International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 15 (2015) pp 35725-35732
© Research India Publications. http://www.ripublication.com

Anonymous and CDCF Based Detection for Blackhole and Wormhole Attacks in DSR Based Manet

M.D.Vimalapriya
Research Scholar
Sathyabama University,
Chennai, India.

Dr.S.Santhosh Baboo
Associate Professor,
Post Graduate and Research,
Department of Computer Applications,
D.G.Vaishnav College,Chennai,India.

Abstract-Wireless networks are gaining popularity to its peak today, as the users want wireless connectivity irrespective of their geographic position. There is an increasing threat of attacks on the Mobile Ad-hoc Networks (MANET). Most of the attacks in MANETs target the routing protocols. The mobility of nodes makes it more vulnerable to routing protocol attacks. By attacking the routing protocols, the attackers can absorb network traffic or inject themselves into the path between the source and destination. Some most recent attacks on the routing protocol in MANETs are Blackhole and Wormhole attacks. They actively participate in the network and conform to forward packets to the destination. In this paper, propose a method called Anomaly based behavior monitoring algorithm for black hole attack and Channel detection and cut defalconin for wormhole attack will detect the malicious nodes in a MANET. Possibly analyze the impact of these attacks on data communication when using a reactive routing protocol called Dynamic Source Routing (DSR) Protocol. The simulation shows that our proposed method has high reliability for detecting both black hole attack and wormhole attacks.

Keywords: Blackhole attack, DSR, MANET, Wormhole attack, Behavior monitoring, cut defalconin.

Introduction

A Mobile Ad hoc Network (Manets) is a self-ruling gathering of mobile devices (nodes) that correspond with one another over wireless links and participate in a circulated way so as to give the vital system usefulness without a settled framework [1]. Ordinary systems use committed node to complete essential capacities like bundle sending, steering, and system administration. In specially appointed systems these are completed collectively by all accessible node. Node on Manets use multi-hop correspondence: node that are inside one another's radio extent can impart specifically through wireless links, while those that are far separated must depend on moderate node to go about as switches to hand-off messages. Versatile node can move, leave and join the system and routes need to be redesigned as often as possible because of the element system topology. Nonetheless, because of their intrinsic qualities of element topology and absence of unified administration, security, MANET is defenseless against different sorts of attacks [2] [3].

Two such discriminating assaults are black hole and wormhole attack. Black hole attack is one of numerous conceivable assaults in MANET. In this assault, a malicious node sends a fashioned Route Reply (RREP) bundle to a source node that starts the course finding keeping in mind the end goal to claim to be a destination node. By thinking about the destination succession number held in RREP packets when a source node gained different RREP, it judges the best one as the latest steering data and chooses the course held in that RREP parcel. On the off chance that the arrangement numbers are equivalent it chooses the course with the most diminutive jump number. On the off chance that the attacker mock the character to be the destination node and sends RREP with a destination succession number higher than the true destination node to the source node, the information activity will stream around the attacker. Accordingly, source and destination nodes got unable to correspond with one another. In [4], the creators examined the impact of black hole attack when development speed and a number association around the victimized person node are changed, and proposed the recognition system at the destination node. On the other hand, we can successfully stay away from the attack, for instance by selecting the redirection route throughout route reproduction, which accomplished by identifying the attack at the source node instead of at the destination node. Therefore, considering the location at the source node is key. In Wormhole attack two challengers arrange by tunneling packets between one another with a specific end goal to make an easy route (or Wormhole) in the system. In the wake of building a wormhole link, one attacker can accept all the messages which go from this route. The DSR protocol [5] is utilized to discover the Black hole attack and Wormhole attack and proposed routing offer various potential advantages over ordinary routing protocols, for example, separation vector in an ad hoc system.

Initially, dissimilar to customary routing protocols, our protocol utilizes no occasional routing advertisement messages, along these lines diminishing system data transmission overhead, especially throughout periods when almost no huge host development is occurring.

In this paper, to defeat the attacks utilizing two sorts of calculations, specifically as Anomaly based behavior monitoring for black hole attack and Channel detection cut defalconin for wormhole attack, to the underlying of DSR protocol.The rest of this paper is organized as follows. In Section 2, provides the related work in MANET and section

3, describe an overview of DSR protocol and black hole and wormhole attacks on DSR routing protocol. In Section 4, the proposed method is presented and simulation results are given in Section 5. Conclude the paper in Section 6.

