ISSN 2278-5612

Black hole Attack Detection in AODV-BTR MANET

[1]Bhavana Gupta, [2]Vikas Jian,[3]Rajesh Tiwari
Corporate Institute of science & Technology, Bhopal
[1]bhavana_nishi@yahoo.co.in
Corporate Institute of science & Technology, Bhopal
[2]vikasjain.cse@gmail.com
Corporate Institute of science & Technology, Bhopal
[3]trajesh.engg@gmail.com

ABSTRACT

Security is a vital requirement in mobile ad hoc networks to provide secured communication among mobile nodes. Due to different characteristics of MANETS, it creates a number of consequential challenges to its security design. To overcome the challenges, there is a need to build a powerful security solution that achieves both broad protection and desirable network performance.

Mobile Ad hoc Network (MANET) has emerged as a new leading edge of technology to provide communication wherever and whenever required. As the wired network needs established infrastructure for communication but the mobile ad hoc network does not need any infrastructure, centralized management and control. Due to movable nature of nodes in Mobile ad hoc network difficult routing between nodes are not very easy task. For this purpose many reactive routing protocols have been implemented like AODV, DSR, and DSDV. In the first part of this work, we propose a new algorithm AODV-BTR to improve existing on demand routing protocol and an attempt has been made to compare the performance of proposed algorithm (AODV-BTR) with existing algorithm AODV. Ad hoc networks are susceptible to many types of attacks; due to movable nature of nodes it is very difficult to provide security at each node. This paper introduces the black hole attack; in this type of attack mischievous node announce that he is having the shortest path to all nodes in the environment by sending fake route reply message. This paper proposes an easiest way to detect Black hole attacks using DLM technique. DML method presents the solution to detect & remove blackhole attack in reactive protocol called AODV-BTR.

Keywords -Mobile Ad hoc Network, AODV, Black hole Attack, Routing protocol.

ISSN 2278-5612

I. INTRODUCTION

Mobile Ad hoc network is a self configuring network where nodes communicate with each other via wireless equipment and nodes in Mobile Ad hoc network form their own network. In Mobile Ad hoc network change in topology is very frequent and no condensed monitoring is there. Each node work as host and a router to participate in the routing and forward packets to the others.

Existing internet routing protocol were designed to support fixed infrastructure and their properties are unsuitable for mobile ad hoc networks due to this fact routing protocol in Ad hoc networks has received wide interest in the past year. The routing protocols in Mobile Ad hoc network protocols are classified into reactive and proactive protocols. Reactive protocols, like DSR [1] and AODV [2], TORA, ABR, find path to the node only when there is need of data transmission. Proactive protocols or table driven protocol on the other hand, find route in advance for all the nodes (source and destination) pairs and exchange topology information time by time to maintain the route information.

I (a) AODV (Ad hoc on demand distance vector routing)

One of the reactive routing protocols that minimize the number of broadcasts by creating routes on demand is AODV. In AODV discovery of routes is done through a route discovery process, whereby the network nodes are queried in search of a route to the destination node. When route to that particular node a node or destination is discovered, that route is reported back to the source node that requested the route.

I (b) DSR (Distance Vector Routing)

DSR is also reactive routing protocol. It is a source routed on demand routing protocol. A node maintains route cache containing the source route that it is aware of and update entries in the route cache as and when it learn about new routes.

In this paper, we proposed modifications to AODV called AODV-BTR works in case of Link breakage or congestion control. The conservative nature of proposed protocol helps to find route in case of link failure and network congestion, while maintains better performance in case of delay and network load like application oriented metrics. In the first part of work, small modification is done in AODV Algorithm.

In the second part, black hole attack is detected on AODV-**BTR**. In this attack a mischievous node announces that it has the shortest path to the node whose packets it wants to intercept.

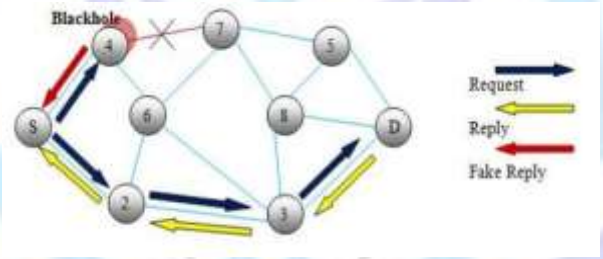

Fig 1: Black hole Attack

In figure 1, in this attack, a malicious node sends a forged Route REPly (RREP) packet to a source node that initiates the route discovery in order to pretend to be a destination node.

