© 2015 IJSRSET | Volume 1 | Issue 6 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Recognition and Removal of Black Hole Attack for Secure Communication in MANETs

S. Rakesh Kumar, N. Gayathri, T. Manikandan
Computer Science and Engineering, Thiagarajar College of Engineering, Madurai, Tamilnadu, 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 (MANETs). Black hole attack is one of the security threat in which the traffic is redirected to such a node that actually does not exist in the network. It's an analogy to the black hole in the universe in which things disappear. The node presents itself in such a way to the node that it can attack other nodes and networks knowing that it has the shortest path. MANETs must have a secure way for transmission and communication which is quite challenging and vital issue. In order to provide secure communication and transmission, researcher worked specifically on the security issues in MANETs, and many secure routing protocols and security measures within the networks were proposed. Previously the works done on security issues in MANETs were based on reactive routing protocol like Ad-Hoc On-demand Distance Vector (AODV) and Dynamic Source Routing (DSR). Different kinds of attacks were studied, and their effects were elaborated by stating how these attacks disrupt the performance of MANETs. The scope of this paper is to develop a technique to identify Black Hole Attack and then removal of Black Hole Attack in Mobile Ad-hoc Networks (MANETs). Simulation is done with Network Simulator (NS2).

Keywords: Black Hole, MANETs, Routing Protocols, NS

I. INTRODUCTION

Mobile Ad-hoc Networks are autonomous and decentralized wireless systems. MANETs consist of mobile nodes that are free in moving in and out in the network. Nodes are the systems or devices i.e. mobile phone, laptop, personal digital assistance, MP3 player. These nodes can act as host/router or both at the same time. They can form arbitrary topologies depending on their connectivity with each other in the network. These nodes have the ability to configure themselves and because of their self configuration ability, they can be deployed urgently without the need of any infrastructure. Internet Engineering Task Force (IETF) has MANETs working group that is devoted for developing IP routing protocols. Routing protocols is one of the challenging and interesting research areas. Many routing protocols have been developed for MANETS, i.e., AODV, OLSR, DSR, ZRP etc. Security in Mobile Ad-hoc Network is the most important concern for the basic functionality of network. The availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met. MANETs often suffer from security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. These factors have changed the battle field situation for the MANETs against the security threats. The MANETs work without a centralized administration where the nodes communicate with each other on the basis of mutual trust. This characteristic makes MANETs more vulnerable to be exploited by an attacker inside the network. Wireless links also makes the MANETs more susceptible to attacks, which make it easier for the attacker to go inside the network and get access to the ongoing communication [1], [2]. Mobile nodes present within the

range of wireless link can overhear and even participate in the network. MANETs must have a secure way for transmission and communication and this is a quite challenging and vital issue as there is increasing threats of attack on the Mobile Networks. Security is the cry of the day. In order to provide secure communication and transmission, the engineers must understand different types of attacks and their effects on the MANETs. Wormhole attack, Black hole attack, Sybil attack, flooding attack, routing table overflow attack, Denial of Service (DoS), selfish node misbehaving, impersonation attack are kind of attacks that MANETs can suffer from. MANETs is more open to these kinds of attacks because communication is based on mutual trust between the nodes, there is no central point for network management, no authorization facility, vigorously changing topology and limited resources.

II. METHODS AND MATERIAL

A. Black Hole Attack

In black hole attack [3], [4] a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept. This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it [2]. In protocol based on flooding, the malicious node reply will be received by the requesting node before the reception of reply from actual node; hence a malicious and forged route is created. When this route is establish, now it's up to the node whether to drop all the packets or forward it to the unknown address [5].

Black hole Attacks are classified into two categories:- Single Black Hole Attack [6], [7] In Single Black Hole Attack only one node acts as malicious node within a zone. It is also known as Black Hole Attack with single malicious node. Collaborative Black Hole Attack [8], [9] In Collaborative Black Hole Attack multiple nodes in a group act as malicious node. It is also known as Black Hole Attack with multiple malicious nodes.

