Journal of Engineering and Applied Sciences 11 (2): 182-191, 2016
ISSN: 1816-949X

A Modified Method for Preventing Black-Hole Attack in Mobile Ad Hoc Networks

[1]R. Sathishkumar and [2]C. Ramesh
[1]Department of Computer Science and Engineering, Satyabama University, Chennai, India
[2]ST Ericsson Pvt India Limited Survey No. 28, 36/5, KR Puram Outer Ring Road,
Doddanakemdi Village, 560037 Bangalore, Karnataka State, India

Abstract: Black hole attack is a serious security problem to be solved for active delivery of packets of data in Mobile Ad-Hoc networks. In this problem, a malicious node uses routing protocol to promote itself as having the shortest path to the node whose packets it wants to snatch. In flooding based protocol, if the malicious node reply reaches the requesting node before the reply from the actual node, a fake route is created and try to send the packets of data. This research study deals with the presentation of preventing black hole attack in Mobile Ad Hoc Network (MANET).Various prevention techniques have been discussed in the study that are used to prevent black hole attack. Mobile Ad Hoc networks are susceptible to various attacks, so attacks have to be mitigated in initial setup.

Key words: Routing, black hole attack and security, AODV, prevention, MANET

INTRODUCTION

Introduction to MANETs: A Mobile Ad-Hoc Network (MANET) is a collection of wireless mobile nodes which have the ability tocommunicate with each other nodes without having fixed network infrastructure or any central Base Station (BS). The communication and connectivity is done from node to node by forwarding packets between themselves. The protocols used for packet forwarding in MANET are dynamic source routing, destination sequenced distance vector and ad-hoc on demand distance vector. Due to non-availability ofnetwork infrastructure and self-governing behavior of nodes, network is vulnerable to many attacks (Alem and Xuan, 2010). Most commonly found attacks are blackhole attack, man in middle attack, Denial of Service (DoS) attack, impersonation, eaves dropping, black hole attack and gray hole attack. The AODV is a source initiated on-demand routing protocol. Every mobile node maintains a routing tablethat maintains the next hop node information for a route to the destination node (Alem and Xuan, 2010). Black hole leads toserious loss or drops in the network by receiving the packet and dropping the received packets that has to receiveby the destinationnode (Kurosawal *et al*., 2007).

Introduction to AODV: As the name describes AODV forms the route from source to destination nodes and between the intermediatenodes, when there is demand for forwarding packets using MANETs. AODV (Ad-hoc On-demand Distance Vector) is a reactive routing protocol, yet it is basically an improvement of DSDV routingprotocol which is proactive protocol (Tamilarasan, 2011). The route discovery process takes place onlywhen required. AODV can handle low, moderate and relatively high mobile rates, together with amultiplicity of data traffic loadings compare with some popular routing protocol. However, it makes no provisions for security in the AODV. In route discovery process of AODV, there are three types of messages they are:

- Route Request (RREQ)
- Route Reply (RREP)
- Route Error (RERR) messages

RREQ: It is basically, the broadcasting request to find the route to a required destination node. Thus, it helps to create a route discovery process by broadcasting route request message to itsneighboring nodes. The neighboring nodes save the path where RREQ request is transmitted. After that, it verifies the new or fresh route to the desired node in the routing table by the use of RREQ request (Nishu and Kundan, 2013).

RREP: When, the node finds a fresh path for destination then a route reply message is unicasted tothe source node or originator of the RREQ if the receiver is either the node using the requested address or is having a valid route to the requested address (Nishu and Kundan, 2013).

Corresponding Author: R. Sathishkumar, Department of Computer Science and Engineering, Satyabama University, Chennai, India

RERR: This type of messages helps to keep eye on link status of the next hopin the appropriate route. RERR (Route Error) messageis broadcasted to whole nodes whenever the breakage in the link is found. This is also called route maintenance (Abid and Khan, 2014).

Advantages of AODV:

- Connection set up delay is less
- Destination sequence numbers are used to find the latest route to the destination
- On-demand route establishment with small delay time
- Link breakages inthe active routes can be efficiently handled

Disadvantages of AODV:

- Periodic beaconing leads to bandwidth consumption
- Intermediate routes can lead to inconsistent routes if the source sequence number is old
- Multiple RERR (error messages) packets in response to single RREQ packet may lead to heavy control overhead

Introduction to black hole attack: A black hole is a malicious node that falsely replies for any Route Request (RREQ) without having active route to specified destination and drops all the receiving packets (Chavda and Nimavat, 2013; Mohanapriya and Krishnamurthi, 2014; Bar *et al*., 2013; Patil and Bhole, 2013; Bhardwaj, 2014; Tan and Kim, 2013). A black hole node has two properties: They are the node enters in AODV by represent itself as a valid route from source to destination. Then, it starts receiving the packet from the valid node, drops the packet containing valuable information.