This paper describes black hole attack. In this type of attacks a false link is advertised between attacker nodes themselves. The rest of the paper is organized in this manner.

Section II presented the literature survey on existing AODV and detection against Black hole attack. Section III defines the Proposed Method. Section IV presented the analysis of Result. The Section V concludes the paper.

2. LITERATURE SURVEY

Previous and recent Researchers proposed AODV using the concept of link-disjoint multipath routing approach, reliable distance; distance vector and source initiated routing approach. Most approaches are based on path accumulation during the route discovery process. And lots of existing researchers examined the problem of detecting internal & external black hole attacks. Some proposals based on clock synchronization and wireless equipment's abilities such as GPS.

Johnson and Maltz (1996) used a source routing approach in which the source node explicitly designates in the header of data packet the route to the destination. Routes are access by records of those paths in RREQ messages and returning the paths in RREP messages (DSR) [1].

Perkins and Royer (1999) shown that AODV is based on a traditional distance vector routing mechanism. In Distance vector routing protocol[2] route is determined on the hop by hop basis .The route is established by leaving a inverted route to the source at midway nodes when RREQ messages are raised and by leaving a forward route to the destination at midway nodes when delivered the RREP message to the source.

Das et. al.(2001) compared performance of DSR and AODV, two prominent on routing protocols for ad hoc networks [3]. They analyze their performance comparisons using varying network load, mobility and network size. They showed that the resultant DSR as compared to AODV generates less routing load. In case of smaller number of nodes and load and/or mobility DSR performs.

Mesut Gunes et. al. (2002) presented the approach that is based ant colony optimization meta-heuristic and swarm intelligence. Author shows that their algorithms are applied for mathematical problems and successfully to several optimization problems in [4].

Gwalani and Belding-Royer (2003) presented a new approach called AODV-PA [5] that incorporates path accumulation to attain extra routing information during the route discovery process in AODV. And it scales better in the large networks It is proved from the results that their approach (AODV-PA) polishes the performance of AODV under conditions of high load and moderate to high mobility. Author says that their improved protocol (AODV-PA) can be used either as an substitute to AODV or as an optimization in scenarios where load varying moderate to high.

Qiang and Hongbo (2008) propose an optimized AODV (OAODV) [6] using the concept of reliable distance that is depended on the nodes velocity and direction information and always smaller than transmission range, The new protocol delimit the area of flooding RREQ in route discovery process. They proved that by using their mechanism route finding is more reliable and better than normal AODV. They had also compared the performance of their algorithm (OAODV) with existing AODV.

Zahary and Ayesh (2008) presented the thought of ORMAD [7]. This concept is based on a link-disjoint multipath routing approach and by this concept routing overhead of both Route Discovery Process (RDP) and Route Maintenance Process (RMP) of multipath extension to AODV is optimized. When link failure is detected in the primary route, ORMAD calls a procedure called local repair procedure that works between the upstream and the downstream nodes. Using RMP is method routing overhead is minimized with route efficiency.

Sethi and Udgata (2010) propose an Optimized Reliable Ad hoc On-demand Distance Vector (ORAODV) scheme that provide quick approbation to dynamic link conditions. They adopted a mechanism for retransmission of data packet which was not delivered with Blocking ERS technique to enable optimal path routing and fast route discovery with an improvement of PDR. They show that their protocol works in large network and perform well in real time communication for high network density and high node mobility [8].

Elson et. al. (2002) analyzed a form of time synchronization method called Reference Broadcast Synchronization. Reference Broadcast synchronization algorithm is more precise, flexible, and resource-efficient technique to synchronize nodes in the network. The important property of author's design is that it synchronizes a set of receivers with one another, as opposed to traditional protocols in which senders synchronize with receivers [9].

