International Journal of Electronics Communication and Computer Engineering
Volume 7, Issue 1, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

Novel Approach for Enhancing the Performance of MANETs Using Reactive Routing Protocols

Mrs. Bharathi M
Research Scholar, Department of ISE,MSRIT, Bangalore
bharathigowda1@gmail.com

Dr. Mydhili K Nair
Professor, Department of ISE,MSRIT, Bangalore
mydhili.nair@gmail.com

Abstract – **MANET is a type of wireless adhoc network and is a self configuring network of mobile nodes connected by wireless links. MANETs are suited for emergency situations as they facilitate fully distributed, self-maintainable dynamic topology networks that applications are limited as its features impart high applicability, yet they manifest unreliability. Another cause of unreliability is the mutual intrinsic trust during communication. Security is a major challenge for these networks due to their features of open medium, dynamically changing topologies. The Black Hole attack is a well known security threat of exploiting the trustworthiness.**

Black hole attack is one of the security threats in which attacker node drops or modify the packets intentionally hence decreasing reliability. In black hole attack an adversary captures a set of nodes in the network to block the packets they receive instead of forwarding them towards the destination. As a result any information that enters the black hole region is captured and does not reach the destination. Due to this attack, high end to end delay and throughput is degraded in the network.

In this paper is to detect and prevent the effects of Black hole attack in MANET using Ad-Hoc on Demand Distance Vector (AODV) and analyse MANETs using single and cooperative Black Hole attack and avoid it by diverting traffic from the Black Hole. The proposed method is based on sending packet confirmation that are verified by the destination to check for Black Hole presence in the proposed AODV and encrypt the data before sending it to destination. The proposed algorithm was then simulated in static node environment and results are observed that the packet delivery ratio is better than the conventional AODV.

Keywords – **Black Hole, AODV, MANETs, Security, Reliability, Routing.**

I. Introduction

A MANET is a collection of mobile nodes forming a network without any supporting infrastructure. Nodes in MANET can join and leave the network dynamically. There is no fixed set of infrastructure and centralised administration. Nodes are connected through wireless interface. The dynamic nature of such type of network make it highly susceptible to various attacks. As transmission takes place in open medium makes the MANET more vulnerable to security attacks can be reduced. There are many attacks that the MANETs are exposed to, these attacks can be classified as active and passive attacks. In active attacks the adversary breaks into the system and is able to insert and capture transmissions thus modifying or corrupting the data whereas in passive attacks the adversary merely listens to the traffic and extracts information from the transmissions. The increasing rate and extent of black hole attacks raise concerns for a defensive mechanism that has the properties of being preventive as well as curative. Therefore this paper is an attempt to defend against "Black hole" attack that compromises reliability of the networks by dropping all data packets routed towards them.

Black hole attack [1] is a kind of denial of service attacks. In this attack, a malicious node advertises that it has the best path to the destination node during the route discovery process. one of the security threats 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 challenging issue.

Existing the work done on Black Hole attack involved in MANET were based on different routing protocols. Black Hole attack is studied under the AODV routing protocol and its effects are elaborated by stating how this attack disrupt the performance of MANET. Attention has been given to the fact to study the impact of Black Hole attack in MANET using Reactive protocol like AODV and the proposed enhanced AODV, to compare the vulnerability of both these protocols against the attack.

II. Literature Review on MANETs

Mobile Ad-Hoc Network is a self organising, self managing network with mobile wireless nodes. All nodes are move freely in any direction, at any speed, which leads unpredictable topology of MANET. MANETs created a new set of demands to be implemented and to provide efficient end to end communication. To transfer the information the nodes need to obey a set of protocols. These protocols are called as routing protocols.

Classification of MANETs Routing Protocols

Routing protocols in MANETs are classified into three different categories according to their functionality

1. Reactive protocols
2. Proactive protocols
3. Hybrid protocols

The hierarchy of these protocols is shown below in the Fig. 1.

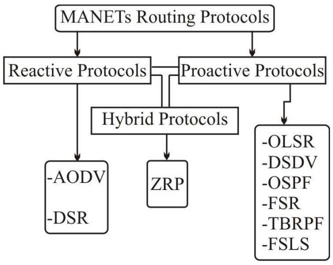

Fig. 1. MANETs Routing Protocols

Copyright © 2016 IJECCE, All right reserved

Proactive routing protocols(table driven): It maintains predetermined up to date routing information from one node to the other within the network. Every time a route is needed from a source to destination, the routing information is used from the routing table that the nodes has.