Single Black Hole Attack: In single black hole attack, only one malicious node attack on the route path (Abid and Khan, 2014). When, the source node broadcast RREQ message then the malicious node takes an advantage of vulnerabilities of AODV protocol showing in Fig. 1.

It responds with high sequence number to its preceding nodein the path. Thus, source node assumed malicious node as a destination node and start the processof data forwarding in the appropriate route. The malicious node then drop all the packet received.

Co-operative black hole attack: The number of malicious nodes is more than one in the network (Sarma *et al*., 2014; Wei *et al*., 2014; Sowmya *et al*., 2012). The overall result of cooperative is complete decrease in throughput and increase in packet dropratio in the network is shown in Fig. 2.

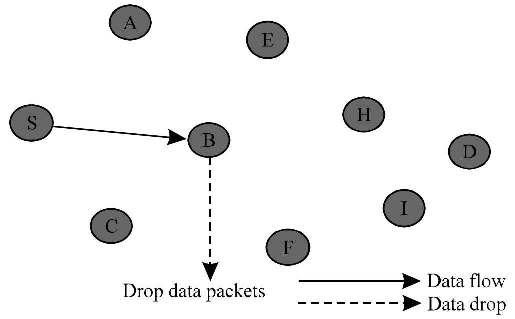

Fig. 1: Single black hole attack

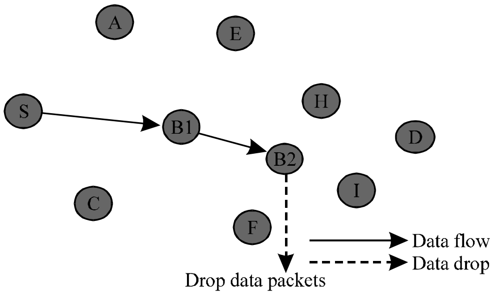

Fig. 2: Collaborative black hole attack

Thus, for better security and better performance in MANETs, it is very important to eradicate the cooperative attack.

Literature review: In various security techniques and routing protocols have been proposed and implemented for the prevention of single and cooperative black hole attacks in the network (Sowmya *et al*., 2012; Devassy and Jayanthi, 2012; Garg and Beniwal, 2012; Goyal *et al*., 2011; Mistry *et al*., 2010; Savner and Gupta, 2014; Hu *et al*., 2006).

Mohanapriya and Krishnamurthi (2014) presented a Modified Dynamic Source Routing Protocol (MDSR) to detect and prevent selective black hole attack. The source node picks the first shortestpath to the destination node to near the number of data packets it sends to the destination. The sourcenode then selects the second shortest path for actual transmission or forwarding of data. Then, packet count andtransmitted data both are compared. If the difference is significant i.e., abnormality is detected thenearby IDS node broadcast a message informing all nodes to obscure all nodes from network.

Yao and co-authors find a new Routing Security Scheme based on Reputation Evaluation (RSSRE) is proposed in this research. There putation evaluation mechanism is built on the basis of correlation among nodes that need to beappraised. It has the mechanism to promote the cooperation of cluster members for forwarding datapackets to execute improved routing when there are malicious nodes in hierarchical Ad Hoc Mobile networks.

Xiaopeng and Wei (2007) researchers proposed check point based multi-hop acknowledgement scheme for detecting selective forwarding attacks which can select the intermediate nodes randomly as check point nodes which will generate acknowledgement for each packet received. Intermediate node has to send the acknowledgment for every packet that it is receiving; the algorithm has to suffer from overhead. Moreover, the channel is assumed perfect. Xiaopeng and Wei (2007) proposed three security algorithms such as:

- Full proof algorithm
- Check-up algorithm
- Diagnosis algorithm

The full proof algorithm was for creating proof and the check-up algorithm was for checking up source route nodes and the diagnosis algorithm was for finding the malicious nodes in the actual network.

Jaisankar *et al*. (2010) invented that each node should have Blackhole Identification Table (BIT) that contains source, target, current node ID, Packet Received Count (PRC), Packet Forwarded Count (PFC). If difference between PRC and PFC is significant then, the node is identified asmalicious and is isolated from the network.

Chavda and Nimavat (2013) researchers proposed an algorithm to remove black hole attack at the cost of overhead. The source node continues to accept RREP packets from the various nodes and compares RREP (RREP R1, RREP R2) which actually compares the destination hop count of two route replies and selects the route reply with high destination hop count if the difference between two hop counts is not significantly high.

Chavda and Nimavat (2013) used a novel approach to improve the AODV routing protocol under the blackhole attack. In this approach, the protected route between source and destination node using NS2 Network Simulator software for simulation was founded. The wireless channel used as a channel which was two ray ground radio propagation model. AODV routing protocol and UDP were used at network and transport layer. All the data packets were CBR (Continuous Bit Rate) packets. This algorithm was applied in the presence of attack and had increased the throughput and packet delivery ratio.

Wang proposed an approach to improve the scalability and competence of MANETs byarranging the nodes on the basis of trust mechanism.