Tamilselvan et.al (2008) presented an approach of "Fidelity table "to combat the Black hole attack in Mobile Ad hoc network. In this method to measure reliability of node every participating node will be assigned a fidelity levels. In case the any node level drops to 0, it is assumed to be a mischievous node, tagged as a 'Black hole' and is eliminated [10].

Tseng et.al. (2011) shows their survey of existing solutions and discuss the state-of-the-art routing methods. They worked on single black hole attack and collaborative black hole attack and also analyze the solutions in these two categories and provide a comparison table. They also recommend their future scope of their work with combing the advantages of proactive routing & reactive routing to make a hybrid detection method. However, we also discover that the attacker's misbehavior action is the key factor [11]

Sowmya. et.al (2012) proposed a method to detect and prevent black hole attacks. Their protocol not only prevents black hole attack but consequently improves the overall performance of (normal) ACO even though the black hole attack is present in their network. Their prevention scheme detects the mischievous nodes and removes it from the data forwarding and routing and reacts by sending ALARM packet to its neighbors [12].

Hafizpour et. al. (2013) presents a technique to prevent the Black hole attack. In this Author implementing negotiation with neighbors who pretense route maintaintenance to destination. Negotiation process is strengthening by apriori method to judge about mischievous node. Apriori algorithm is a low complexity algorithm based on association rule mining method, which is proper for MANETs [13].

Sharma, Ashish, et al.(2014) In this paper Author presented the protocol named TAODV is a secure routing protocol based on trust model for mobile ad-hoc network. TAODV routing protocol approach is used to focus on analyzing and improving the security of Black hole in AODV routing protocol. The metrics, throughputs and packet delivery ratio, energy are used to determine the performance of AODV, AODV affected with black hole attack and Trusted AODV [14].

Gupta, Nidhi et.al.(2014) analyzed different kinds of the routing methods and solutions for detection and prevention of black hole attack .they also presented the comparison table for analyzing all the methods [15].

3. PROPOSED METHOD

3.1 AODV-BTR (Ad hoc on demand distance vector routing with backup temporary route)

AODV-BTR is based on reactive routing. The route discovery (Route Request and Route Reply) process of AODV-BTR is similar to the AODV protocol. We slightly change the AODV protocol by establishing temporary route feature in case of link failure and congestion control. Here we assume the nodes follows completely connected structure.

(i) Creation of route: In the route discovery process sender node searches a route by flooding a RREQ packet. A middle node, upon receiving a non-duplicate RREQ, records the previous hop and the source node information in its route table. It then broadcasts the packet or sends back a Route Reply (RREP) packet to the source if it has a route to the destination.

Temporary path are established during the route reply phase. Because of the broadcast nature of Mobile Ad hoc network, a node constantly "overhears" packets that are transmitted by their neighboring nodes. From these packets, a node obtains temporary route information. When a node that is not part of the route overhears a RREP packet not directed to itself transmit by a neighbor it records that neighbor as the next hop to the destination in its **alternate route table.** A node may receive numerous RREPs for the same route if the node is within the radio propagation range of more than one intermediate node ofthe primary route. In this way the source node also selects the best route to send the packet to the destination.

(ii) Maintain Route: Initially data packets are send via the main route if there is no link disconnection. When a node detects a link failure, it accomplishes a one hop data broadcast to its adjacent neighbors. The node specifies in the data header that the link is not connected and thus the packet is candidate for temporary path. Upon receiving this packet, neighbor nodes that have an entry for the destination in their alternate route table, unicast the packet to their next hop node. Data packets therefore can be passed through one or more alternate routes and are not dropped. When any node receive data packet from the temporary path its check the packet ID to prevent from duplicate copy and operate normally and send packet to the next hop. The node that detected the link failure also sends a ROUTE ERROR (RERR) packet to the source to start a salvage route rediscovery.

Example: Figure 2 shows the temporary path construction in case of link failure.