Reactive routing protocols(demand driven): These protocols do not initiate route discovery by themselves, until they are requested, when a source node request to find a route. These protocols setup routes when demanded[3,4]. When a node wants to communicate with another node in the network and the source node does not have a route to the node it wants to communicate with, reactive protocols will establish a route for the source to destination node.

Hybrid routing protocols: These protocols use the combination of both proactive and reactive protocols , it inherits the advantages of both the protocols.

III. AODV Routing Protocol and Black Hole Attack

A. Adhoc On Demand Distance Vector [AODV]:

AODV[2] is one of the effective routing protocol in MANET. In this protocol when a node needs a path to a destination, it has to find a path. It uses three routing packets in the process of route discovery.

1. RREQ: Route Request

RREQ packet generated by the source to find a path to the destination. AODV floods RREQ message using expanding ring technique. Time to live (TTL) value is present in every RREQ message, the value of TTL states the number of hops the RREQ should be transmitted.

2. RREP: Route Reply

RREP is generated by the intermediate node(IN)which have a fresh enough route to the destination. A node having a requested identity or any intermediate node that has a route to the requested node generates a route reply RREP message back to the originator node.

3. RERR: Route Error

Every node in the network keeps monitoring the link status to its neighbour's nodes during active routes. When the node detects a link crack in an active route, RERR message is generated by the node in order to notify other nodes that the link is down.

B. Black Hole Attack:

Black Holes are maliciousnodes that follows the following features of AODV:

1) AODV does not perform authentication of a new node during its entry in a MANET.

2) It does not verify the route promised by any node. Black Hole node's motive is to divert all the data traffic in the network toward itself.

Black Holes send RREP's to the source node with the least hop count or highest sequence numbers. Since Black Holes do not search their routing tables before generating a reply, they usually are the quickest. Thus, the RREP packet so received from the black hole is the first and appears to bear the latest network configuration, causing the source to route towards the Black Hole. The Black Hole node finally drops these data packets.

Black Hole attacks can be independent, that is, performed by a single malicious node or can be collaborative as shown in Fig 2 and Fig 3

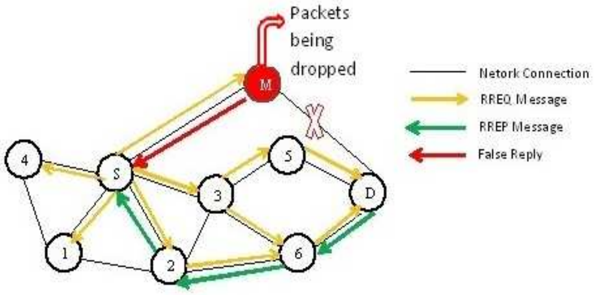

Fig. 2. Black Hole Attack(single black hole attack)

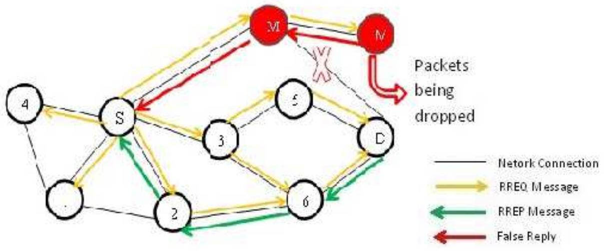

Fig. 3. Black Hole Attack (cooperative black hole attack)

Black Hole attacks can be independent, that is, performed by a single malicious node or can be collaborative as shown in Fig. 2 and Fig. 3

In Fig.2 the operation of a single black hole attack is portrayed. 'S' being a source node broadcasts the RREQ message to all the nodes for the route discovery. 'M' being the malicious node sends a false reply as a RREP message back to the source even it does not have a network connection with the destination node. The source gets replies from different nodes but malicious node gives the shortest path it has a high probability of getting selected if the malicious node is not identified. If the path is selected the malicious node gets all the required information resulting in drastic amount of packet loss. Fig. 3 depicts a cooperative black hole attacks where two malicious nodes work in cooperation making the identification of the malicious node even more difficult. These type of attack may also include more than two malicious nodes.

IV. Related Work

A number of solutions to handle the black hole attack have been proposed.