Ullah and Anwar (2013) proposed the reactive and proactive protocols against the blackhole attack on MANET. This study had compared the simulation results of proactive (OLSR) and reactive (AODV) routing protocol under the black hole attack on MANET. The parameters taken were throughput, network load and end-to-end delay and simulation is done in Optimized Network Engineering Tool (OPNET). They have used OPNET for modeling the nodes, picking its statistics and then operating its simulation to get the result used for the analysis. In the end-to-end delay, under black hole attack both protocols were compared and analyzed. AODV showed high delay as of OLSR because of its route search and reactive behavior. But, in the throughput and network load of AODV performed better results.

Arora and Barwar (2014) performed the analysis over the performance of MANET routing protocols like AODV, OLSR and ZRP with or exclusive of black hole attack and have compared their analysis results. In this, the performance analysis the various parameters like packet delivery ratio, average throughput, average end to end delay and packet drop rate using NS2 simulator under different scenarios have been judged. In the comparison, the hybrid protocol (ZRP) performed better among other protocols in MANET.

Rani and Kumar (2013) researchers proposed to diminish the blackhole attack using AOMDV (Ad hoc on Demand Multipath Distance Vector) routing protocol with some improvements in it. These developments formulate the protocol vigorous against black hole attack and multipath route discovery process. This approach was based on to avoid multiple blackhole attacks when transitional nodes respond to the RREQ packet. Then there would be various connections to the destination. But, only, one path from source to destination could be opted. At that time, intermediate node will generate a route which did not contain any node whose validity threshold crosses the lower level. In this research RREQ and RREP packets were also improved.

Dangore and Sambare (2013) used the AODV routing protocol for detection and had overcome the blackhole attack. The network parameters like throughput, packet delivery ratio and average end to end delay had been calculated for authentic network and a network with black hole attack using the NS2 software tools. The algorithm used some steps for detection of malicious node. They are:

- Step 1; If a node sends various information packets to destination, it is understood as a truthful node
- Step 2; If a node obtains numerous packets but, does not pass identical information packets, it is probably a malicious node

Yang proposed Anti Blackhole Mechanism (ABM) (Sarma *et al*., 2014). Suspicious value of a node is estimated by ABM on the basis of amount of significant difference between RREQs and RREPs transmitted by the node. If an intermediate node, i.e., not the destination node receives a RREQ but, do not forward, it for a specific route but, forward RREP for the route then, its suspicious value is increased by 1 in the apprehensive node table of neighbor IDS node. If suspicious value of a node exceeds its threshold value then, IDS node broadcasts a block of message to all the nodes to isolate apprehensive node from the network. But, the gray-hole nodes participate in the process of route discovery.

Marti and co-authors proposed the use of watchdog and path rater (Chavda and Nimavat, 2013). Watchdog lustfully listens to the transmission of the next node in the path to detect mis behaviors. Path rater keeps the ratings for other nodes varieties vary from 0-0.8 where 0.5 signifies node as neutral. These values are updated periodically by 0.01 each 200 m sec and performs route selection by selecting routes that do not contain selfish nodes. However, the watchdog mechanism needs to maintain the state information on the monitored nodes and the transmitted packets which undoubtedly increases memory overhead.

Salehi *et al*. (2012) proposed a new black hole attack with DSR protocol and compared the simulation results with ordinary blackhole attack. In this research, a new attack named deep black hole attack which promotes fake RREPs more powerfully than ordinary black hole attack had introduced. Researchers had used the NS2 for the simulation of DSR protocol parameters. The new attack has two phases. In the advertisement phase node makes fake RREPs in reply to received RREQs and also regarding overheard RREPs. But in the packet drop phase, node generates and sends a new fake RREP having anfalse source route which is almost shorter than the main source route and contains malicious node itself as a hop in the route. With the help of fake RRRPs, it receives the packet from other nodes and starts dropping their packets silently. To avoid this DSR algorithm which by default helps to find the activated original node had been used.

Pramod Kumar Singh and Govind Sharma proposed method uses immoral mode to detect malicious node and propagates the information of malicious node to all the other nodes in the network. It does not require any back end database, extra memory and more processing power (Nath and Chaki, 2012).

Nabarun Chatterjee and co-authors proposed a triangular encryption technique for the detection of black hole attack (Bhosle *et al*., 2012). According to this approach source node send a plain text along with RREQ when intermediate node receives a RREQ, its ends this packet to the destination node in its placeof RREP to the source node. Destination node encrypts the plain text with pre agreed partition with key and sends, it with RREP. On receiving these packets intermediate node update their index and hop count. If the RREP packet contains cipher text, it is unquestionable to have reached the destination.