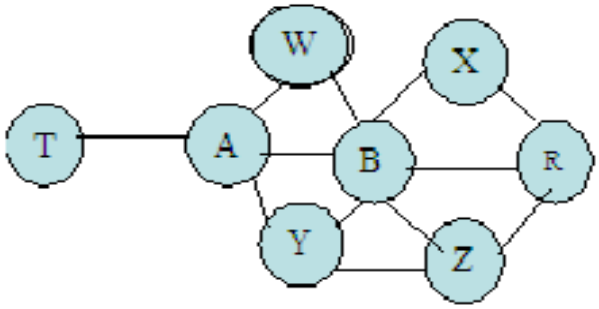

Fig 2: Backup Temporary route construction

When the route request packet reaches the destination R then the main route < T-A-B-R > is selected. The destination node R send route reply packet to node B. the node X and Z is in the communication range of R overhear the packet and change the alternate routing table accordingly. After receiving this RREP packet, only node B relaying the packet to node A since it is in the main route. Nodes W and Y record node B as the next hop to the destination R in their alternate route table. Finally node A send RREP packet to the Source node T.

Now suppose Source node T wants to send data packet to the destination node R and the node B is moved out from the transmission range of A. After receiving the data packet from node T node A forward it to node B. The packet will fail to deliver because node B is not in the communication range of node A, then node A broadcast the packet to its neighbor (W and Y) for temporary route. Node W and Y identify the main route disconnection by reading the packet header. And looks up in its alternate route table and finds the path to the destination. Therefore the packet is delivered through the path < T-A-Y-Z-R>.

3.2 Black hole attack:

In an ad-hoc network that uses the AODV protocol, a black hole node pretends to have fresh enough routes to all destinations requested by all the nodes and absorbs the network traffic. When a source node broadcasts the RREQ message for any destination, the black hole node immediately responds with an RREP message that includes the highest sequence number and this message is perceived as if it is coming from the destination or from a node which has a fresh enough route to the destination. The source node then starts to send out its data packets to the black hole trusting that these packets will reach the destination.

ISSN 2278-5612

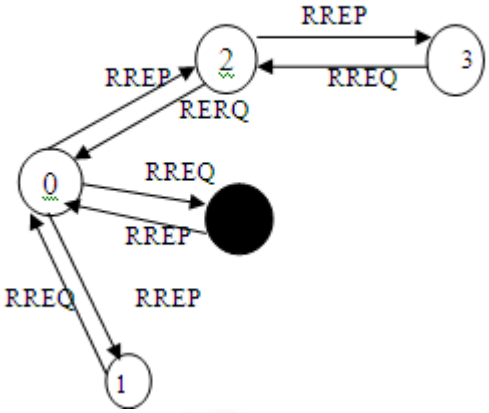

Fig 3: RREQ Broadcast

A malicious node sends RREP messages without checking its routing table for a fresh route to a destination. As shown in fig.3, source node 0 broadcasts an RREQ message to discover a route for sending packets to destination node 2. An RREQ broadcast from node 0 is received by neighboring nodes 1, 3 and 4. However, malicious node 4 sends an RREP message immediately without even having a route to destination node 2. An RREP message from a malicious node is the first to arrive at a source node. Hence, a source node updates its routing table for the new route to the particular destination node and discards any RREP message from other neighboring nodes even from an actual destination node. Once a source node saves a route, it starts sending buffered data packets to a malicious node hoping they will be forwarded to a destination node. A malicious node drops all data packets rather than forwarding them on.

4. Distance Learning method:

In order to detect this attack, the destination sequence number is taken into account. In normal state, each node's sequence number changes depending on its traffic conditions. When the number of connections increases the destination sequence number tends to rise, when there are few connections it tends to be increased monotonically. However, when the attack took place, regardless of the environment the sequence number is increased largely. Also, usually the number of sent out RREQ and the number of received RREP is almost the same. From these reasons we use the following features to express the state of the network.

(i)Number of sent out RREQ messages

(ii)Number of received RREP messages

(iii)The average of difference of DstSeq in each time slot between the sequence number of RREP message and the one held in the list.

Here, the average of the difference between the DstSeq in RREQ message and the one held in the list are calculated as follows. When sending or forwarding a RREQ message, each node records the destination IP address and the DstSeq in its list. When a RREP message is received, the node looks over the list to see if there is a same destination IP address. If it does exist, the difference of DstSeq is calculated, and this operation is executed for every received RREP message. The average of this difference is finally calculated for each time slot as the feature.