Table I. Summary of attacks and counter measures

Technique proposed by	Method/solution	Modifies AODV/ Routing tables	Type of black hole attack	Drawbacks
Kamarularifin Abd. Jalil, Zaid Ahmad, Jamalul-Lail Ab Manan, 2011 [5].	Enhance Route Discovery for AODV (ERDA)	yes	Single black hole	Co operative black holes
Mohammad Abu Obaida, Shahnewaz Ahmed	Compares the RREP sequence	no	Single black hole	Cannot detect co-operative

Faisal, Md. Abu Horaira, Tanay Kumar Roy, 2011 [6]	numbers. With threshold value and selects the Routes			black hole nodes.
Ming-Yang Su; Kun-Lin Chiang; Wei-Cheng Liao, Sept. 2010 [7].	Anti black hole mechanism(ABM) using IDS	yes	Multiple black hole	Time delay
Songbai Lu; Longxuan Li; Kwok-Yan Lam; Lingyan Jia, Dec. 2009 [8].	Using SRREQ and SRREP based on the random numbers generation	no	Single black hole	Time delay and network overhead
Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon, and Kendall Nygard,2003[4]	'THROUGH' and 'FROM' bit in the DRI table to detect the collaborative Black Hole Chains	yes	Multiple black holes	redundant bit transmissions of 'THROUGH' bits.
Watchara Saetang, Sakuna Charoenpanyasak , 2012[9]	credit based mechanism is used to detect the Black hole attack.	no	Single black hole	redundant bit transmissions
Neelam Khemariya , Ajay Khuntetha,2013[10]	Uses Threshold and Sequence numbers for detection of Black hole attack.	no	Single black hole	Increased Network Overhead and Communication overhead
P. K. Singh and G. Sharma,2012[11]	Uses 'hello'packets and also uses promiscuous mode in each node	no	Single black hole	Can't detect co-operative black hole.

V. The Proposed Algorithm: DB-AODV Protocol

The AODV protocol has a provision of sending a RREP packet to the destination node. Whenever an intermediate node has a route towards destination, it also unicasts a gratuitous RREP to the destination node. In our protocol the gratuitous RREP is conceptualized and simulated as the CONFIRM packet. Thus, a CONFIRM packet is unicasted/ routed by the RREPN1 to the destination. Note that it can be sent only if the RREPN1 has a route towards destination. It is only after the receipt of CONFIRM will the destination await for packets from the source.

The source unicasts a CHCKCNFRM to the destination through RREPN2. Upon CHCKCNFRMs receipt the destination replies by unicasting a REPLYCONFIRM with a key to the source, only if it received a CONFIRM and a CHCKCNFRM. Since a black hole does not possess a route towards the destination, it fails to send the CONFIRM, thus reply to the CHCKCNFRM is never generated by the destination. This leads the source to conclude that the RREP sending node was the black hole one and route the data through RREPN2 node.

The proposed algorithm can be called as the **DB-AODV** protocol i.e. **Detection of Black hole using AODV**. It gets its name because it detects and divert the data transfer through other route where there is no black hole.

The proposed DB-AODV method uses the same RREQ and RREP messages for route discovery process of classical AODV and apart from that it also uses the three important mechanisms.

These three modules are:

1. Destination Finding Process
2. CHECK CONFIRM and REPLY CONFIRM process
3. File sending Process

The data flow diagram for the proposed DB -AODV is shown below:

