER DIVERGENCE THEOREM

A. Intrusion Detection System

By performing the anti-Blackhole mechanism in the IDS nodes, estimate the suspicious value of a node according to the amount of abnormal variation between RREQs and RREPs transmitted from the node. Whenever the suspicious value exceeds the threshold value, a block message is broadcast to all the nodes to coactively separate the malicious node. This block message contains the identified black hole node, the time of identification. After receiving the block message the normal nodes locate the malicious nodes on their blacklists. There are three algorithms are used as follows:

1.Malicious node: This node selectively executes the BAODV (Black hole AODV) routing algorithm for black hole attacks.

2.Normal node: It executes a slightly revised AODV, called MAODV (Modified AODV) perform normal routing, and also blocks the malicious nodes in collaboration with IDS nodes.

3.IDS node: The Anti-Blackhole Mechanism is executed to detect black hole nodes and issues a Block message.

A malicious node act as a normal node and conducts routing by performing the MAODV (modified AODV). At that time a malicious node performed black hole AODV and set the largest sequence number and 1 hop count in response to RREQ, as it easily attain the route. If the IDS nodes detect the malicious nodes, it sends the block message. After receiving the block message the normal nodes set the malicious node ID‘s in the blacklists. The anti-black hole mechanism performs at the IDS nodes. ABM uses the two tables called RQ and SN tables. The RQ table maintains the RREQ packets of the IDS nodes. The RREQ packets indicates a source node, destination node, the source sequence number. The SN(suspicious node) table is used to record the suspicious nodes of the nodes within the transmission range. The suspicious value is necessary to estimate the malicious node. The suspicious value of the nodes is compared with the threshold value. If not exceeds, it is considered as inactive state. Suppose the suspicious value reach the threshold it considered as active state.

B. ABM for Route Request Process

When IDS nodes sniff the RREQ packets, it searches at both ends of routes as well as source sequence number. If there is no entry, the entry is added. It includes the two ends of the route, Src_seq, hop count, and the ID of the RREQ broadcasting node are copied into the new entry, and ‘‘Expiration time” is set as the current time + 15 s. Suppose already there is an entry, in the broadcasting field the ID of the broadcasting node is and decide whether the hop count in RREQ is greater than Maximal hop count of this entry. If yes, this field value is replaced with the RREQ’s hop count, and then, the Expiration time is added with 3 s to prolong the lifetime of the entry.

```
// When an IDS node sniffs a RREQ transmitted by node N, does the following:
// RQT: RQ Table, RQTE: an entry of RQT
Search RQT for the entry with (Src, Dest, Src_seq)= (RREQ.src_ip, RREQ.dest_ip, RREQ.src_seq);
 if the RQTE exists
        Store N to the RQTE.broadcasting_nodes field;
         if RREQ.hopcount  > RQTE.max_hopcount
        RQTE.max_hopcount ← RREQ.hopcount;
  RQTE.expiration_time←  RQTE.expiration_time+3;
 endif
 else
  Create a RQTE and store data of the RREQ into the new entry;
RQTE.expiration_time ← CURRENT_TIME+15;
endif
return;
```

C. ABM for Route Reply Process

While the IDS nodes sniff the RREP verify the forwarding node is the destination node, if yes, no processing is required otherwise the (Src node, Dest node) in RREP are indexed to inquire of the RQ table. If there is no entry in the RQ table and , it denotes the RREP forwarding node is not within transmission range. So, the algorithm stops the further processing. Suppose if there is an entry in RQ table and broadcasting node includes the ID of RREP forwarding nodes, it denotes a reply to RREQ. So the algorithm stops the process. If the broadcasting field does not contain the RREP forwarding node ID, it denotes this is not a reasonable RREP

reply, thus, it must search the SN table by this RREP forwarding node, by probing the ”Node ID”. In the SN table check the status of the node in the SN table. Otherwise it added value 1 in the SN table, and verify the suspicious value. If it exceeds the threshold the status is active. Block message is broadcast to all nodes.

```
//When an IDS node sniffs a RREP transmitted by node N, does the following:
//S:souce node, D: destination node
//RQT:RQ Table, RQTE: an entry of RQT
//RPT: RP Table, RPTE: an entry of RPT
//SNT: SN Table, SNTE: an entry of SNT
if N is not D
  Search RQT for the entry with (Src, Dest) = (RREP.src_ip, RREP.dest_ip)
  Case 1: the RQTE does not exist
          Drop the RREP;
          return;
Case 2: the RQTE exists and N is in RQTE.broadcasting_nodes field
           Drop the RREP;
           return;
Case 3: the RQTE exists and N is not in RQTE.broadcasting_nodes filed
          Search SNT for the entry with Node_ID=N;
           if the SNTE exists
           if SNTE.status=”active”;
          Drop the RREP;
          else //SNTE.status=”inactive”
          SNTE.suspicious_value++;
           if(SNTE.suspicious_value >= threshold) //a new black hole node
          SNTE.status ← “active”
          Broadcast block message;
          endif
          endif
           else // the SNTE does not exist
  Create s SNTE and store (N, 1, “inactive”) to the new entry;
           endif
          endif
          return;
```