Fidel Tachil and co-authors proposed a trust based approach for AODV protocol (Chavda and Nimavat, 2013). In this approach, every node monitors neighboring nodes and calculates its trust value. If this value goes underneath threshold value then the monitoring node considered as malicious node. The trust value of a node is calculated as a ratio of number of packets dropped to the number of packet forwarded by that node. The cache mechanism implemented by every node in order to confirm that data sent by it are being forwarded or not.

Existing work: In the study, conducted by Nath and Chaki (2012) the researchers have tried to prevent the black hole in the network using the concept of clustering. The black hole nodes come in the path from sourcenode to destination node. According to the characteristics of malicious node during black hole deployment, node just receive data packets but never forward to further destination nodes. Thus, if server only check all nodes activity for sending and receiving of packets then server is able to detect the malicious nodes. So, by doing the clustering, it will be easy for the server to check the nodes for their communication behavior. If any node is just receiving the data and is not forwarding any packets then, it will suspect to be black hole node in the network.

However, the researchers have not provided any solution to detect the malicious cluster head in the network and the internal malicious attacker. The researchers have presented the detection and prevention scheme to study the effect of external malicious node entering in the network and the internal nodes have been measured as trusted nodes. The attacker may cooperation some internal node in the network and get access to important information in the network. There get up a need to detect and prevent any malicious node present internally in the network including the cluster head which can be compromised node present.

MATERIALS AND METHODS

Proposed work: In our research, here it is aim at detecting and preventing the black hole attack in the network by using the concept of secure clustering. Here, in this study, aim at modifying the process of cluster formation using the concept of acknowledgement message. Initially, the network will be divided into the grids of networks. The server node will be positioned at the centre of the network. The server node will choose one randomly selected node from the grid that will start the process of clustering.

The server node will send hello message to the randomly carefully chosen node. If the node replies back to the sink with acknowledgement then it can start the clustering process else it cannot take part in clustering process Fig. 3.

Once the initiator node has been selected for each grid then, it will send the hello message to the every node in the grid to start the clustering process. Here, we tend to select the cluster head on the basis of highest energy, so that lifetime of the network is also taken into an account. Every legitimate node in the network will reply back with their energy level to the initiator node. But, the malicious nodes would not reply back. In this way, only the legitimate node will take part in the clustering process.

After the initiator node received reply from all the genuine nodes, it will maintain a table of reply messages. If any node has not replied then it will added into suspected node in the Fig. 4.

After the clusters are formed and cluster head is selected, the nodes will start communicating with the cluster heads. Further to verify all the nodes in the alleged node table maintained, their behavior will be analyzed. If those nodes are not forwarding any messages then they will be confirmed as malicious nodes.

Experimental setup: In this part, here, it is estimate our proposed work. Initially, here calculate right protection method and have to take care of whether it retains original distance graph of the original dataset or not. Finally, here compare our new approach with the existing system approach. Here, check our approaches on different datasets. Usually, most of the experiments were conducted on 3GHz Intel CPU with 4GB RAM. And also, the scalability checking experiments have been conducted on a 3.40GHz Intel CPU with 8GB RAM. Here are using Java framework (version jdk 6) on

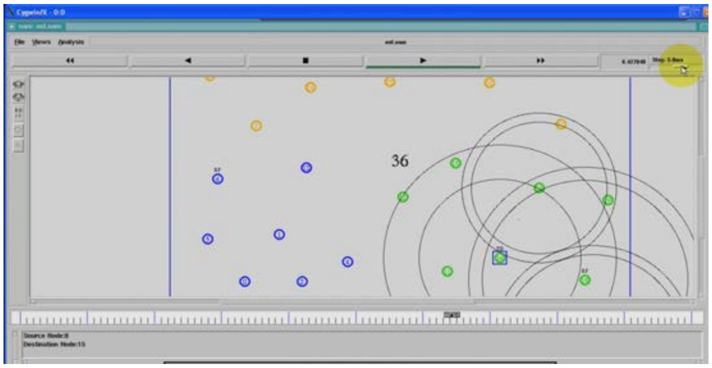

Fig. 3: Simulation results in NS2

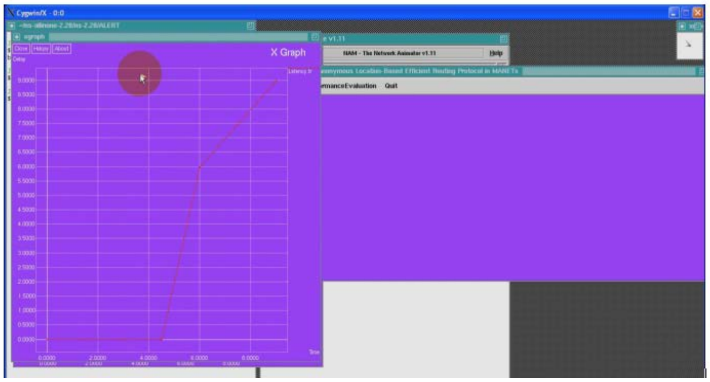

Fig. 4: X-graph for communication clusters

Windows platform. The Net beans (version 6.9) are used as a development tool for this system.