Related Works

Black hole attack and Wormhole attack are one of the most dangerous attacks. Many researchers did their work on these attacks and try to provide the solution for these attacks. The researchers provide a lot of solutions based on different techniques and different routing protocols. Some important approaches are described below

Latha Tamilselvan, Dr. V Sankaranarayanan [6] proposed a solution with the enhancement of the AODV protocol, which avoids multiple black holes in the group. A technique is given to identify multiple black holes cooperating with each other and discover the safe route by avoiding the attacks. It was assumed in the solution that nodes are already authenticated and therefore can participate in the communication. It uses Fidelity table where every node that is participating is given a fidelity level that will provide reliability to that node. Any node having zero value is considered as malicious node and is eliminated.

Rutvij, Sankita et., al.[7] explored on a proportion of the current methodologies for black hole and gray hole strike and exhibited a novel result against these attacks which can discover sufficiently short and secure routes to destinations. Their assumed dissection showed that this methodology appropriately can build the packet delivery ratio (PDR) with irrelevant distinction in routing overhead. The initiators accepted that this calculation could be utilized for the other reactive protocol and likewise discovers and destroys malicious nodes inside the route discovering stage. Nodes accepting a RREP sustain reality of routing data; source node shows an arrangement of malicious nodes when sending RREQ. Nodes redesign route tables when they get any data of malicious nodes from getting routing packets. No extra control packet might be specified as a profit of this calculation and there is a minor contrast in routing overhead, which is the degree of the amount of routing related transmissions to the amount of information related transmissions. Furthermore, the malicious nodes might be separated and packet delivery proportion (PDR) will enormously be progressed.

Kuldeep Sharma et al [8] proposed an approach which is based on the MHA (Multiple hop count analysis). In this approach they use a general concept that the route contains the hop count 5 or 6, but the route under a wormhole has a hop count value 2. So, if the users avoid the route with smallest hop count can easily avoid most of the wormhole attacks. In this approach, they calculate the hop count value for all the routes and then select a safe set of routes for the transmission of the data. And then send the packet in a random order of these safe routes. They implemented their approach in the AODV routing protocol. Then they assign a unique ID to each and every node so that we can easily differentiate between the simple node and the attacker malicious node.

Y. C. Hu et.al. [9] have recognized packet loss – geographic and temporal. In geographic chains, node location information is utilized to bound the separation a packet can cross. Since wormhole attacks can influence localization, the location information must be acquired by means of an out-of-band component, for example, GPS. Further, the "legitimate" separation a packet can cross is not generally simple to focus. In temporal chains, amazingly exact all inclusive synchronized clocks are utilized to bound the stimulating time of packets that could be tricky to get especially in minimal effort sensor fittings. Actually when accessible, such timing analysis will be unable to catch cut-through or physical layer wormhole attacks.

Khalil et al [10] propose a protocol for wormhole attack discovery in static networks they call LiteWorp. In LiteWorp, once deployed, nodes obtain full two-hop routing information from their neighbors. While a standard ad hoc routing protocol node usually keep track of who their neighbors are, in LiteWorp they also know who the neighbors‟ neighbors are, - they can take advantage of two-hop, rather than one-hop, neighbor information. This information can be exploited to detect wormhole attacks. After authentication, nodes do not accept messages from those they did not originally register as neighbors. Also, nodes observe their neighbors‟ behavior to determine whether data packets are being properly forwarded by the neighbor, so called „watchdog‟ approach. LiteWorp adds an interesting wormhole-specific twist to the standard watchdog behavior: nodes not only verify that all packets are forwarded properly, but also make sure that no node is sending packets it did not receive (as would be the case with the wormhole).

Overview on Dynamic Source Routing Protocol

The Dynamic Source Routing protocol (DSR) is a basic and effective routing protocol outlined particularly for utilization in multihop remote ad hoc networks of portable mobile nodes. DSR permits the system to be totally dealing with toward self-organizing and self-configuring, without the requirement for any current system base or administration. DSR maintains a route cache, which leads to memory overhead. And maintains a routing table, which stores the each node information and the next hop information/address. There are two important mechanisms in DSR: Route discovery mechanism and Route maintenance mechanism, which discover and maintains a source route to random destinations in the ad hoc network route to the destination. DSR protocol is popular reactive routing protocols.