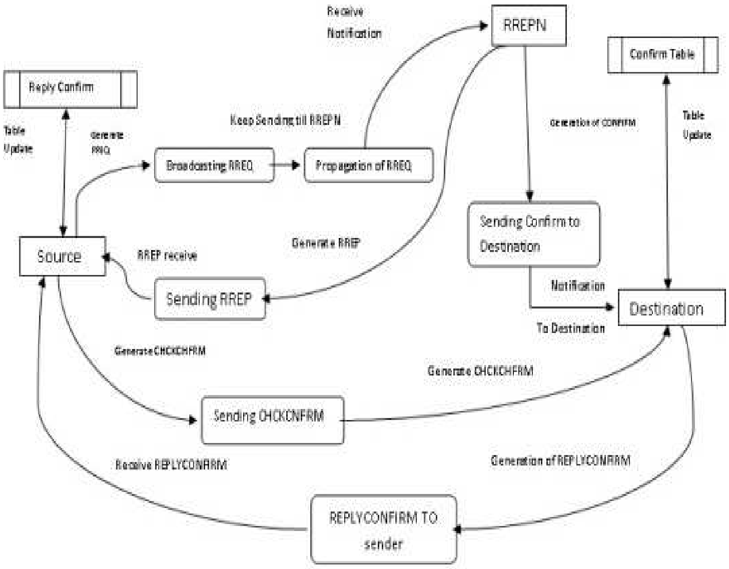

Fig. 4. Data Flow Diagram of proposed DB-AODV

The following figures shows the sequence diagrams for the above modules

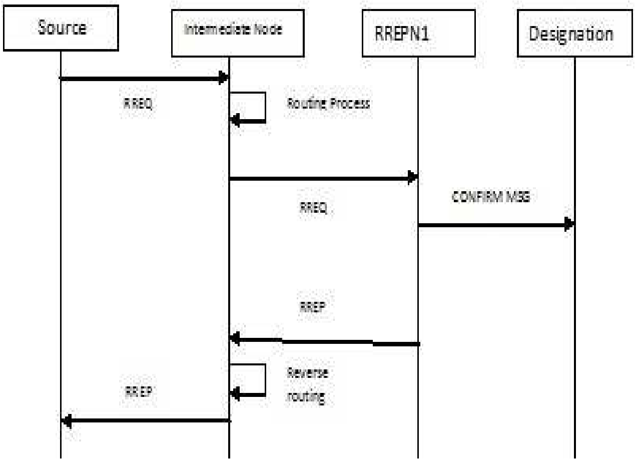

Fig. 5. Destination finding process through RREPN1

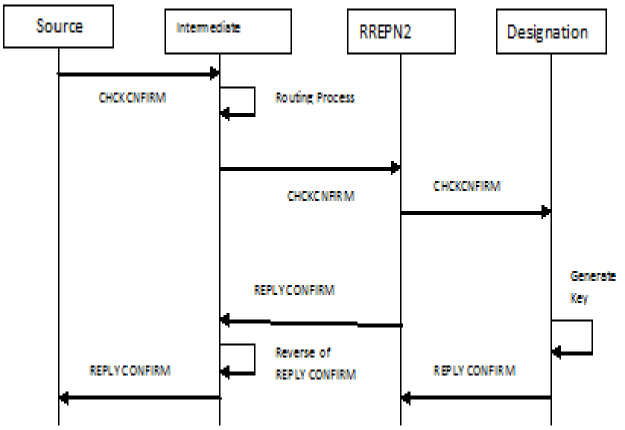

Fig. 6. CHECKCONFIRM and REPLAYCONFIRM process

Copyright © 2016 IJECCE, All right reserved

VI. Simulation and Results

The analysis is carried on performance of BD-AODV and AODV. The most commonly used quantitative indicators are used to judge the performance of the routing protocol: Data Delivery Ratio, and Average End to End delay versus number of black holes in both the protocols.

1. Average End to End Delay versus number of Black Holes(Fig 7)- The average end to end delay is the average time taken to send data from source to destination. It is observed that Average End to End Delay of DB-AODV is less when compared to AODV.

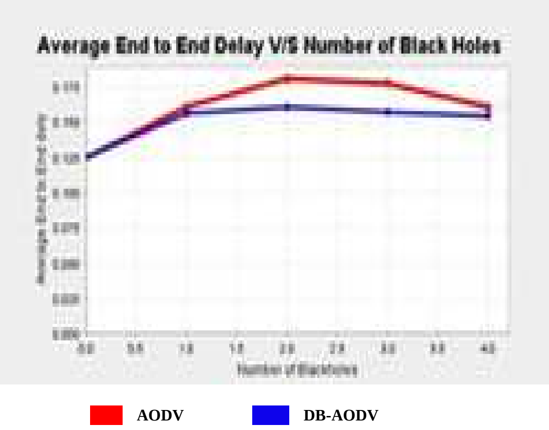

Fig. 7. Average End to End delay Versus Number of Black holes

2. Throughput Vs Number of Black Holes(Fig.8)- The throughput can be defined as number of data packets transmitted per unit time. Higher the throughput, higher will be the performance of the routing protocol. The throughput of DB-AODV is higher than the AODV.