B. Zone Routing Protocol (ZRP)

The Zone Routing Protocol [10], as its name implies, is based on the concept of zones. A routing zone is defined for each node separately, and the zones of neighboring nodes overlap. The routing zone has a radius r expressed in hops. The zone thus includes the nodes, whose distance from the node in question is at most r hops. An example routing zone is shown in Fig. 1, where the routing zone of S includes the nodes A–I, but not K. In the illustrations, the radius is marked as a circle around the node in question. It should however be noted that the zone is defined in hops, not as a physical distance. The nodes of a zone are divided into peripheral nodes and interior nodes. Peripheral nodes are nodes whose minimum distance to the central node is exactly equal to the zone radius r. The nodes whose minimum distance is less than r are interior nodes.

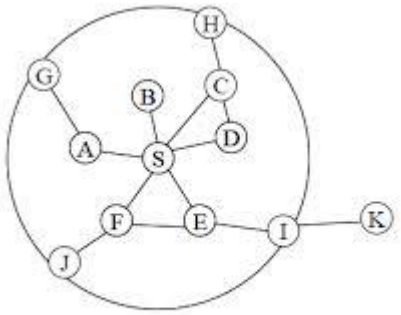

Figure 1: Example routing zone with r= 2

Example Routing Zone with r = 2 In Fig. 1, the nodes A–F are interior nodes; the nodes G–J are peripheral nodes and the node K is outside the routing zone. Note that node H can be reached by two paths, one with length 2 and one with length 3 hops. The node is however within the zone, since the shortest path is less than or equal to the zone radius. The number of nodes in the routing zone can be regulated by adjusting the transmission power of the nodes. Lowering the power reduces the number of nodes within direct reach and vice versa. The number of neighboring nodes should be sufficient to provide adequate reach ability and redundancy. On the other hand, a too large coverage results in many zone members and the update traffic becomes excessive. Further, large transmission coverage adds to the probability of local contention.ZRP refers to the locally proactive routing component as the IntrA-zone Routing Protocol (IARP). The globally reactive routing component is named IntEr-zone Routing Protocol (IERP). IERP and IARP are not specific

routing protocols. Instead, IARP is a family of limited-depth, proactive link-state routing protocols. IARP maintains routing information for nodes that are within the routing zone of the node. Correspondingly, IERP is a family of reactive routing protocols that offer enhanced route discovery and route maintenance services based on local connectivity monitored by IARP. The fact that the topology of the local zone of each node is known can be used to reduce traffic when global route discovery is needed. Instead of broadcasting packets, ZRP uses a concept called bordercasting. Bordercasting utilizes the topology information provided by IARP to direct query request to the border of the zone. The bordercast packet delivery service is provided by the Bordercast Resolution Protocol (BRP). BRP uses a map of an extended routing zone to construct bordercast trees for the query packets. Alternatively, it uses source routing based on the normal routing zone. By employing query control mechanisms, route requests can be directed away from areas of the network that already have been covered. In order to detect new neighbor nodes and link failures, the ZRP relies on a Neighbor Discovery Protocol (NDP) provided by the Media Access Control (MAC) layer. NDP transmits "HELLO" beacons at regular intervals. Upon receiving a beacon, the neighbor table is updated. Neighbors, for which no beacon has been received within a specified time, are removed from the table. If the MAC layer does not include a NDP, the functionality must be provided by IARP. The relationship between the components is illustrated in Fig. 2. Route updates are triggered by NDP, which notifies IARP when the neighbor table is updated. IERP uses the routing table of IARP to respond to route queries. IERP forwards queries with BRP. BRP uses the routing table of IARP to guide route queries away from the query source.