Steps of Applying DLM

1. Make the groups of normal states are considered to be gathered close in feature space In contrast, the abnormal state is considered to be the scattering data that deviates from the cluster of normal state.

2. Calculate the mean vector $\bar{x}^{D}$

D= training data set

N=time slot

$$\bar{x}^{D} = \frac{1}{N}\sum_{i=1}^{N} x_i \qquad (1)$$

3. Now calculate the distance from input data sample x to mean vector $\bar{x}^{D}$

$$d(x) = \| x - \bar{x}^{D} \|^2 \qquad (2)$$

When the distance is larger than the threshold T_h (out of range of normal traffic), it will be judge as an attack.

$$\begin{cases} d(x) > T_h : Attack \\ d(x) \le T_h : Normal \end{cases} \quad (3)$$

Let ΔT_0 be the first time interval for a node participating in MANET. By using data collected in this time interval, the initial mean vector is calculated, then the calculated mean vector will be used to detect the attack in the next period time interval ΔT.If the state in ΔT is judged as normal, then the corresponding data set will be used as learning data set. Otherwise, it will be treated as data including attack and it will be consequently discarded. This way, we keep on learning the normal state of network. The procedure is shown in Figure 4.

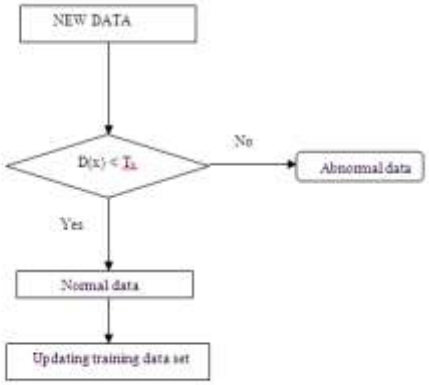

Fig 4: Flow chart of Distance learning method

By doing this, we update the training data set to be used for the next detection. Then, the mean vector which is calculated from this training data set is used for detection of the next data. By repeating this for every time interval ΔT, we can perform anomaly detection which can adapt to MANET environments.

5. RESULT ANALYSIS

The NS-2 network simulator was used to create a simulation environment to develop and analyze the proposed protocol (AODV-BTR).The node mobility is expressed by the pause time. We performed simulations with 6 different pause times 10, 25, 45, 65, 80, 95 seconds. In the cases of 0 seconds pause time, the nodes move constantly.

As mentioned in the introduction our main goal was to reduce the routing overhead. And increase the packet delivery rate. So we will mainly discuss this aspect of AODV-BTR.The parameters are similar to those in [6].The mobility model uses the random waypoint model. In the random waypoint mobility model, each mobile node begins at a random location and moves independently during the simulation.

Performance Metrics

The following metrics are used in varying scenarios to evaluate the different protocols:

1) **Packet delivery rate** - $\frac{\text{Data packets received}}{\text{Data packets originated.}}$

2) **Normalized load** - $\frac{\text{Routing messages transmitted}}{\text{Data packets received.}}$

4) **Routing load -** Routing load gives a measure routing overhead of the protocol. This is the ratio of overhead bytes to delivered data bytes.

5.1Comparison with existing routing algorithms

A new routing algorithm should show its performance in comparison with existing and known algorithms. We take simulation on 100 nodes.

Figure 5(a) exhibits the simulation results of two protocols AODV, and AODV-BTR based on parameter packet delivery rate on 100 nodes. AODV-BTR performs better because node become more stationary will lead to more stable path from source node to destination node. AODV performance dropped as number of nodes increase because more packets dropped due to link breaks.