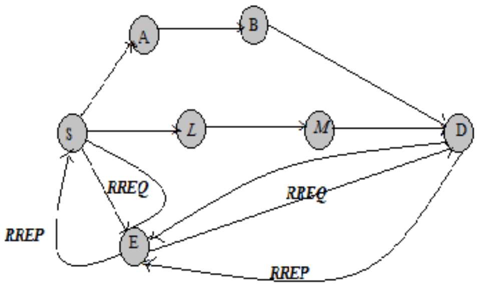

Fig 1 Route Recovery Process

The Route discovery mechanism is used to find the route between the sender and the receiver. In this mechanism, consider the Fig 1, a node **S** longing to send a packet to a destination node **D** gets a source route to D. Route Discovery is utilized just when S activities to send a packet to destination node D and it doesn't know a route to D. [11]. S will acquire a suitable source route via looking its Route Cache of routes beforehand adapted, however in the event that no route is found in its cache, it will launch the Route Discovery convention to rapidly discover a new route to D.

To initiate the Route Discovery [11] the source transmits a ROUTE REQUEST (RREQ) message to all nodes within wireless transmission range of source. Each RREQ also holds a record posting the location of each one moderate node through which this specific duplicate of the RREQ message has been sent. At the point when an alternate node gets a RREQ, on the off chance that it is the focus of the Route Discovery, it gives back a ROUTE REPLY (RREP) message to the initiator of the Route Discovery. At the point when the initiator gets this ROUTE REPLY, it reserves this route in its Route Cache for utilization in sending resulting packets to this goal. On the off chance that it observes that its own particular location is as of now recorded in the route record in the RREQ message, it tosses the REQUEST.

Route Maintenance [11] is the system by which node S can recognize, while utilizing a source route to D, if the system topology has changed such that it can no more utilize its route to D in light of the fact that a connection along the route no more meets expectations. At the point when Route Maintenance demonstrates a source route is broken, S can endeavor to utilize whatever available route it happens to know to D, or can conjure Route Discovery again to discover another route. Route Maintenance is utilized just when S is really sending packets to D. Route Discovery and Route. When all nodes are approximately stationary with respect to each other and all routes needed for current communication have already been discovered. As nodes start to move more or as correspondence examples change, the routing bundle overhead of DSR naturally scales to just that required to track the courses at present being used. In response to a single Route Discovery, a node may learn and cache multiple routes to any destination. This caching of multiple routes also keeps away from the overhead of expecting to perform another Route Discovery each one time a course being used breaks. The DSR protocol is a secure, efficient approach for the detection of the Black hole attack and Wormhole attack in the Mobile Ad-hoc Networks.

Description of Routing Attack on DSR Protocol

In black hole attack, a malicious node waits for the neighbors to initiate a RREQ packet. As the node receives the RREQ packet, it will immediately send a false RREP packet with a modified higher sequence number. So, that the source node assumes that the node is having the fresh route towards the destination. The source node ignores the RREP packet received from other nodes and begins to send the data packets over malicious node. A malicious node takes all the routes towards itself [12]. It does not allow forwarding any packet anywhere. This attack is called a Black Hole Attack. And then the attacker will decide whether the data may be forwarded or to be discarded.

For example, in Fig. 2, consider a source node S, destination node D and intermediate node A, B. Here the source node S sends packets to the destination D through the intermediate nodes A, B. The source node S, first send the RREQ to the node A and wait for the RREP message from A. And then A sends the RREQ to the next hop and receive the RREP from B node. Intermediate node B is the malicious node, it does not allow any packets to anywhere, and it holds the packet information. Node Finally the malicious node sends fake or false routing information to the source node. So the destination could not receive any data packets from the source node.