D. Anti-Blackhole Mechanism

When the suspicious value of the node attains the threshold, the IDS node broadcasts the block message to the normal nodes within the transmission range to update the block table. At the same time near IDS nodes hear this block message verify if the malicious node ID is in the Node ID field of the SN table. If it is in the table, the status is inactive, modify the status to active and inform the normal nodes within the transmission range. When the node status is active, the data is dropped without handling, generate a new entry, store the recognized node in the SN table, and place the suspicious value as the threshold value and the Status as active, and then, re-broadcast this Block message.

```
Algorithm For Block Message

For Normal Node
//BT: Block table, BTE: an entry of BT
//BM: Block message;
//BM node: the identified black hole node ID  which is contained in BM
Search BT for the entry with Malicious_Node= BM.node;
  if the BTE exists //already known
     Drop the block message;
  else
  Create a BTE and store (IDS_A, BM.node, CURRENT_TIME) to the new entry;
   endif
   return;

For Neighbouring IDS
  //When an IDS node receives a Block message,  does the following:
   //SNT: SN table, SNTE: an entry of SNT
   //BM: Block message
   //BM.node: the identified black hole node ID  which is contained in BM
   Search SNT for the entry with  Node_ID=BM.node;
    if the SNTE exists
    if SNTE.status=”active” //already known
       Drop the Block message;
    else //SNTE.status=”inactive”
       SNTE.status ← “active”;
      SNTE.suspicious_value←threshold;
       Transmit the Block message;
   endif
  else //the SNTE does not exist
   Create a SNTE and store(BM.node, threshold, “active”) to the new entry;
       Transmit the Block message;
   endif
   return:
```

E. Advanced Intrusion Detection System

An advanced intrusion detection system is introduced to detect the malicious nodes when the nodes act as an attacker rarely. This detection method is accomplished by using the computation of divergence of each node behaviour. To compute the divergence of each node we employ kulback liebler divergence. The kulback liebler divergence is a non-symmetric measure of the difference between two probability distributions P and Q. Usually, the kulback liebler divergence of Q from P expressed as D(P||Q), is a measure of the information lost when Q is used to approximate P. Kullback-Leibler divergence measures the predictable number of extra bits required to code samples from P when using a code based on Q, than using a code based on P. Normally P symbolizes the "true" allocation of data, annotations. The measure Q usually corresponds to an approximation of P. Basically, the symmetric Kullback–Leibler divergence is defined as,

D(P||Q) + D(Q|| P)

The symmetric Kullback-Leibler divergence is calculated for discrete probability mass distributions P and Q,

$$SD_{KL}(P||Q) = \sum_i \ln\left(\frac{p(i)}{Q(i)}\right) P(i) + \sum_i \ln\left(\frac{Q(i)}{P(i)}\right) Q(i)$$

If p(x) and q(x) are distributions defined for continuous random variables, the Kullback-Leibler divergence is ,

$$SD_{KL}(p||q) = \int_{-\infty}^{\infty} \ln\left(\frac{p(x)}{q(x)}\right) p(x)\, dx + \int_{-\infty}^{\infty} \ln\left(\frac{q(x)}{p(x)}\right) q(x)\, dx$$

IV. Experimental Results

Finally, in this section an intrusion detection system(IDS) and the advanced intrusion detection system(AIDS) is compared. The experimental results validate the detection and isolation efficiency of the intrusion detection system and advanced intrusion detection system against black hole nodes. For data communication twenty pairs of nodes are randomly selected. Their random speed is ranging between 0 and 20 m/s. Addition to that, four types of pause times of the normal nodes 0 s, 5 s, 10 s, and 15 s were separately considered. Pause time is nothing but the time that a portable node can stay in one place, and then persist in moving.

A. Packet Loss Rate

The total packet loss rates is defined as the ratio of missing packets to sent packets; in other words, the number of packets that failed to reach their destinations, to the total number of packets transmitted from all source nodes of the whole network. Fig 1. illustrates the packet loss rate. One Blackhole node move randomly like the normal nodes at max.20m/s, the total packet loss rate is varied for the different numbers of IDSs and also for the advanced intrusion detection system. It clearly shows that the number of IDSs are increased there is reduction in the packet loss rate.

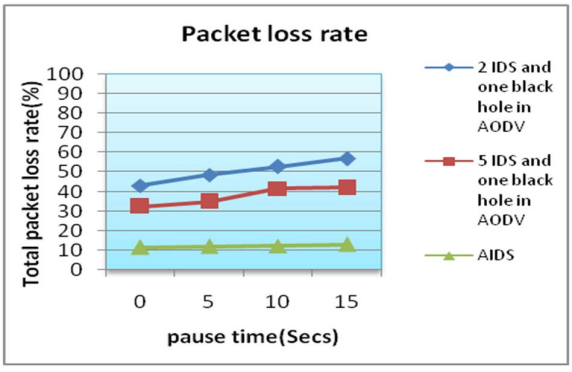

Figure 1: Packet loss rate

B. End-to-end Delay

Fig 2 shows that end-to-end delay. End-to-end delay is defined as the time taken for a packet to be transmitted across a network from source to destination.This clearly shows that the end-to-end delay increases as the number of nodes increases. The number of IDSs are increased the end-to-end delay is reduced. In the advanced intrusion detection system the end-to-end delay is decreased when compared to the existing system.