RESULTS AND DISCUSSION

Experimental setup and analysis: This study is applied to NS2 software tool to validate the detection and isolation efficiency of theproposed method against black-hole nodes. In an area of 1500×1500 m^2, 102 normal nodes executing AODV routing protocol were randomly distributed and a couple of hateful nodes performing black-hole attack and 4 check-point nodes are arbitrarily located is find out. The number of blackhole node is 5 and traffic type is UDP-CBR. The major parameters of experiment are listed in Table 1. Data obtained by taking average value which results from 10 experiments.

Packet delivery ratio: In our approach is 1, i.e., the number of nodes asource node sends is same as the number of packets destination node receives (Fig. 5). It is calculated as:

$$p = (\text{No. of packets received})/(\text{No. of packets sent}) \times 100$$

Table 1: Simulation Parameters

Properties	Values
Simulator	NS2
Coverage area	1500×1500 m^2
Number of nodes	102
Simulation times	600 sec
Mobility	Random way point model
Mobility speed	20 m sec^{-1}
Number of black-hole nodes	5
Mobile check-point nodes	4
Traffic type	UDP-CBR

In all figures, throughout the document, the red solid linewith the square markers represents the original protocol andthe green solid line with the triangular markers representsthe modified protocol. Both of the two black lines above andbelow each of the red and the green lines represent themargin of errors for the experiments of the correspondingline. The margin of errors is computed at confidence 95% (Fig. 6).

Thus, on comparing our approach with it is PDR in both cases is same. In our approach, mobile check points will notice the number of data packets forwarded to and by the nodes in the route and monitor the data packet loss (Fig. 7).

Detection rate: Is total number of nodes detected (whether these are malicious or not) from the overall

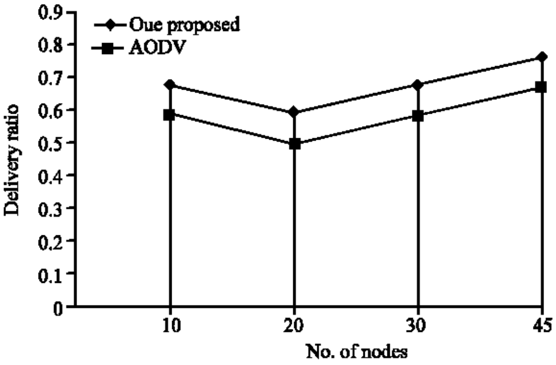

Fig. 5: Packet delivery ratio: 1 black hole

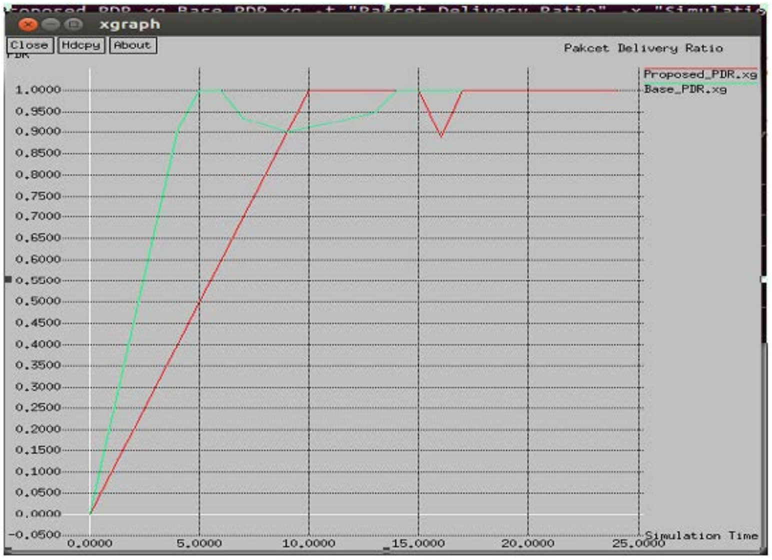

Fig. 6 : Packet delivery ratio

networks, therefore, the detection rate should be high in Mobile Ad-Hoc Network (MANETs). In the novel and the proposed approach, the detection rate is about four times of the approach.

Throughput: Is number of data packets delivered per second. It is also expressed in numberof bits per second.

In our proposed approach throughput obtained is near about 1.7 times that inapproach. It is calculated as:

$$\text{Average throughput} = (\text{Received packet size}/(\text{Stop time-starttime})\times(8/1000)$$

Table 2 summarizes different approaches used by researchers to mitigate the effect of black hole attack on AODV.