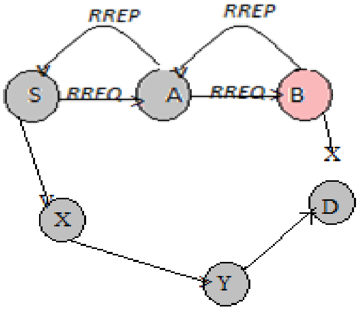

Fig. 2 Black Hole Attack

Worm hole attack

In Worm hole attack**,** two or more malicious nodes together make a tunnel in the network, in which the traffic is enter from one end and passes through the tunnel and leaves from the other end [13]. Wormhole link or tunnel can be created by means of a high quality wireless link or a logical link. After building a wormhole link, one attacker is able to receive all the messages which travel from this route. This attacker node, then copies packets from its neighbors, and forwards them to the other malicious attacker through the wormhole link. Then another malicious node which receives these packets, replays them into the network in its locality.

The following Fig. 3 shows the worm hole attack, consider a source node S, a destination node D, and intermediate nodes

A, B, C. The source node S wants to communicate with D, then send the route request packet to the intermediate node A, and receives route reply messages from node A. Likewise, the node A sends route request packet to the node B, and receives route reply messages from node B. Here the node B is a malicious node and the next node C is also a malicious node, both the nodes form a tunnel (or) link. The link is called Worm hole link, through this link the malicious nodes are forward the packets from one end to another end. The B node forward the data packets to see, that the node C modified the packet information and sent to the destination node D. In the worm hole attack, the needed original data packets are not properly received by the destination node.

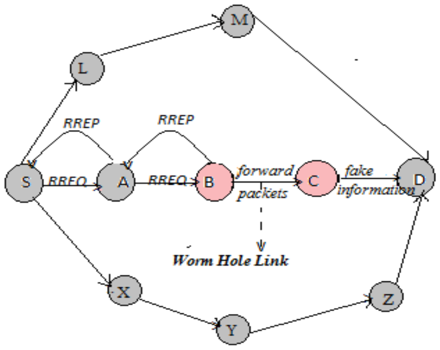

Fig 3 Worm Hole Attack

Anomaly based behavior monitoring

In a mobile ad-hoc network, the Black hole attack is one of the issue, while communication between source and destination. In this black hole attack, a malicious node hold the packet information from the neighboring nodes, while forwarding the packets from the source to the destination. To overcome this problem, the proposed algorithm called Anomaly based behavior monitoring.In this algorithm, number of packets send by the source node X_n is equal to the number of packets received by the destination nodeY_n. If number of packets send by source node is less than or greater than number of packets received by destination node to be an indication of anomalous behavior.

For example in fig. 4, if a source node S wants to send packets to a destination node D through the intermediate nodes A, B and C Using Route Discovery mechanism to initiate the route between S to D. Then the source node sends a number of packets to the destination node through A, B, C. In the Source node maintains a table X, it contains the number of packets send by the source node. Likewise, the destination node maintains a table Y, it contains the number of packets received by the destination node. In case of any malicious node occurred, using our proposed algorithm in DSR protocol the source node compares its tables X with a destination table Y. Here source node sends four packets through the route A-B-C and the destination node receives two packets through the route C-B-A. Now the number of packets received by destination node is different from the number of packets send by the source node. Through this comparison, the source node could detect the malicious node, using monitoring the behavior of each node. After detect the malicious node, the source node rejects that route and choose a new route using *route discovery* mechanism. Through this new route S can send packets to the same destination node D. So using this algorithm a source node easily detect the black hole attack and overcome it.