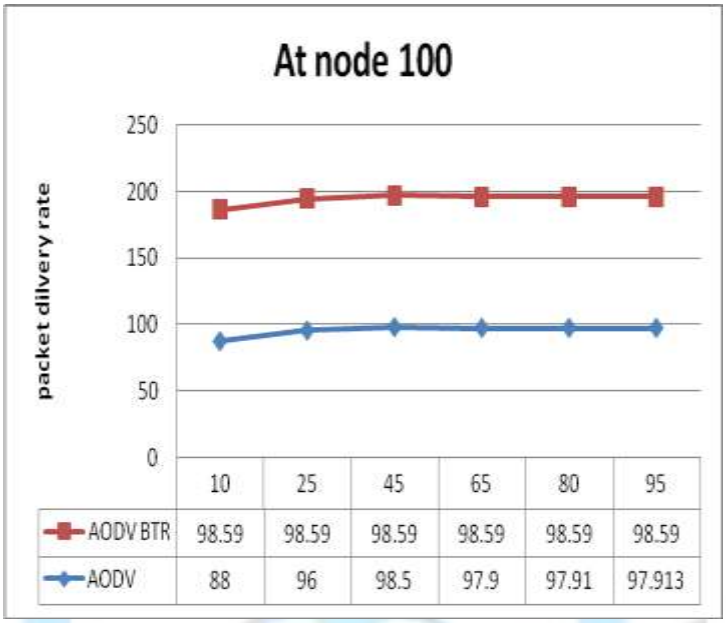

Fig 5 (a): Comparison of two protocols by the fraction of successful delivered packets as a Function of pause time

Above figure also shows Packet delivery rate, i.e., the part of packets a certain routing protocol was able to deliver properly. In the case with low pause time, i.e., high topology changes, only AODV and AODV- BTR are able to deliver more than 95% of the sent packets. In situations with very high dynamics AODV- BTR shows the best performance followed by AODV. With less dynamic, up to 45 seconds of pause time, AODV is very close to AODV- BTR.

Figure 5(b) exhibits the simulation results of three protocols AODV, DSR and AODV-BTR based on parameter Routing overhead on 100 nodes.AODV-BTR exhibits a flexible property on routing overhead.AODV is almost close to each other but AODV-BTR is slightly better than both when pause time increases.

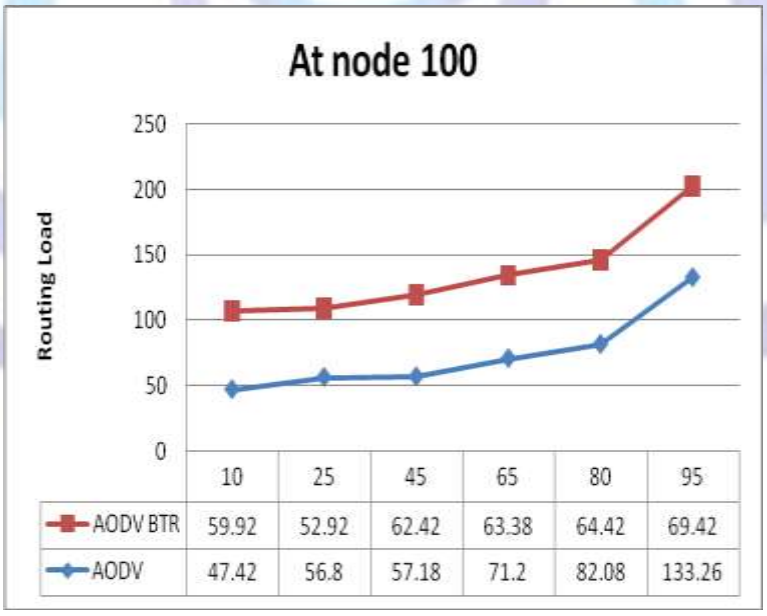

Fig 5 (b): Comparison of two protocols based on Routing Load (the number of needed routing packets)

Figure 5(b) also shows the fraction of routing packets needed to deliver a data packet. We counted bits used for routing, because the different protocols generate the overhead in very different ways. Here AODV-BTR shows its advantage. In the case of 0 - 50 seconds of pause time, it generates the least overhead. At pause time 65-95 the generated overhead stabilizes and is very high for the whole simulation time. In cases with pause time of 65-95 seconds AODV is very close in generating overhead. AODV-BTR generates less overhead than AODV but the difference is small. So AODV- BTR is highly efficient.

Figure 5(c) exhibits the simulation results of three protocols AODV and AODV-BTR based on parameter Normalized routing load on 100 nodes. It has been seen from the table that AODV-BTR provides less Normalized load as compare to AODV.