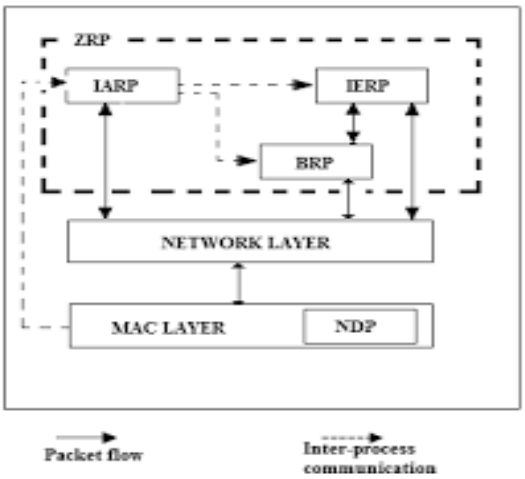

Figure 2: ZRP Architecture

1) Routing

A node that has a packet to send first checks whether the destination is within its local zone using information provided by IARP. In that case, the packet can be routed proactively. Reactive routing is used if the destination is outside the zone. The reactive routing process is divided into two phases: the route request phase and the route reply phase. In the route request, the source sends a route request packet to its peripheral nodes using BRP. If the receiver of a route request packet knows the destination, it responds by sending a route reply back to the source. Otherwise, it continues the process by bordercasting the packet. In this way, the route request spreads throughout the network. If a node receives several copies of the same route request, these are considered as redundant and are discarded. The reply is sent by any node that can provide a route to the destination. To be able to send the reply back to the source node, routing information must be accumulated when the request is sent through the network. The information is recorded either in the route request packet, or as next-hop addresses in the nodes along the path. In the first case, the nodes forwarding a route request packet append their address and relevant node/link metrics to the packet. When the packet reaches the destination, the sequence of addresses is reversed and copied to the route reply packet. The sequence is used to forward the reply back to the source. In the second case, the forwarding nodes records routing information as next-hop addresses, which are used when the reply is sent to the source. This approach can save transmission resources, as the request and reply packets are smaller.

The source can receive the complete source route to the destination. Alternatively, the nodes along the path to the destination record the next-hop address in their routing table. In the bordercasting process, the bordercasting node sends a route request packet to each of its peripheral nodes. This type of one-to-many transmission can be implemented as multicast to reduce resource usage. One approach is to let the source compute the multicast tree and attach routing instructions to the packet. This is called Root-Directed Bordercasting (RDB). Another approach is to reconstruct the tree at each node, whereas the routing instructions can be omitted. This requires that every interior node knows the topology seen by the bordercasting node. Thus, the nodes must maintain an extended routing zone with radius 2r-1 hops. Note that in this case the peripheral nodes where the request is sent are still at the distance r. This approach is named Distributed Bordercasting (DB). The zone radius is an important property for the performance of ZRP. If a zone radius of one hop is used, routing is purely reactive and bordercasting degenerates into flood searching. If the radius approaches infinity, routing is reactive. The selection of radius is a tradeoff between the routing efficiency of proactive routing and the increasing traffic for maintaining the view of the zone.

2). Route maintenance

Route maintenance is especially important in ad-hoc networks, where links are broken and established as nodes move relatively to each other with limited radio coverage. In purely reactive routing protocols, routes containing broken links fail and a new route discovery or route repair must be performed. Until the new route is available, packets are dropped or delayed. In ZRP, the knowledge of the local topology can be used for route maintenance. Link failures and sub-optimal route segments within one zone can be bypassed. Incoming packets can be directed around the broken link through an active multi-hop path. Similarly, the topology can be used to shorten routes, for example, when two nodes have moved within each other's radio coverage. For source-routed packets, a relaying node can determine the closest route to the destination that is also a neighbor. Sometimes, a multi-hop segment can be replaced by a single hop. If next-hop forwarding is used, the nodes can make locally optimal decisions by selecting a shorter path.

3). Query-control mechanisms

Bordercasting can be more efficient than flooding, since route request packets are only sent to the peripheral nodes, and thus only on the corresponding links. Further efficiency can be gained by utilizing multicast techniques. In that case, only one packet is sent on a link although several peripheral nodes can reside behind this link. However, since the routing zones of neighboring nodes overlap, each node may forward route requests several times, which results in more traffic than in flooding. When a node bordercasts a query, the complete routing zone is effectively covered. Any further query messages entering the zone are redundant and result in wasted transmission capacity. The excess traffic is a result from queries returning to covered zones instead of covered nodes as in traditional flooding. To solve this problem, ZRP needs query-control mechanisms, which can direct queries away from covered zones and terminate query packets before they are delivered to peripheral nodes in regions of the network already covered by the query. ZRP uses three types of query-control mechanisms: query detection, early termination and random query-processing delay. Query detection caches the queries relayed by the nodes. With early termination, this information is used to prune bordercasting to nodes already covered by the query.