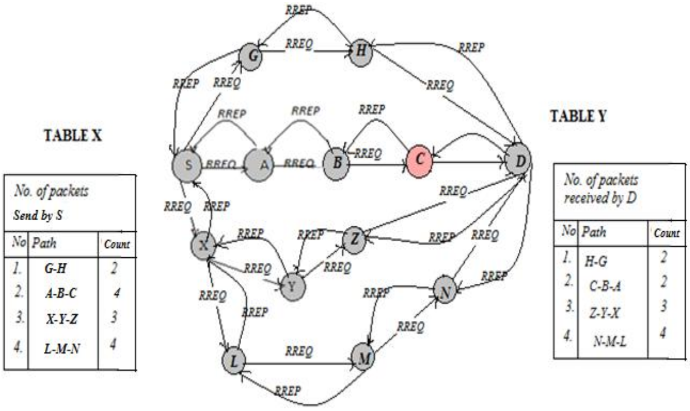

TABLE X

No. of packets Send by S

No	Path	Count
1.	G-H	2
2.	A-B-C	4
3.	X-Y-Z	3
4.	L-M-N	4

TABLE Y

No. of packets received by D

No	Path	Count
1.	H-G	2
2.	C-B-A	2
3.	Z-Y-X	3
4.	N-M-L	4

Fig.4. Analysis of packets sending and Receiving

A. Pseudo code for black hole attack detection using Anomaly based behavior monitoring

```
For t containing n
Split tx, ty
For all RREQ from source check RREPs.
Compute all the number of Intermediates IN
Check if IN(i)== RREQ[forward] and IN(i)==RREP(i)
if IN(i)!=RREP(i) then
Check neighbor RT in (tx,ty)
For IN(i+1) to IN(i+n)
If  IN(i)!=RREP(i) then
(Tx,ty)→ blackhole
IN(I to n) in (Tx,Ty)→ malicious
End if
End for
 For which ever IN(I to n), if IN(i)== RREQ[forward] and IN(i)==RREP(i) then
Read Txi,Tyi
Repeat RREQ and RREP for all IN(j to n) that belongs to (Txi,Tyi)
For each and every N that belongs to (Tx,Ty) or (Txi,Tyi)
Check if N(i) forwards all RREQ if N(i)!=Destination
If N(i)==Destination then RREQ==RREP
End if
End for

Case1:
If number of RREP<<RREQ then
Re-broadcast for N(i)
End if
Case2:
If number of RREP>RREQ then
Update the RT as new Neighbor (Directly connected)
```

```
Check if all N(i to n) satisfies the above condition.
If yes, then choose them as intermediate nodes.
End if
```

Where
RT→ Routing Table
N(i to n)→ node ‘i’ to ‘n’
RREQ→ Route Request
RREP→ Route Reply
N(i)→ Node ‘i’
(Tx,Ty)→Topology sector that belongs to a network Region
(Txi,Tyi)→ New Topology Sector
IN→ Intermediate node

Channel detection and cut algorithm to Detect Worm hole attack

The worm hole attack is one of the problems in mobile ad-hoc network, while communication between a source node and a destination. In the worm hole attack, a group of malicious nodes join and create a tunnel between the source and destination. Through this tunnel, the malicious node sends packets to the next malicious node, end of the tunnel, a modified data packet or false data packet forward to the destination. To overcome this worm hole attack using *Channel detection and cut algorithm.* The malicious nodes m1, m2, m3 are occurring between a source node S and destination node D. Here the source node maintains a *Threshold value* (a node gets higher priority if it sends less numbers of RREQ packets and defined the threshold value). While forwards packet from source to destination with the malicious nodes, its take more *Round Trip Time* (RTT) to forward the packets to the destination. Forwards packet from source to the destination without the malicious nodes, its take less RRT to forward the packets to the destination. Based on the RTT, a source node set the threshold value.

The round trip time (RTT) is taken by ascertaining the time distinction between the packet, it had sent to its neighbor and the answer gained by it. The delay per hop value (DPH) is ascertained as RTT/2h, where h is the hop count to the specific neighbor. Under typical circumstances, a littler h will additionally have more modest RTT. In any case, under wormhole attack, even a more diminutive hop count might have a bigger RTT. In the event that one DPH value for hub X surpasses the progressive one by some threshold, then the way through hub X to all different ways with DPH values bigger than it is dealt with as under wormhole attack. In the wake of sending the RREQ, the source sits tight for the RREP. The source gets numerous RREP going the distance diverse routes. The connection with high recurrence is checked using the following expression:

$Ei = ni / N$, for all Ii
$Emax = max (Ei)$,

Where R is the set of all obtained routes, Ii is the ith link, ni is the number of times that Ii appears in R, N is the total number of links in R, and Ei is the relative frequency that Ii appears in R. If $Emax > Pthreshold$, check the trust information available in the RREP of that route. If the value of correlation coefficient for packets dropped to that sent is greater than the pre-set threshold t, then the node is malicious, inform the operator. Then the operator detects which channel (link) is affected by the wormhole attack, and cut the route channel. And choose a fresh route to forwards the packet from source to destination. Else continue with routing process.

