Approach for detecting Black hole attack in MANETs

Gaurav Gupta
Dept. of Computer Science & Engg.
NIT, Bhopal
India

Dr. R. K. Pateriya
Associate Professor
Dept. of Computer Science & Engg.
NIT, Bhopal
India

Abstract

Black Hole attack is a serious threat in the modern era of mobile Ad Hoc network. In this attack when a sender node wants to communicate to the destination. A malicious node sends a reply with a shortest path or highest sequence number. In view of that sender sends the entire data packet through the malicious node and all the data dropped. Every conventional method to detect such an attack has a defect of high rate of failure. In order to overcome from this security issue, we propose a new detection method based on confirmation of route to destination and also propagates the information of malicious node to all other nodes in the network. The simulation results with graph show the efficiency of the proposed method. As it is obvious that once malicious node detected the throughput of the network will not get affected due to presence of black hole in attack.

1. Introduction

Mobile Ad-hoc network (MANET) consists of wireless mobile nodes that are communicate without any infrastructure i.e., MANET is a self organized network [4].

Features of MANET are no fixed infrastructure, automatic self configuration and maintenance, quick deployment, no centralized administration etc. In MANET, there is no infrastructure so every node is free to join, leave and move independently. As a result, the network topology changes rapidly and unpredictably, and connectivity among the terminal vary with the time. It requires nodes to dynamically establish routing among themselves and form the network on the fly.
Moreover, as the mobility leads to fluctuations in the link capacity, the nature of high bit error rate of wireless connection is more profound in MANET. In the absence of a central control of the network operation, the control and management of the network is distributed among the terminals; the nodes are required to collaborate amongst themselves. Moreover, the flexibility of mobile nodes results in a dynamic topology [1]. Therefore, it is hard to develop a secure routing protocol in MANET in comparison to traditional wired network because of additional problems and challenges. However, several routing algorithms are available in the literature which may be categorized as proactive, reactive, and hybrid on the basis of routing information update mechanism [11]. Proactive or table-driven routing algorithms maintain the network topology information in the form of routing tables which are exchanged periodically to keep them update. Whenever a node requires a path to a destination it runs a path-finding algorithm as per its routing table. Few examples of such routing algorithms are DSDV [12], WRP [13], and CGSR [14]. Reactive or on-demand routing protocols do not maintain network topology. They seek and obtain a path as and when required. Few examples of such routing algorithms are DSR [15], AODV [2, 16], and ABR [17]. Hybrid routing protocols combine the best features of both proactive and reactive protocols. These algorithms use reactive approach when the destination is within the range and use proactive approach when the destination is outside the range. Few examples of such routing algorithms are CEDAR [18], ZRP [19], and ZHLS [20]. Because of their inherent characteristics, MANETs are more vulnerable to attacks. These attacks are generally

classified as active attacks and passive attacks [21].

Table 1 Classification Of Security Attacks[3]

Active attacks	Spoofing, Fabrication, Wormhole Attack, Modification, Denial of Service, Sinkholes, Sybil Attack
Passive Attacks	Eavesdropping, traffic analysis, monitoring

1.1. Active Attacks

Active attacks are the attacks that are performed by the malicious nodes that bear some energy cost in order to perform the attacks. Active attacks [8] involve some modification of data stream or creation of false stream.

1.2. Passive Attacks

In passive attacks the attacker does not disturb the routing protocol, instead try to extract the valuable information like node hierarchy and network topology from it. Passive attack [10] is in nature of eavesdropping on, or monitoring of transmission. The goal of opponent is to obtained information that is being transmitted [5]. Passive attacks are very difficult to detect because they do not involve any alteration of data.

Other Advanced attacks:-

- Black hole attack
- Byzantine attack
- Rushing attack
- Replay attack
- Location disclosure attack

1.3. Black hole attack

A Black hole attack is a kind of denial service where a malicious node can attract all packets by falsely claiming a fresh route to the destination and then drop all the packets without forwarding them to the destination. When the source node wants to transmit a data packet to the destination, it first sends out the RREQ packet to the neighbouring nodes. As malicious nodes are existing in the network, it will immediately send RREP and source node just send all the packets through that node and malicious node simply drop all the packets, instead of forwarding to the destination.

2. Related work

There are many approaches that are proposed to overcome from Black Hole Attack and to defend the attack have been proposed. According to Algorithm proposed by Deng et al. [5], every node crosses check with its next hop node on the route to the destination on receiving or overhearing a RREP packet. If the next hop node does not have a link to the node that sent the RREP, then the node that sent the RREP is considered as malicious. This solution assumes that there exists at most one malicious node and thus not cover the case with two or more malicious node, which is quite possible in real solutions. An algorithm proposed in [6] detects the black hole attack in a MANET which is based on relationships of a certain trust level among the nodes. However in the real network it is quite impossible to set an value for the trust level. In the method [7], every node has a function of learning the traffic flow in the network and evaluating the possibility criterion of black hole attack based on such learning results in order to detect the malicious node. If the value of criterion is larger than a predetermined threshold, the node judges that there exists a black hole attacker. This methods provide only detection of a single black hole attacker and cannot detect a chain of malicious nodes co-operate with each other. In the method [9] this mode allows a node to intercept and read each network packet that arrives in it's entirely, In other words, it is based on promiscuous mode means that if a node within the range of other node , it can overhear communication to and from other node even if those communication do not directly involve node.