i). Query detection

When a bordercast is issued, only the bordercasting node is aware that the routing zone is covered by the query. When the peripheral nodes continue the query process by bordercasting to their peripheral nodes, the query may be relayed through the same nodes again. To be able to prevent queries from reappearing in covered regions, the nodes must detect local query relaying activity. BRP provides two query detection methods: QD1 and QD2. Firstly, the nodes that relay the query are able to detect the query (QD1). Secondly, in single-channel networks, it is possible to listen to the traffic by other nodes within the radio coverage (QD2). Hence, it is possible to detect queries relayed by other nodes in the zone. QD2 can be implemented by using IP broadcasts to send route queries. Alternative, unicast can be used if the MAC and IP layers operate in promiscuous mode. In the above example, all nodes except node B relay the query of S. They are thus able to use QD1. Node B does

not belong to the bordercast tree, but it is able to overhear the relayed query using QD2. However, node K does not overhear the message, and is therefore unaware that the zone of node S is covered. A query detection table is used to cache the detected queries. For each entry, the cache contains the address of the source node and the query ID.

ii) Early termination

With Early Termination (ET), a node can prevent a route request from entering already covered regions. Early termination combines information obtained through query detection with the knowledge of the local topology to prune
branches leading to peripheral nodes inside covered regions. These regions consist of the interior nodes of nodes that already have bordercast the query. A node can also prune a peripheral node if it has already relayed a query to that node. Early termination requires topology information extending outside the routing zone of the node. The information is required to reconstruct the bordercast tree of other nodes within the routing zone. The extended routing zone has a radius of 2r-1. Alternatively, in the case of root-directed bordercast (RDB), the topology of the standard routing zone and information about cached bordercast trees can be used.

iii) Random query-processing delay

When a node issues a node request, it takes some time for the query to be relayed along the bordercast tree and to be detected through the query detection mechanisms. During this time, another node may propagate the same request. This can be a problem when several nearby nodes receive and rebroadcast a request at roughly the same time. To reduce the probability of receiving the same request from several nodes, a Random Query-Processing Delay (RQPD) can be employed. Each bordercasting node waits a random time before the construction of the bordercast tree and the early termination. During this time, the waiting node can detect queries from other bordercasting nodes and prune the bordercast tree. To avoid additional route discovery delay, the delay can be combined with the pre-transmission jitter used by many route discovery protocols. Assume that in Fig. 7 the nodes C and S both receive a query. Node C schedules a bordercast to its peripheral node E, and node S to its peripheral node F. Without RQPD, both nodes would issue the broadcast simultaneously, and thereafter detect the message of the neighbor node. With RQPD, the node C may detect the query sent by node S during the delay, and prune the branch leading to E.

C. Related Work

Bait DSR (BDSR) based on Hybrid Routing Scheme [11] to avoid the collaborative Black Hole Attacks. The proposed solution is composed of both proactive and reactive method to make a hybrid routing protocol. The base routing protocol used is the DSR on-demand routing. Initially the source node sends bait RREQ packet. The destination address for this bait RREQ does not exists. The same method as used in DSR is used here to avoid the traffic jam problem generated by bait RREQ. The initially sent bait RREQ can attract the forged RREP and can easily remove malicious node to avoid black hole attack. In this solution the RREPs additional field records the identity of theses malicious nodes. Now the source node can easily detect the location of malicious node and will discard all the RREPs coming from that location. BDSR has an increased packet delivery ratio when compared to existing DSR and WD approach. Bluff-Probe Based Black Hole Node Detection and prevention [12] is an algorithm designed using IERP protocol. An additional code is added for bluff probe packet and for detecting and avoiding Black Hole node. This algorithm is divided into following parts (i) when intra zone communication takes place. (ii) When there is inter zone communication. When intra zone communication takes place the source node broadcast bluff probe packet. This packet contains the address of nonexistent destination node. This massage is named as bluff probe request packet. The direct neighbor node receives this bluff probe packet. Now the neighbor node check their routing table entries if they have entry for this non-existent destination node than they forward the packet to the next neighbor. If the node is suspected to be malicious node then they will give immediate response to the source node through the intermediate node. As it response, the source node label it as a black hole node and blocks this node. After this, the source node informs their direct neighbor for updating their routing table entries.