A Pseudo code for worm hole attack detection using Channel detection and cut defalconin

```
For all node I to n
IF BCST==RREQ
{
Update RT
Check RREQs
if {id} is in RT then discard
else if {id} not in RT then update RT
else if{id==destination id} then
end RT update
and deliver P(i)
else if {id==RT(i)id} then
initiate bcst
If again {id==RT(i)id} then
Terminate the connection
Remove RT entry
Call Neighbor ()
}
IF BCST==RREP
{
Check RREPs
if {id(RREQ)} is in RT then discard
else if {id(RREQ)} not in RT then update RT
else if{id==source id} then
update RT
and deliver A(i)
else if {RREQ(id)==RREQ[RT(i)id]} then
check if P(i) to P(n) is end
if end then remove RT entry
else repeat RT update
If again {RREQ[id]==RREQ[RT(i)id]} then
End BCST
Flush all RT entries
}

Neighbor ()
{
For all RT(i) assign Mac(i)
For(data 1 to n) check
If mac(i)!=mac(j) then
Add new_RT(j)
Else discard
For all neighbor (i) to neighbor (n)
Check if mac[pac(i)]!= mac[pac(j)] unless fragmented
Call neighbor() until pac(i) to pac(n) reached D(i) from S(i)
}
```

Where
BCST→ Broadcast
Pac→ packet
D→ Destination

S→ Source
RT(j)→ 'j'th routing table entry

Advantages of the Proposed Scheme:

- The proposed technique is very effective and efficient for secure data sharing among the source and destination.
- In this proposed scheme can easily detect the malicious node using behavior monitoring of the node and threshold value of the node compared to another algorithms.

Performance Evaluation

Simulation model was carried out using the NS-2 simulator. It is a useful research tool for achieving good simulation results. Mobility scenarios are generated by using a Random waypoint model by 50 nodes moving in a terrain area of 1340 x 640 . Each node independently repeats this behavior and mobility is changed by making each node stationary for a short period. The simulation parameters are summarized in Table 1.

Table 1. Simulation Parameters

Simulation and Network Parameters	
Network Area	1340 x 640
Protocol	DSR
No. of Mobile Nodes	50
Network Topology	Flat Grid
IEEE Standard	802.11
Broadcasting Range	550mts
Application Type	CBR/ FTP
Application rate	1.0mb
No. of Packets	1500
Simulation Time	10s

A. Result Analysis

The simulation results could be used to analyze the performance metrics of the network. The metrics are:
1) Packet Delivery Ratio: It depends upon the number of data packets that have been received successfully at the destination among the N number of data packets generated at the source.
2) Average End-to-End delay: Delay is the time taken for a packet to reach the destination after it has been relieved from the source. It includes all end hop time, wait time, queuing time, regeneration time and segmentation time between source and destination.