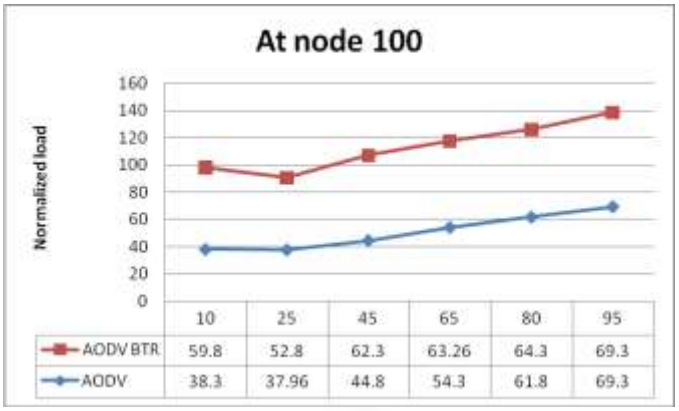

Fig 5(c): Comparison of two protocols based on Normalized Load

It can be seen from Figure 5(c) that the difference in Normalized routing load between AODV-BTR, AODV increases slowly with the increase in velocity. As the velocity increases, a larger percentage of nodes come within the range of each other, and the network topology information is quickly distributed. In all the cases AODV-BTR has lower Normalized load when compare with both the protocol. Relative to AODV's the Normalized routing load of AODV-BTR is fairly stable with increasing number of sources. A relatively stable Normalized routing load is a desirable property for scalability of the protocols, as this indicates the actual routing load increases linearly with the number of sources.

In the second part of the work the Black hole is detected by using DLM technique.

Table 1.1. Effect of Black hole Attack on AODV-BTR based on parameter Packet Delivery rate

No. of Nodes	50				
Pause Time	25	45	65	80	95
AODV-TP with Black hole Attack	97.6	97.42	97.6	97.06	97.92
AODV-TP without Black hole Attack	98.5	98.58	98.58	98.5	98.58

Table 1.1 shows the simulation result of protocol AODV-BTR in two cases (i) with Black hole attack (ii) without Black hole attack based on parameter Packet Delivery rate.

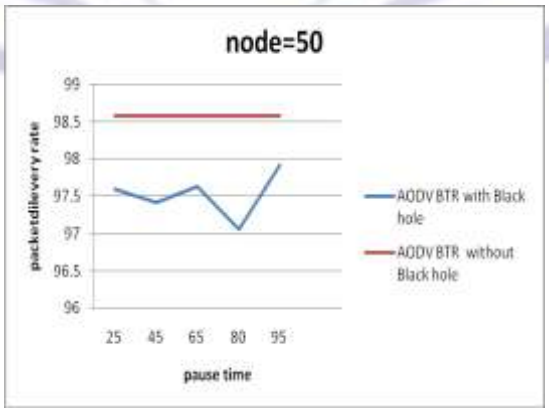

Fig 6: Effect of Black hole attack on Packet Delivery Rate

Figure 6 illustrates the graph of 50 nodes. At the time of wormhole attack detection the packet delivery rate is decreases to 97% while before the wormhole attack the packet delivery rate was 98.5% at 50 nodes.

6. CONCLUSION

As the popularity of mobile ad hoc networks (MANET) has increased manifolds, the security in MANETs has become of vital importance.

In this paper we presented a new on-demand routing approach AODV-BTR for mobile multi-hop ad hoc networks. The approach is based on providing Backup temporary Route in case of network congestion and Link failure condition. And the approach shows its ability to perform well in networks where mobility is high.

In this work, the basis analysis is on black hole attack and introduced the feature in order to define the normal state of the network. We have presented a new detection method based on dynamically updated training data. Detection by using DLM method is very well-organized and easy. In future, the experiments can be further extended for investigations with high network load and multimedia data.

REFERENCES

[1] D. B. Johnson and D. A. Maltz, “Dynamic Source Routing in Ad Hoc Wireless Networks,” in Mobile Computing, Academic Publishers, 1996, pp 153-181.

[2] C. E. Perkins and E. M. Royer, “Ad hoc On-Demand Distance Vector Routing,” in Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA, February 1999, pp. 90–100.

[3] S. R. Das, C. E. Perkins, E. M. Royer, and M. K. Marina, “Performance Comparison of Two On-Demand Routing Protocols for Ad Hoc Networks”, in IEEE Personal Communications Magazine special issue on Ad hoc Networking, February 2001,Vol 8,pp. 16–28.