III. RESULTS AND DISCUSSION

A. Simulation Setup In our scenario, we simulated 20 nodes distributed over 700m x 700m terrain with varying node mobility on NS-2 [13]. The initial positions of the nodes were random. The implementation used 802.11 MAC layer and CBR traffic over UDP. Each session generated 500 data packets of 512 bytes each at the rate of 10 packets per second. All simulations were run for 500 seconds of simulated time. Our goal was to determine a technique which shows less vulnerability in case of black hole attack. We choose ZRP routing protocol which is hybrid routing protocol. In the case of ZRP, malicious node buffer size is lowered to a level which increase packet drop. Furthermore the simulation parameters are given in Table 1.

Table1. Simulation parameters

Examined Protocol	-	ZRP
Simulation Time	-	500 seconds
Simulation area (m*m)	-	700*700
Number of Nodes	-	20
Traffic Type	-	UDP
Performance Parameter	-	Average Network Delay, Network Throughput, Total Dropped Packets, Packet Delivery Ratio
Mobility (m/s)	-	0-250
Packet Size (bits)	-	512

- **Packet Delivery Ratio**

Packet Delivery Ratio in case of Black Hole attack and without attack depends on the protocol routing procedure and number of nodes involved. In Figure 5, Packet Delivery Ratio in case of node mobility having max value 250 m/s for ZRP is high when there is no attack on the network nodes. This is because during the Black hole attack, the malicious node drops the packets when the source node sends any packet to it. This is the property of Black hole node to drop all the packets send to it.

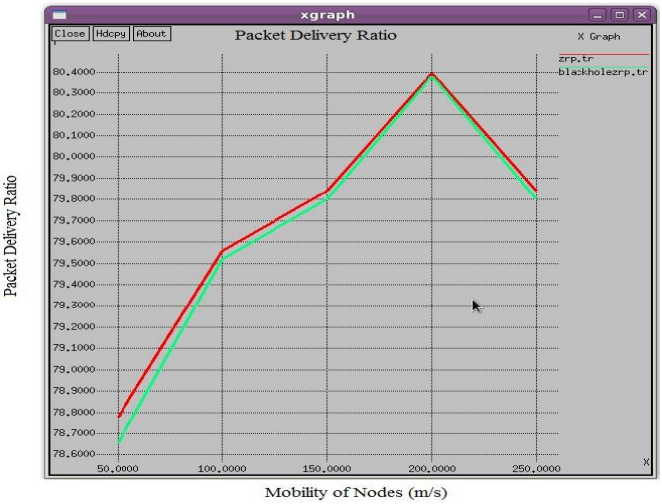

Figure 5: Packet Delivery Ratio v/s Node Mobility for ZRP and blackholeZRP

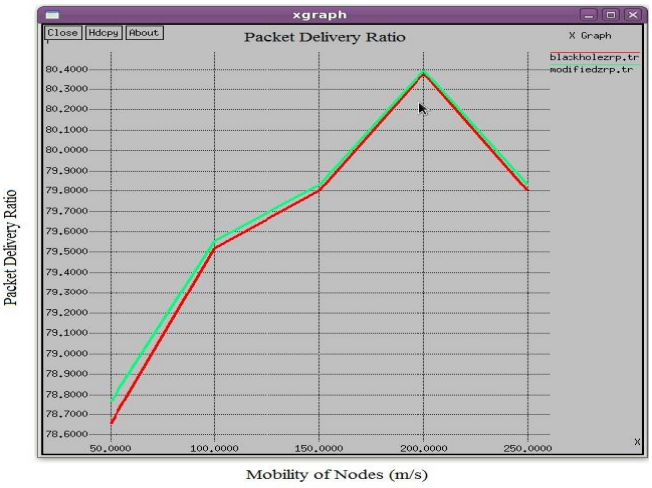

Figure 6: Packet Delivery Ratio v/s Node Mobility for blackholeZRP and modifiedZRP

Fig. 6 shows that modifiedZRP has slightly higher Packet Delivery Ratio than to blackholeZRP. However with the increase in node mobility an increase in the Packet Delivery Ratio of modifiedZRP has been observed. In terms of Packet Delivery Ratio the performance of modifiedZRP improves with the increase in node mobility but it decreases when the mobility increases the 200 m/s. modifiedZRP performs better when mobility is set to 200 m/s.