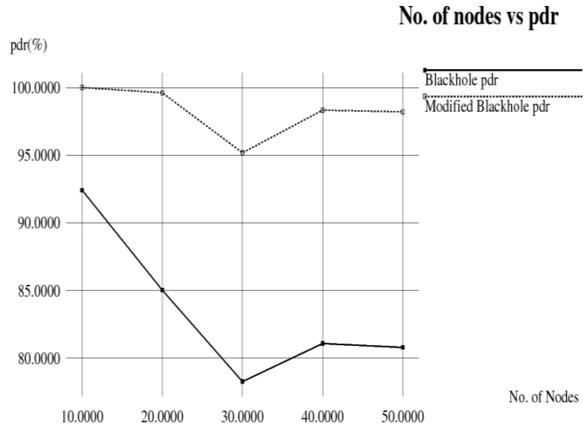

Fig. 5.a Number of nodes Vs packet delivery ratio

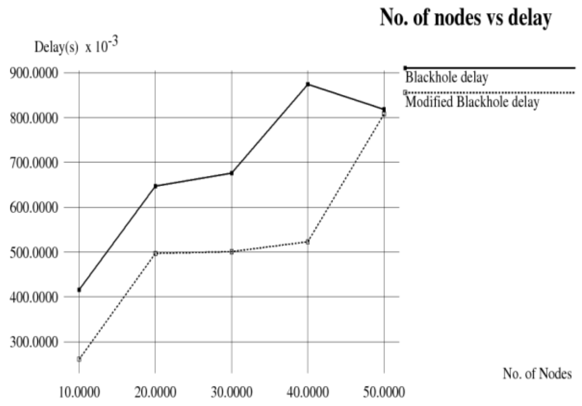

Fig. 5.b Number of nodes Vs Delay

In Fig.5.a shows the packet delivery ratio of black hole attacked DSR and secured DSR with a proposed Anomaly based behavior monitoring scheme. In this scenario with 50 mobile nodes, operated at a constant CBR/FTP, for a throughput of 1500 packets, in attacked DSR protocol the delivery ratio is found to be 88% and in secured DSR protocol the delivery ratio is found to be 99%. Table 2 shows the performance results with five topologies such as 10, 20, 30, 40 and 50 respectively and percentage increase in PDR by launching Anomaly based behavior monitoring scheme with varying number of nodes. In fig. 5.b shows end-to-end delay increases if the number of packets in the network is increased. In attacked DSR protocol the delay is found to be 61% and in secured DSR protocol the delay is found to be 54%. Table 3 shows the decrease in delay with Anomaly based behavior monitoring scheme

Table.2. Packet delivery ratio in Percentage

Number of nodes	Blackhole Attacked DSR (pdr %)	Modified DSRwith solution (pdr%)
10	92.4124	100
20	85.0176	99.6168
30	78.2541	95.1742
40	81.0706	98.3333
50	80.7748	98.2035

Table.3 End to end delay in sec

Number of nodes	Blackhole attacked DSR (end to end delay in seconds)	Modified DSR with Solution (end to end delay in seconds)
10	0.426	0.252
20	0.667	0.459
30	0.676	0.493
40	0.774	0.516
50	0.811	0.796

In Fig. 6.a shows the packet delivery ratio of worm hole attacked DSR and secured DSR with a proposed Channel detection and cut defalconin scheme. In this scenario with 50 mobile nodes, operated at a constant CBR/FTP, for a throughput of 1500 packets, in an attacked DSR protocol the delivery ratio is found to be 62% and in secured DSR protocol the delivery ratio is found to be 89%. Table 4 shows the percentage increase in PDR by launching Channel detection and cut defalconin scheme. In fig. 6.b compares the number of nodes and End to end delay. In an attacked DSR protocol the delay is found to be 63% and in secured DSR protocol the delay is found to be 49%. Table 5 shows the decrease in delay with Channel detection and cut defalconin scheme.

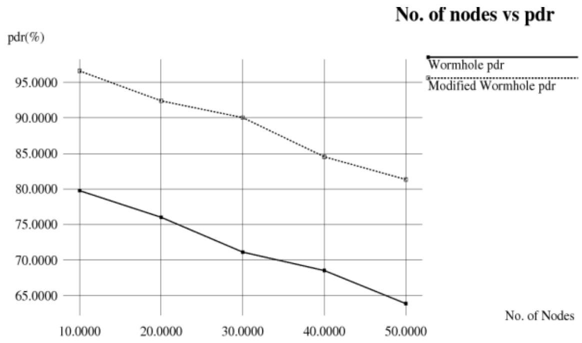

Fig. 6.a Number of nodes Vs packet delivery ratio

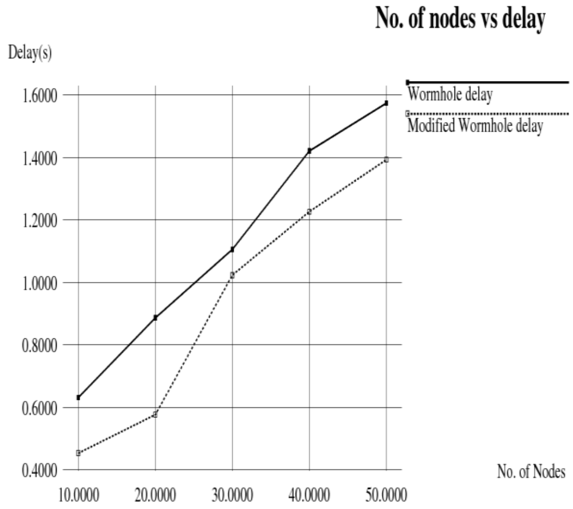

Fig. 6.b Number of nodes Vs Delay

Table 4. Packet delivery ratio in Percentage

Number of nodes	Worm attacked DSR(pdr %)	Modified DSRwith solution(pdr%)
10	79.7574	96.6142
20	76.0062	92.3974
30	71.1014	90.0420
40	68.5085	84.5242
50	63.8417	81.3314