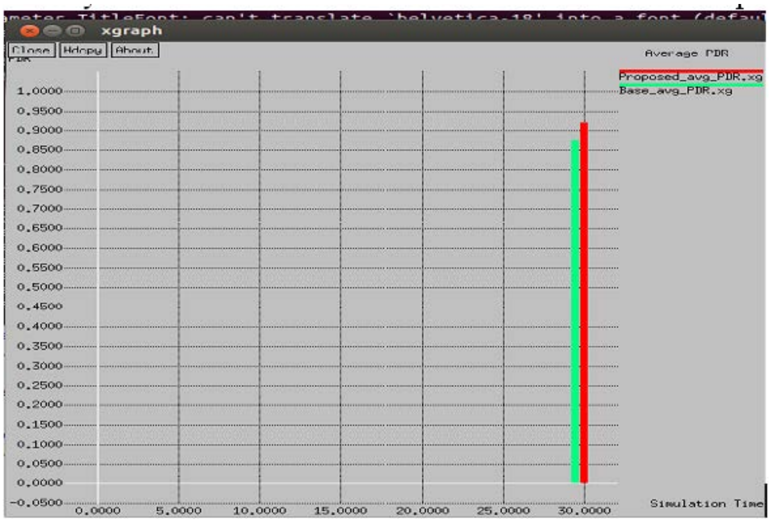

Fig. 7: Average packet delivery ratio

Table 2: Comparative study of existing solutions

Paper title	Authors	Publication year	Features	Simul tools used
Modified AODV protocol to prevent black hole attack in Mobile Ad-hoc network (Tan and Kim, 2013)	Romina Sharma, Rajesh Shrivastava	March 2014	Working of AODV protocols is modified by addition of next hop information in the RREP message along with two control message which includes further route request and further route reply	NS2
Detecting blackhole attack in wsn by check agent using multiple base stations (Alem and Xuan, 2010)	Swarnali Hazra and S.K. Setua	2013	Detects black hole attacker in entire network. In that high detection rate as shown in simulation result. Their proposed trust computation and trust model define trust level of relationship between nodes in network. One node believes or disbelieves its trustee depending on trust level. With disbelief of thruster, black hole attacker are detected and removed from route	NS2
Black hole attack defending trustedon-demand routing in ad-hoc network (Santhamurthy *et al*., 2011)	Harmandeep Sinh and Manpreet Sinh	2014	The effect of black hole in ad hoc wireless networks.They implemented an AODV protocol that Simulates behaviour of a black hole in NS2. For this method, they have used very simple and effective way of providing security in AODV against black hole attack that causes the interception and confidentiality of ad hoc wireless sensor networks. Their solution detects malicious nodes and removes it from the active data forwarding. As per graphs showed in result they easily conclude that performance of the normal AODV drops under the presence of black hole attack.	NS2
Securing MANET s routing protocol under black hole attack (Nishu and Kundan, 2013)	M. Mohanapriya and Ilango Krishnamurthi	2014	That is simple acknowledgement scheme to detect black hole nodes in MANET. It can be incorporated with any existing on demand ad hoc routing protocols. By their proposed algorithm, destination node detect the presence of malicious node in the source route and with the help of intrusion detection system the malicious nodes are removed from the network. Their IDS nodes resulting less energy loss which makes their method suitable for the resource constrained characteristics of MANET	NS2

Table 2: Continue

Paper title	Authors	Publication year	Features	Simul tools used
			By simulationresults percentage of data packet loss in their proposed work is better than DSR in presence of multiple grayhole nodes	
Modified DSR protocol for detection and removal of selective black hole attack in MANET (Abid and Khan, 2014)	Satyajayant Misra and Guoliang Xue	2011	BAMBi:Black hole Attacks Mitigation with multiple base stations in wireless sensor networks. That effectively mitigate the effect of black hole attack on WSNs. It's based on deployment of multiple base stations in the network and routing of copies of data packets to that base stations. Their solution is highly effective and require very little computation and message exchanges in the network, so saving the energy of the SNs.	
Struggling against simple and cooperative black hole attacks in multi-hop wireless ad hoc networks (Chavda and Nimavat, 2013)	Abderrahmane Baadache and Ali Belmehdi	2014	An authenticated end-to-end acknowledgment based approach that checks correct forwarding of packets by intermediate nodes.Their approach detects the black hole launched in simple or cooperative manner. No modification and the no reply of messages are required to fully deliver the message to the destination node. Compared to 2-hop ACK and watchdog approach, their approach has best delivery ratio of packet and the highest detection ratio.	NS2
Elimination of black hole and false data injection attacks in wireless sensor networks (Mohanapriya and Krishnamurthi, 2014)	R. Tanuja and M.K. Rekha	2013	A new acknowledgement based detection scheme which helps to simplify the removal of black holes and guarantees successful delivery of packets to destination. Their algorithm can successfully identify and eliminate 100% black hole nodes and ensures >99% packet delivery	NS2
Application of formal modeling to detect black hole attack in wireless sensor network routing protocols (Pati *et al*., 2013)	Kashif Saghar and David Kendall	2014	RAEED (Robust formally Analyzed protocol for wireless sensor networks Deployment) is developed routing protocol. Which is ableto address the problem of black hole attacks using formal modeling and proves that RAEED avoids such kind of attacks	NS2
Security against black hole attack in wireless sensor network. A review	Binod Kumar Mishra and Mohan C. Nikam	2014	They will prepare lightweight security model which validate the sensor node and then allow transmit true information to the base station	NS2
Detection and defense technology of blackhole Attacks in wireless sensor network (Devassy and Jayanthi, 2012)	Huisheng Gao, Ruping Wu	2014	In proposed technique, detection and prevention of blackhole attack to reduce the possibility of selecting a path having blackhole nodes in the route discovery process. This technique works effectively for analysis and defines blackhole attack	NS2
Acknowledgement-ased Trust framework for wireless sensor networks (Goyal *et al*., 2011)	X. Anita, J. Martin Leo Manickam	2014	Here, 2-ACKT-1 is proposed trust based evaluation framework. They showed that their protocol has better performance as compare to conventional multihop and trust based routing protocol for control overhead, packet delivery ratio and network life time. Malicious attackersare revealed by individual sensor node	NS2
Effect of black hole attack on single hop and Multihopleach protocol (Hu *et al*., 2006)	S. Iqbal, A. Srinivas, G. Sudarshan and S. Kashyap	2014	In this study, we are giving simulation results to information transmitted, number of alive hubs and comparing so as to linger vitality single bounce LEACH, multi jump LEACH and the impact of Black hole assault on them. The information transmitted is minimum in the multi jump LEACH system influenced by Black hole assault and most extreme in the system of single jump LEACH without assault.The simulation result is comparison between our modified proposed scheme and standard AODV. Throughput of novel scheme is higher thanoriginal AODV. End to end delay of our proposed novel scheme is lower than original AODV	NS2