- **Average Network Delay**

Figure 7: Average Network Delay v/s Node Mobility for ZRP and blackholeZRP

Average Network Delay in case of Black Hole attack and without attack depends on the protocol routing procedure and number of nodes involved. In Fig. 7, delay in case of node mobility of 0 to 250 m/s for blackholeZRP is high then ZRP. This is because during the Black Hole attack, there is no need of RREQs and RREPs because the malicious node already sends its RREQs to the sender node before the destination node reply having less delay

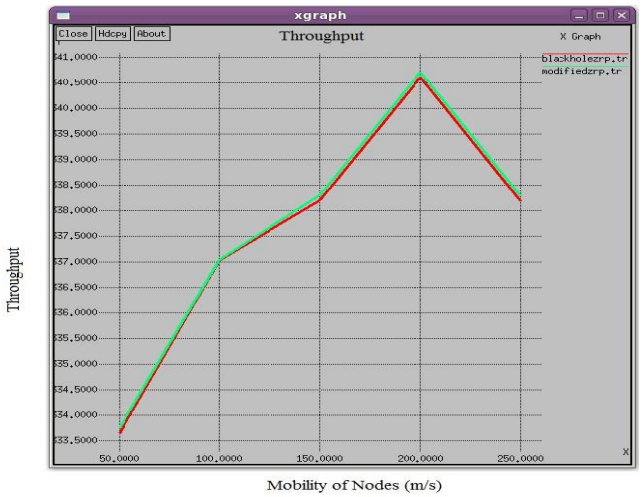

Figure 8: Average Network Delay v/s Node mobility for blackholeZRP and modifiedZRP

Average Network Delay in case of Black Hole attack and without attack depends on the protocol routing procedure and number of nodes involved. In Fig. 8, delay in case of node mobility of 0-250 m/s for blackholeZRP is high then modifiedZRP. This is because during the Black Hole attack, there is no need of RREQs and RREPs because the malicious node already sends its RREQs to the sender node before the destination node reply having less delay.

- **Total Dropped Packets**

Figure 9: Total Dropped Packets v/s Node Mobility for blackholeZRP and modifiedZRP

Total Dropped Packets are higher in blackholeZRP Fig.9

.• **Network Throughput**

From Fig. 10, for mode mobility from 0 to 250 m/s, it is obvious that the throughput for ZRP is high compared to that of blackholeZRP. This is because of the fewer routing forwarding and routing traffic. Here the malicious node discards the data rather than forwarding it to the destination, thus affecting throughput.

Figure 10: Throughput v/s Node Mobility for ZRP and blackholeZRP

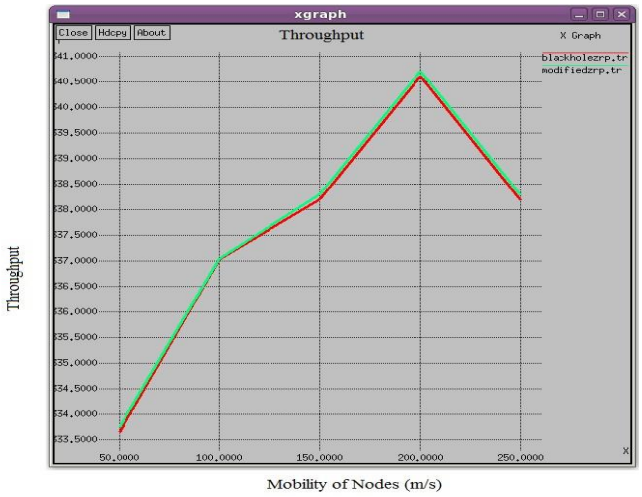

Figure 11: Throughput v/s Node Mobility for blackholeZRP and modifiedZRP

From Fig. 11, for mode mobility from 0 to 250 m/s, throughput for modifiedZRP is high as compared to blackholeZRP. This is because of the fewer route forwarding and routing traffic. Here the malicious node discards the data rather than forwarding it to the destination, thus effecting throughput. In case of Network Throughput the modifiedZRP performs better when node mobility is set to 200 m/s.