3. The Proposed Method

In this paper, an approach has been proposed to combat black hole attack in AODV routing protocol.

3.1. Motivation

As all the techniques proposed above are not very effective to overcome from Black Hole Attack Problem. In most of the above methods can detect only one black hole attacker and do not provide an effective mechanism to cover the situation with more than one attacker in the network.
To defend against the black hole attack and to overcome the disadvantages listed above, we propose a new detection method based on the confirmation from destination node.

3.2. ALGO FOR DETECTION OF BLACK HOLE ATTACK (DAODV)

Step 1: Source node initiate RREQ message for delivering packet to destination.

Step 2: Any Intermediate node which has a route to the destination node, generates RREP message to the source node.

Step 3: On receiving the first RREP message , the source node set the clock and waits for a time t for receiving some more RREP messages. In case if there is no RREP message received by the source node it enters in the random back off time and again initiate the RREQ message.

Step 4: RREP message which has least HOP count is selected and a RRPD_chk message is sent to the node from which RREP message was sent.

Step 5: On receiving the RRPD_chk message from the source, the intermediate node forwards this to the destination through the defined path.

Step 6: On receiving the RRPD_chk message the destination node changes the bit from 0 to 1.

Step 7: The source node waits for a RRPD_chk message for the time t. On receiving RRPD_chk message source node will check the bit and if it is 1.
Source node sends data packets through the intermediate node.
Else
{
Broadcast the ID of that intermediate node as a black hole.
Go to step 4 and try other RREP messages received by source node till the source node receives RRPD_chk message from destination node. }

4. Simulation Results & Discussion

To evaluate the performance of our solution and compare it with AODV and the solution proposed by this proposed method, we consider the following performance metrics.
Throughput
Packet Delivery ratio.
End to End Delay
No. of Packet routed through malicious node
No. Of Malicious Node detected.

Table 2 Simulation Scenario

Examined protocols	AODV & DAODV
Simulation time	1000 seconds
Simulation area (m x m)	1000 x 1000
Number of Nodes	600
Malicious Node	5 to 25
Traffic Type	TCP
Performance Parameter	Throughput, End to End Delay, Packet Delivery Ratio, No. of Packet routed through Malicious Node, No. of Malicious Node detected
Mobility (m/s)	10 to 90 m/s
Packet Inter-Arrival Time (s)	exponential(1)
Packet size (bits)	8 bits

Transmit Power(W)	0.005
Date Rate (Mbps)	11 Mbps
Mobility Model	Random waypoint

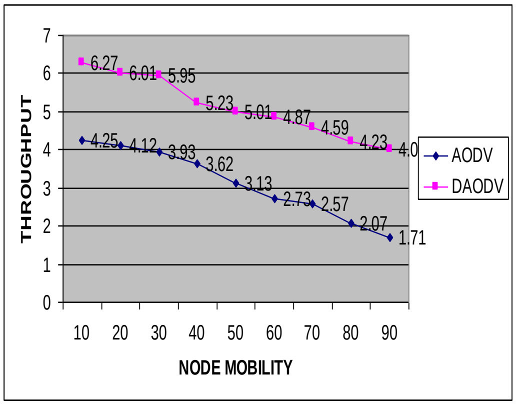

Figure 1. Node mobility vs Throughput

Figure 1 depicts that in presence of 25 malicious node, Network Throughput is well maintained in proposed DAODV.

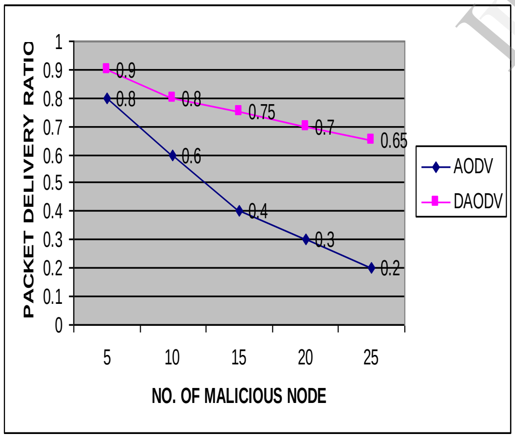

Figure 2 No. of Malicious Node vs Packet delivery ratio.