CONCLUSION

There is no fix mechanism to detect or prevent the blackhole attack, researcher finds new methods to detect blackhole attack. And, also new methods will come because blackhole attack is active research area. The proposed protocol modifies the behavior of the original AODV to check the reliability of the received routes before sending the data packets. During the process of route discovery, for each node receives a RREQ, it checks the behavior of the broadcasting node. Once the behavior of the broadcasting node is normal, it is added to the trust table of the receiving node of the appropriate route. The RREP is over loaded with an extra field to indicate the reliability of the responding node. The value of the trust field is initialized to zero by the responding node and might be adapted by its previous hop during the trip of the RREP.

In case the trust field value equals to 1 or 2, the source node sends otherwise, the source node waits for further route. The protocol reduces the bad effects of the black hole problem and out performs the original AODV in terms of packet delivery ratio, number of dropped packets. For example, the results show that, when the node is attacked by two black hole nodes and the pause time is set to zero, the protocol out performs the original AODV by 10, 55, 40 and 12% regarding the mentioned above metrics, respectively. The main priority of the protocolis to send the data through reliable route. The protocol needto be supported by a technique to eliminate the black hole node from the network. Most of the researches need to be keen interest to reduce it.

REFERENCES

Abid, S. and S. Khan, 2014. Improving performance of routing protocols using MRP framework. Intl. J. Ambient Syst. Appl., 2: 1-8.

Alem, Y.F. and Z.C. Xuan, 2010. Preventing black hole attack in mobile ad-hoc networks using anomaly detection. Proceedings of the 2010 2nd International Conference on Future Computer and Communication (ICFCC), May 21-24, 2010, IEEE, Wuhan, China, ISBN: 978-1-4244-5821-9, pp: 663-672.

Arora, N. and N.C. Barwar, 2014. Performance analysis of black hole attack on different MANET routing protocols. Intl. J. Comput. Sci. Inf. Technol., 5: 4417-4419.

Bar, R.K., J.K. Mandal and M.M. Singh, 2013. QoS of MANet through trust based AODV routing protocol by exclusion of black hole attack. Proc. Technol., 10: 530-537.

Bhardwaj, A., 2014. Secure routing in DSR to mitigate black hole attack. Proceedings of the 2014 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), July 10-11, 2014, IEEE, Kanyakumari, India, ISBN: 978-1-4799-4191-9, pp: 985-989.

Bhosle, A.A., T.P. Thosar and S. Mehatre, 2012. Black-hole and wormhole attack in routing protocol AODV in MANET. Int. J. Comput. Sci., Eng. Appl., 2: 45-54.

Chavda, K.S. and A.V. Nimavat, 2013. Removal of black hole attack in AODV routing protocol of MANET. Proceedings of the 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), July 4-6, 2013, IEEE, Tiruchengode, India, ISBN: 978-1-4799-3925-1, pp: 1-5.

Dangore, M.Y. and S.S. Sambare, 2013. Detecting and overcoming blackhole attack in AODV protocol. Proceedings of the 2013 International Conference on Cloud & Ubiquitous Computing & Emerging Technologies (CUBE), November 15-16, 2013, IEEE, Pune, India, ISBN: 978-1-4799-2234-5, pp: 77-82.