IV. CONCLUSION

A Black Hole attack is one of the serious security problems in MANETs. Although many solutions have been proposed but still these solutions are not perfect in terms of effectiveness and efficiency. If any solution works well in the presence of single malicious node, it cannot be applicable in case of multiple malicious nodes. The proposed technique is hybrid in nature and based on the concept of ZRP. It provides a solution for identification of Black Hole Attack and removal of Black Hole from the network. The proposed technique gives a better solution towards Black Hole Attack within the network. Black Hole attack with five different scenarios with respect to the performance parameters of Average Network Delay, Network Throughput, Total Dropped Packets and Packet Delivery Ratio had been simulated. There is a need to analyze Black Hole attack in other MANETs routing protocols such as DSR, TORA and GRP. Other types of attacks such as Wormhole, Jellyfish and Sybil attacks are needed to be studied in comparison with Black Hole attack. They can be categorized on the basis of how much they affect the performance of the network. Black Hole attack can also attack the other way around i.e. as Sleep Deprivation attack. The detection of this behavior of Black Hole attack as well as the elimination strategy for such behavior has to be carried out for further research.

V. REFERENCES

[1] P.V.Jani, "Security within Ad-Hoc Networks," Position Paper, PAMPAS Workshop, Sept. 2002.

[2] K. Biswas and Md. Liaqat Ali, "Security Threats in Mobile Ad-Hoc Network", Master Thesis, Blekinge Institute of Technology Sweden, March 2007.

[3] E. A .Mary Anita and V. Vasudevan, "Black Hole Attack Prevention in Multicast Routing Protocols for Mobile Adhoc networks using Certificate Chaining", International Journal of Computer Applications (0975 – 8887) Vol. 1, Issue 12, pp. 21-28, 2010

[4] Umang S, Reddy BVR, Hoda MN, "Enhanced Intrusion Detection System for Malicious Node Detection in Ad Hoc Routing Protocols using Minimal Energy Consumption", IET Communications Vol.4, Issue17, pp2084–2094. doi: 10.1049/ietcom. 2009.

[5] G. A. Pegueno and J. R. Rivera, "Extension to MAC 802.11 for performance Improvement in MANET", Karlstads University, Sweden, December 2006.

[6] N. Bhalaji and A. Shanmugam, "A Trust Based Model to Mitigate Black Hole Attacks in DSR Based Manet", European Journal of Scientific Research, Vol.50 No.1, pp.6-15, 2011

[7] Latha Tamilselvan and Dr. V Sankaranarayanan, "Prevention of Blackhole Attack in MANET", the 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, 0-7695-2842-2/07, 2007.

[8] Chang Wu Yu, Tung-Kuang Wu, Rei Heng Cheng, and Shun Chao Chang, "A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Networks", PAKDD 2007 Workshops, LNAI 4819, pp. 538–549, 2007

[9] Santhosh Krishna B V, Mrs.Vallikannu A.L, "Detecting Malicious Nodes For Secure Routing in MANETS Using Reputation Based Mechanism" International Journal of Scientific & Engineering Research, Vol. 1, Issue 3, ISSN 2229-5518, December-2010.

[10] N.Beijar, "Zone Routing Protocol (ZRP)", Networking Laboratory, Helsinki University of Technology.

[11] Tsou P-C, Chang J-M, Lin Y-H, Chao H-C, Chen J-L, "Developing a BDSR Scheme to Avoid Black Hole Attack Based on Proactive and Reactive Architecture in MANETs". Paper presented at the 13th International Conference on Advanced Communication Technology, Phoenix Park, Korea, 13-16 Feb. 2011.

[12] Prof. Sanjeev Sharma, Rajshree, Ravi Prakash, Vivek, "Bluff-Probe Based Black Hole Node Detection and prevention", IEEE International Advance Computing Conference (IACC 2009), 7 March 2009.

[13] Official NS-2 website. http://www.isi.edu/nsnam/ns