[4] Mesut Gunes,,Udo Sorges, Imed Bouazizi, **“**ARA -The Ant-Colony Based Routing Algorithm for MANETs”,.International Workshop on Ad Hoc Networking (IWAHN 2002), Ancouver, British Columbia, Canada, August 18-21,pp79-85, 2002

[5] S.Gwalani,E.M. Belding-Royer, C.E. Perkins, “AODV-PA: AODV with path accumulation”, in Proceedings of the IEEE Symposium on Next Generation Internet (NGI), Anchorage, AK, May 2003,Vol 1,pp. 527-531.

[6] Zhao Qiang Zhu Hongbo, “An optimized AODV protocol in mobile ad hoc Network”, in Wireless comm. networking &mobile computing 2008(WiCOM’08), 4th international conference on Oct 12-14, 2008, pp.1-4.

[7] Ammar Zahary and Aladdin Ayesh,“On-demand Multiple Route Maintenance in AODV”,in Computer Engineering &System, 2008, International Conference on Nov 25-27 , 2008, pp. 225-230.

[8] Sung-Ju Lee and Mario Gerla, “AODV-BR: Backup Routing in Mobile Ad hoc Networks”, Proceeding of IEEE WCNC, 6 Aug 2000, Vol 3, pp.1311-1316.

[9] J.Elson, L.Girod, D.Estrin, “Fine–Grained Network Time Synchronization using Reference Broadcasts”,Proc.Fifth Symposium on Operating Systems Design and Implementation (OSDI 2002), Vol 36, pp.147-163, 2002.

[10] Tamilselvan, Latha, and V. Sankaranarayanan. "Prevention of co-operative black hole attack in MANET." Journal of networks 3.5 (2008): 13-20 .

[11] Tseng, Fan-Hsun, Li-Der Chou, and Han-Chieh Chao. "A survey of black hole attacks in wireless mobile ad hoc networks." Human-centric Computing and Information Sciences 1.1 (2011): 1-16.

[12] Sowmya, K. S., T. Rakesh, and P. Hudedagaddi Deepthi. "Detection and Prevention of Blackhole Attack in MANET Using ACO." International Journal of Computer Science and Network Security 12.5 (2012): 21-24.

[13] L.Qian , N.Song ,X .Li, “Detecting and Locating Wormhole Attacks in Wireless Ad Hoc Networks through Statistical Analysis of Multi-path”, Proc.IEEE WCNC, New Orleans, LA, USA,Vol 4,pp 2106-2111,March 2005.

[14] Hafizpour, Hadis, and S. Mirabedini. "Using Apriori algorithm to prevent black hole attack in mobile Ad hoc networks." Management Science Letters 3.1 (2013): 351-358.

[15] Sharma, Ashish, et al. "Prevention of Black Hole Attack in AODV Routing Algorithm of MANET Using Trust Based Computing." International Journal of Computer Science & Information Technologies 5.4 (2014).

[16] Gupta, Nidhi, Sanjoy Das, and Khushal Singh. "A Comprehensive Survey and Comparative Analysis of Black Hole Attack in Mobile Ad Hoc Network." International Journal of Computer, Information, Mechatronics, Systems science and Engineering 8.1 (2014).

[17] Y. A. Huang and W. Lee, “Attack analysis and detection for ad hoc routing protocols,” in The 7th International Symposium on Recent Advances in Intrusion Detection (RAID’04), pp. 125-145, French Riviera, Sept. 2004

[18]S.Sethi, S. K. Udgata, “Optimized and Reliable AODV for MANET”, International Journal of Computer Application, Vol 3, No. 10, July 2010.

[19] Kurosawa, Satoshi, et al. "Detecting Black hole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method." *IJ Network Security* 5.3 (2007): 338-346.

[20]Kurosawa, Satoshi, et al. "Detecting Black hole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method." *IJ Network Security* 5.3 (2007): 338-346.

[21] Network Simulator-2 http://www.isi.edu/nsnam/ns/accessed on 1 April 2004.control (ICNSC),Chicago, April 10-12, pp.366-371,2010.