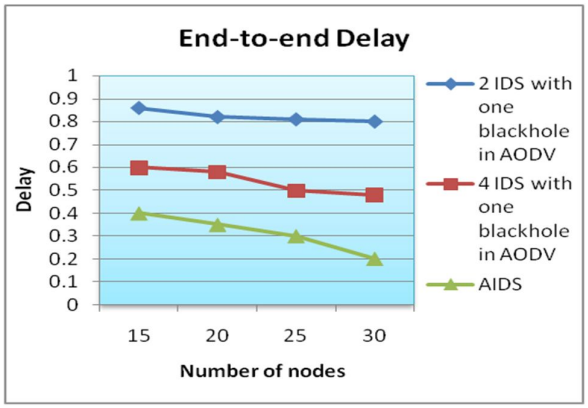

Figure 2: End-to-end delay

C. Overhead

Fig 3 shows that overhead. Overhead is defined is the number of routing packets transmitted per data packet delivered at the destination. This clearly shows that the overhead increases as the number of nodes increases. When the number of IDSs are increased the overhead is reduced. Compared to existing system the overhead is decreased in the advanced intrusion detection system.

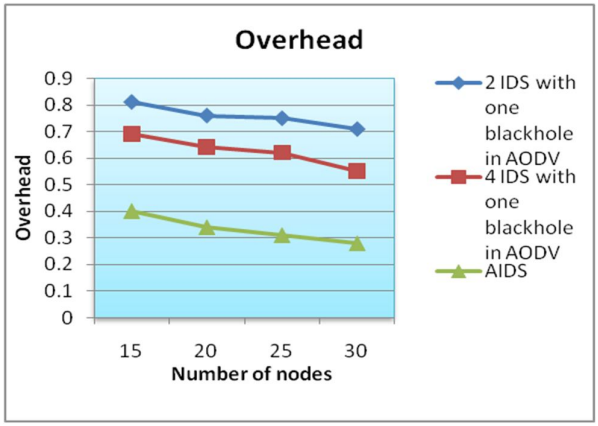

Figure 3: Overhead

V. Conclusion and Future Work

An intrusion detection system is one of the methods to detect and isolate the malicious nodes. The Intrusion detection nodes

employ the anti-Blackhole mechanism that computes the suspicious value of all the nodes. It compares with the threshold value and identify the malicious nodes. In order to identify the infrequent occurred attacks, we compute the divergence of each node behaviour. By using kulback liebler divergence to compute the divergence in node's behavior. By using this method we identify the malicious node efficiently. For future work, in order to examine the multiple hosts connected through a network as well as a network itself we use Distributed Intrusion Detection for large-scale network environment. The design and implementation of the Distributed Intrusion Detection prototype relies on Security Agents which monitor network traffic and report intrusion alerts to a central management node.

REFERENCES

[1] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, Yoshiaki Nemoto, "Detecting Blackhole attack on AODV-based Mobile Ad Hoc Networks by dynamic learning method", *International Journal of Network Security 5 (3)* (2007) 338–346.

[2] Latha Tamilselvan, Dr.V. Sankaranarayanan, "Prevention of co-operative black hole attack in MANET", *Journal of Networks 3 (5)* (2008) 13–20.

[3] T. Clausen, P. Jacquet, "Optimized Link State Routing Protocol (OLSR)", *IETF RFC 3626*, October 2003.

[4] Kimaya Sanzgiri, Daniel LaFlamme, Bridget Dahill, Brian Neil Levine, Clay Shields, Elizabeth M. Belding-Royer, "Authenticated routing for Ad hoc networks", *IEEE Journal on Selected Areas in Communications 23 (3)* (2005) 598–610.

[5] Charles E. Perkins, Pravin Bhagwat, "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers", *SIGCOMM* (1994).

[6] Manel G. Zapata, N. Asokan, ''Securing Ad-hoc Routing Protocols", *in: Proc. of the ACM Workshop on Wireless Security (WiSe)*, 2002.

[7] Yih-Chun Hu, Adrian Perrig, David B. Johnson, ''Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks", *in: Proc. of the ACM Conference on Mobile Computing and Networking (MobiCom)*, pp. 12–23, 2002.

[8] Semih Dokurer, Y.M. Erten, Can Erkin Acar, ''Performance Analysis of Ad-hoc Networks under Black Hole Attacks", *in: Proc. of the IEEE SoutheastCon*, pp. 148–153, 2007.

[9] Junhai Luo, Mingyu Fan, Danxia Ye, ''Black Hole Attack Prevention Based on Authentication Mechanism", *in: Proc. of the IEEE Singapore International Conference on Communication Systems (ICCS), pp. 173–177*, 2008.

[10] R.A. Raja Mahmood, A.I. Khan, ''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. 1–6, 2007.