Figure 2 depicts when malicious node increases from 5 to 25, it is obvious that the packet delivery ratio of proposed DAODV protocol is quite high.

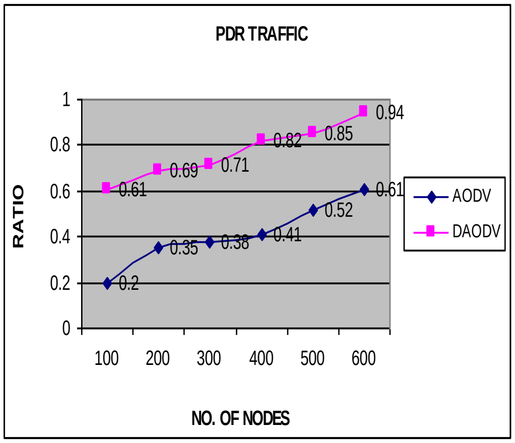

Figure 3. No. of node vs PDR

Figure 3 depicts that when no. of node increases from 100 to 600 it is obvious from figure that PDR in proposed DAODV method is considerably good.

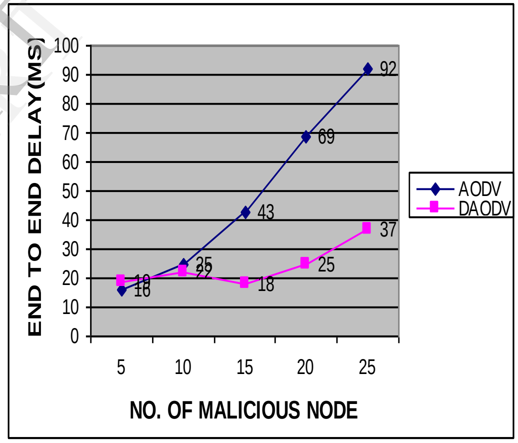

Figure 4. No. of malicious node vs End to End Delay(milli seconds)

Figure 4 depicts that when no. of malicious node increases from 5 to 25 it is very clear from the figure that the End to End delay is considerably low in proposed DAODV method.

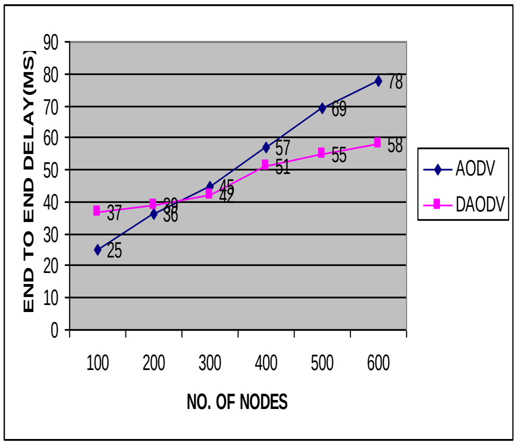

Figure 5. No. of node vs End to End Delay (milli seconds)

Figure 5 depicts that when no. of node increases from 100 to 600, the End to End delay is less in proposed method.

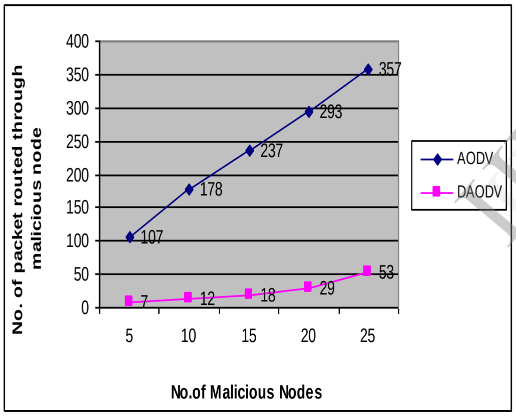

Figure 6. No. of malicious node vs No. of packet routed through malicious node

Figure 6 depicts that when no. of malicious node increases from 5 to 25 it is very clear from the figure that the packet routed through malicious node is very less in proposed DAODV method.

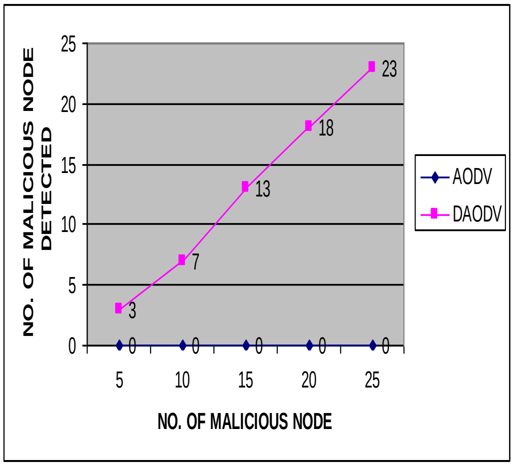

Figure 7. No. of Malicious node detected

Figure 7 depicts that when no. of malicious node increases from 5 to 25 it is very clear from the figure that the no. of malicious node detected in proposed method is considerably good.