Table 5. End to end delay in seconds

Number of nodes	Wormhole Attacked DSR(end to end delay in seconds)	Modified DSR with solution(end to end delay in seconds)
10	0.632	0.454
20	0.887	0.577
30	1.106	1.024
40	1.421	1.227
50	1.574	1.393

Conclusion

Black hole attack and Worm hole attack are the most important attacks in MANET, while communication between a source node and a destination node. In this paper, effect of these attacks on the network were analyzed on the basis of packets received, delay, throughout and packet delivery ratio. Then proposed algorithm was used in order to secure the network from these attacks. Finally, the comparison of the attacked DSR and secured DSR was done considering again the same four parameters packets received, end-to-end delay, throughput, and packet delivery ratio. It is clear from the results that the proposed techniques are very effective in securing the network from the black hole and wormhole attacks.

References

[1] X. Xiang and X. Wang. An Efficient Geographic Multicast Protocol for Mobile Ad HocNetworks. In IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), Niagara-Falls, Buffalo, New York, June 2006.

[2] C Sreedhar, Dr. S. Madhusudhana Verma, Dr. N. Kasiviswanath, “Potential Security Attacks on Wireless Networks and their Countermeasures”, In IJCSIT, Vol.02, No. 05.

[3] A. Martin, J. Smith, and M. Koethe, “A Platform Independent Model and Threat Analysis for Mobile Ad hoc Networks”, proc. of the 2007 Software Defined Radio Technical Conference, Denver, Colorado, Nov. 2007.

[4] M. A. Shurman, S. M. Yoo, and S. Park, “Black hole attack in wireless ad hoc networks,” in ACM 42nd Southeast Conference (ACMSE’04), pp. 96-97, Apr. 2004.

[5] D. Johnson and D. Maltz, Dynamic Source Routing in Ad Hoc Wireless Networks, Kluwer Academic Publisher, 1996.

[6]Tamilselvan, L. Sankaranarayanan, V. “Prevention of Blackhole Attack in MANET”, JournalOfNetworks ,Vol.3,No.5,May2008.

[7] Rutvij H. Jhaveri , Sankita J. Patel. (2012). DoS Attacks in Mobile Ad-hoc Networks: A Survey. 2012 Second International Conference on Advanced Computing & Communication Technologies. 2 (2), p535-540.

[8] Kuldeep Sharma**,** Dr.G.Mahadevan, “Advance Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANET”, Int. J. on Recent Trends in Engineering & Technology, Vol. 05, No. 01, Mar 2011.

[9] Y. C. Hu, A. Perrig, and D. Johnson, “Packet leashes: a defense against wormhole attacks in wireless networks,” in INFOCOM, 2003.

[10] I.Khalil, S.Bagchi, N.B.Shroff, “A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks”, In Proceedings of the 2005 International Conference on Dependable Systems and Networks (DSN‟ 05).

[11] David B. Jhonson ,David A.Maltz and Josh Broch „ DSR:The Dynamic Secure Routing protocol for Multi-Hop Wireless Adhoc Networks.http://www.monarch.cs.cmu.edu.

[12] Piyush Agrawal, R. K. Ghosh, Sajal K. Das, Cooperative Black hole attack in Mobile Ad Hoc Networks In Proceedings of the 2nd international conference on Ubiquitous information
management and communication, Pages 310-314, Suwon, Korea, 2008.

[13]. Ritesh Maheshwari, Jie Gao, Samir R Das, "Detecting Wormhole Attacks in Wireless Networks using Connectivity Information”, in IEEE INFOCOM 2007, Alaska.