Devassy, A. and K. Jayanthi, 2012. Prevention of black hole attack in mobile ad-hoc networks using MN-ID broadcasting. Intl. J. Mod. Eng. Res., 2: 1017-1021.

Garg, A. and V. Beniwal, 2012. A review on security issues of routing protocols in mobile ad-hoc networks. Intl. J. Adv. Res. Comput. Sci. Software Eng., 2: 145-148.

Goyal, P., V. Parmar and R. Rishi, 2011. MANET: Vulnerabilities, challenges, attacks, application. Int. J. Comput. Eng. Manage., 11: 32-37.

Hu, Y.C., A. Perrig and D.B. Johnson, 2006. Wormhole attacks in wireless networks. IEEE J. Selected Areas Commun., 24: 370-380.

Jaisankar, N., R. Saravanan and K.D. Swamy, 2010. A novel security approach for detecting black hole attack in MANET. Proceedings of the International Conference on Recent Trends in Business Administration and Information Processing, March 26-27, 2010, Thiruvananthapuram, India, pp: 217-223.

Kurosawa, S., H. Nakayama, N. Kato, A. Jamalipour and Y. Nemoto, 2007. Detecting blackhole attack on AODV-based mobile ad hoc networks by dynamic learning method. Int. J. Network Security, 5: 338-346.

Mistry, N., D.C. Jinwala and M. Zaveri, 2010. Improving AODV protocol against black hole attacks. Proceedings of the International MultiConference of Engineers and Computer Scientists, Volume 2, March 17-19, 2010, Hong Kong, pp: 1-6.

Mohanapriya, M. and I. Krishnamurthi, 2014. Modified DSR protocol for detection and removal of selective black hole attack in MANET. Comput. Electr. Eng., 40: 530-538.

Nath, I. and D.R. Chaki, 2012. BHAPSC: A new black hole attack prevention system in clustered MANET. Intl. J. Adv. Res. Comput. Sci. Software Eng., 2: 113-121.

Patil, P.N. and A.T. Bhole, 2013. Black hole attack prevention in mobile Ad Hoc networks using route caching. Proceedings of the 2013 Tenth International Conference on Wireless and Optical Communications Networks (WOCN), July 26-28, 2013, IEEE, Bhopal, India, ISBN: 978-1-4673-5997-9, pp: 1-6.

Rani, J. and N. Kumar, 2013. Improving AOMDV protocol for black hole detection in mobile ad hoc network. Proceedings of the 2013 International Conference on Control Computing Communication & Materials (ICCCCM), August 3-4, 2013, IEEE, Allahabad, India, pp: 1-8.

Salehi, M., H. Samavati and M. Dehghan, 2012. Evaluation of DSR protocol under a new black hole attack. Proceedings of the 2012 20th Iranian Conference on Electrical Engineering (ICEE), May 15-17, 2012, IEEE, Tehran, Iran, ISBN:978-1-4673-1149-6, pp: 640-644.

Sarma, K.J., R. Sharma and R. Das, 2014. A survey of black hole attack detection in MANET. Proceedings of the 2014 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), February 7-8, 2014, IEEE, Ghaziabad, India, pp: 202-205.

Savner, J. and V. Gupta, 2014. Clustering of mobile ad hoc networks: An approach for black hole prevention. Proceedings of the 2014 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), February 7-8, 2014, IEEE, Ghaziabad, India, pp: 361-365.

Sowmya, K.S., T. Rakesh and D.P. Hudedagaddi, 2012. Detection and prevention of blackhole attack in MANET using ACO. Intl. J. Comput. Sci. Netw. Secur., 12: 21-24.

Tamilarasan, S., 2011. A comparative study of multi-hop wireless ad-hoc network routing protocols in MANET. Intl. J. Comput. Sci., 8: 176-184.

Tan, S.C. and K. Kim, 2013. Secure route discovery for preventing black hole attacks on AODV-based MANETs. Proceedings of the 2013 IEEE 10th International Conference on High Performance Computing and Communications and 2013 IEEE International Conference on Embedded and Ubiquitous Computing (HPCC_EUC), November 13-15, 2013, IEEE, Zhangjiajie, China, pp: 1159-1164.

Ullah, I. and S. Anwar, 2013. Effects of black hole attack on MANET using reactive and proactive protocols. Intl. J. Comput. Sci., 10: 152-159.

Wei, Z., H. Tang, F.R. Yu, M. Wang and P. Mason, 2014. Security enhancements for mobile ad hoc networks with trust management using uncertain reasoning. Veh. Technol. IEEE. Trans., 63: 4647-4658.

Xiaopeng, G. and C. Wei, 2007. A novel gray hole attack detection scheme for mobile ad-hoc networks. Proceedings of the IFIP International Conference on Network and Parallel Computing Workshops NPC, September 18-21, 2007, IEEE, Liaoning, China, ISBN: 978-0-7695-2943-1, pp: 209-214.