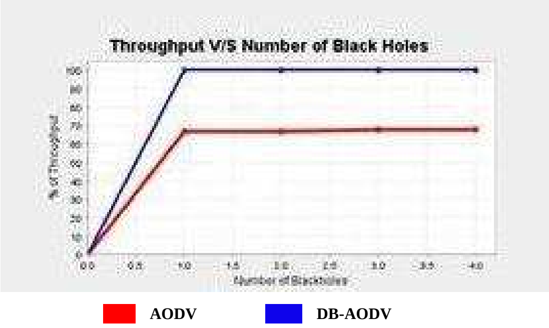

Fig. 8. Throughput Vs Number of Black Holes

VII. Conclusion

Reliable data delivery is one of the important issue in MANETs. The simulation results are analysed for the presence of black hole in both classical AODV and proposed DB-AODV. With the control packets called confirm, CHCKCNFRM and REPLYCONFIRM, the presence of black hole is detected and hence successfully diverted all the traffic from it. The proposed protocol shows that a single run of the algorithm can detect the presence of single and collaborative black hole nodes. The proposed protocol can achieve maximum reliability by detecting black hole and sending the encrypted data by diverting the route traffic. As a part of future endeavour, the aim is to study the processing time the black holes, to analyse their behaviour. Also we would work upon decreasing the number of packets transmitted per route in our algorithm.

VIII. Acknowledgement

I would like to thank my guide Dr. Mydhili K Nair, Professor, department of ISE, MSRIT, without her motivation, assistance and dedicated involvement in every step to make this paper accomplished. Also I would like to thank Dr. Chandrashekara S.N, HOD of department of CSE for his immense time support throughout the entire process to take this paper in right path.

References

[1] A. Jain and V. Tokekar. “Classification of denial of service attacks in mobile ad hoc networks,” Proceedings of International Conference on Computational Intelligence and Communication Networks (CICN), pages 256–261, 2011

[2] N Marchang and R Datta,” lighe weight trust bsed routing protocol from mobile adhoc networks”, information security, IET, Vol. 6, PP. 77-83, 2012.

[3] Deng H., Li W. and Agrawal, D.P., ”Routing security in wireless ad hoc networks,”Communications Magazine, IEEE , vol.40, no.10, pp. 70- 75, October, 2002.

[4] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon, and Kendall Nygard, Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks, Proceedings of 2003 International Conference on Wireless Networks (ICWN03), Las Vegas, Nevada, USA, pp. 570-575.

[5] Kamarularifin Abd. Jalil, Zaid Ahmad, Jamalul-Lail Ab Manan, “Mitigation of Black Hole Attacks for AODV Routing Protocol”, Society of Digital Information and Wireless Communications (SDIWC) Vol01_No02_30, 2011.

[6] Mohammad Abu Obaida, Shahnewaz Ahmed Faisal, Md. Abu Horaira, Tanay Kumar Roy, “AODV Robust (AODVR): An Analytic Approach to Shield Ad-hoc Networks from Black Holes” International Journal of Advanced Computer Sciences and Applications, Vol: 2 Issue: 8 Pages: 97-102, 2011.

[7] Ming-Yang Su; Kun-Lin Chiang; Wei-Cheng Liao, "Mitigation of Black-Hole Nodes in Mobile Ad Hoc Networks," Parallel and Distributed Processing with Applications (ISPA), 2010 International Symposium on, vol., no., pp.162-167, 6-9 Sept. 2010.

[8] Songbai Lu; Longxuan Li; Kwok-Yan Lam; Lingyan Jia, "SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack," Computational Intelligence and Security, 2009. CIS '09. International Conference on, vol.2, no., pp.421-425, 11-14 Dec. 2009.

[9] Watchara Saetang, Sakuna Charoenpanyasak ”CAODV Free Blackhole Attack in Ad HocNetworks”, International Conference on Computer Networks and Communication Systems (CNCS 2012)IPCSIT vol.35(2012) © (2012) IACSIT Press, Singapore.

[10] Neelam Khemariya , Ajay Khuntetha ,” An Efficient Algorithm for Detection ofBlackhole Attack in AODV based MANETs “,International Journal of ComputerApplications (0975 – 8887) Volume 66– No.18, March 2013.

[11] P. K. Singh and G. Sharma, "An Efficient Prevention of Black Hole Problem in AODV Routing Protocol in MANET," in 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), IEEE, 2012, pp. 902-906.

Author's Profile

Mrs. Bharathi. M is presently working as associate professor at S.J.C.I.T, chickballapur, india. She is a Research student of Information science department, MSRIT, Bangalore.

Dr. Mydhili K Nair is working as Professor in information Science and engineering at MSRIT, Bangalore.

Copyright © 2016 IJECCE, All right reserved