5. Conclusion

In this paper, we proposed a new destination confirmation method, which can effectively detect the black hole attack in MANETs. In this method source just wait for confirmation message from destination, only after that it will start sending packet through that route. The simulation results have demonstrated that our method shows significant effectiveness in detecting the black hole attack.

6. Refrences

[1] Elizabeth M, Royer, and Chai-Keong Toh: "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks," IEEE Personal Communications, pp. 46-55, (April 1999)
[2] C.E. Perkins, S,R, Das, and E. Royer: "Ad-hoc on Demand Distance Vector(AODV)", RFC 3561
[3] H. Lan Nguyen and U, Trang Nguyen: "A study of different types of attacks on multicast in mobile ad hoc networks", Ad Hoc Network, VoI.6, No. I, (2007)
[4] L. Zhou and Z. 1. Haas: "Securing Ad Hoc Networks", IEEE Network Magazine, Vol.13, No.6, (November/December 1999)

[5] H. Deng, W. Li, and D. P. Agrawal: "Routing security in wireless ad hoc network". IEEE Communications Magazine, pages 70- 75, (2002)

[6]Latha Tamilselvan, V. Sankaranarayanan: "Prevention of Black Hole Attack in MANEr", The 2nd international conference on wireless, Broadband and Ultra Wideband Communications (January 2007)

[7] Mohanmmad AI-Shurrnan et al: "Black Hole Attack in Mobile Ad Hoc Network", ACMSE' 04, (April 2004)

[8] Jean-Pierre Hubaux, Levente Buttyan, Srdjan Capkun,"The Quest for security in Mobile Ad Hoc Networks". Proceedings of the 2010 ACM International Symposium on Mobile ad Hoc networking & computing, Long Beach, CA. 2001.

[9] Pramod Kr. Singh, Govind Sharma, "An Efficient Prevention of Black hole Problem in AODV Routing Protocol in MANET", IEEE Computer Society 2012, p.p. 902-906.

[10] Rakesh kumar Sahu, Narendra S. Chaudhari, "Performance Evaluation of Ad hoc Network Under Black hole Attack" IEEE 2012, 978-1-4673-4805-8/12 pp. 780-783

[11] C. Siva Ram Murthy and B.S. Manoj, "Ad Hoc Wireless Networks: Architectures and Protocols", Prentice Hall, 2004.

[12] C. K. Perkins and P. Bhagwat, "Highly Dynamic Destination- Sequenced Distance-Vector Routing (DSDV) for Mobile Computers", Proceedings of ACM SIGCOMM 1994, August 1994, pp. 234-244.

[13] S. Murthy and J. J. Garcia-Luna-Aceves, "An Efficient Routing Protocol for Wireless Networks", ACM Mobile Networks and Applications Journal, Special Issue on Routing in Mobile Communication Networks, Vol. 1, No. 2, October 1996, pp. 183-197.

[14] C. C. Chiang, H. K. Wu, W. Liu and M. Gerla, "Routing in Clustered Multi-Hop Mobile Wireless Networks with Fading Channel", Proceedings of IEEE SICON 1997, April 1997, pp. 197-211.905

[15] D. B. Johnson and D. A. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks", Mobile Computing, Kluwer Academic Publishers, Vol. 353, 1996, pp. 153-181.

[16] C. E. Perkins and E. M. Royer, "Ad Hoc On-Demand Distance Vector Routing", Proceedings of IEEE Workshop on Mobile Computing Systems and Applications 1999, February 1999, pp. 90-100.

[17] C. K. Toh, "Associativity-Based Routing for Ad Hoc Mobile Networks", Wireless Personal Communications, Vol. 4, No. 2, March 1997, pp. 1-36.

[18] P. Sinha, R. Sivakumar and V. Bharghavan, "CEDAR: A Core Extraction Distributed Ad Hoc Routing Algorithm", IEEE Journal on Selected Areas in Communications, Vol. 17, No. 8, August 1999, pp. 1454-1466.

[19] Z. J. Hass, "The Routing Algorithm for the Reconfigurable Wireless Networks", Proceedings of ICUPC 1997, Vol. 2, October 1997, pp. 562-566.

[20] M. Jao-Ng and I. T. Lu, "A Peer-to-Peer Zone-Based Two-Level Link State Routing for Mobile Ad Hoc Networks", IEEE Journal on Selected Areas in Communications, Vol. 17, No. 8, August 1999, pp. 1415-1425.

[21] Loay Abusalah, Ashfaq Khokhar and Mohsen Guizani, "A Survey of Secure Mobile Ad Hoc Routing Protocols," IEEE Communications Surveys & Tutorials, Vol 10, No. 4, 2008, pp. 78-93.