Mitigate Black Hole Attack In Dynamic Source Routing (DSR) Protocol By Trapping

K.Mahamuni[1*] and Dr.C.Chandrasekar[2]

[1*]Assistant Professor, Department of Computer Applications, Government Arts College(Autonomous), Salem-7, TamilNadu, India.

[2]Associate Professor, Department of Computer Science, Periyar University, Salem-11, TamilNadu, India.

Abstract

Ad hoc network maximize the total network throughput by using all available nodes for routing and forwarding. MANETs are highly vulnerable to attacks than wired networks due to the open medium, dynamically changing network topology, cooperative algorithms, and lack of centralized monitoring. Hence, a node can misbehave and fail to establish route or route the data due to its malicious activity to decrease the performance of ad hoc network. In this paper, a method to mitigate the malicious nodes forming black hole attack in dynamic ad hoc network is proposed. This paper studies black hole attack impact in ad hoc networks with DSR routing protocol when the nodes are mobile.The proposed routing is based on DSR and is modified with detection algorithm. It is divided into two phases: Detection before route establishment and avoidance of malicious nodes during data forwarding. The silent feature of proposed scheme is its simplicity and effectiveness in detecting malicious nodes.

Keywords: *Ad hoc network, network attacks, Dynamic Source Routing (DSR), Black Hole Attack, Trap Header(TH).*

1. Introduction

Mobile Ad hoc Networks (MANET) are utilized to set up wireless communication in improvised environments without a predefined infrastructure or centralized administration [1]. MANET has been normally deployed in adverse and hostile environments where central authority point is not necessary. Another unique characteristic of MANET is the dynamic nature of its network topology which would be frequently changed due to the unpredictable mobility of nodes [2]. Furthermore, each mobile node in MANET plays a router role while transmitting data over the network. Hence, any compromised nodes under an adversary's control could cause significant damage to the functionality and security of its network since the impact would propagate in performing routing tasks.

Because these networks are temporary, they can be attacked from within, due to being constructed without protection, in poor conditions. Attacks are also launched if nodes are compromised. Another issue is the node number. Hundreds/thousands of nodes might be required in a network and security measures undertaken must be efficient and cost-effective for a vast network. Exchange of topological information among nodes is facilitated by routing protocols to establish routes and this is used by attackers for acts including bogus routing, incorrect forwarding, lack of error messages, restricted reply time, thereby leading to retransmission and inefficient routing[3]. Several work addressed the intrusion response actions in MANET by isolating uncooperative nodes based on the node reputation derived from their behaviors. Such a simple response against malicious nodes often neglects possible negative side effects involved with the response actions. In MANET scenario, improper countermeasures may cause the unexpected network partition, bringing additional damages to the network infrastructure. To address the above-mentioned critical issues, more flexible and adaptive response should be investigated.

Common attacks faced by networks include blackhole, grey hole and wormhole attacks, and IP spoofing[4]. Black hole attacks are malicious nodes that refuse to forward traffic[5]. External attacks can typically be prevented by using standard security mechanisms such as firewalls, encryption and so on. Internal attacks are typically more severe attacks, since malicious insider nodes already belong to the network as an authorized party and are thus protected with the security mechanisms the network and its services offer. Thus such malicious insiders who may even operate in a group may use the standard security means to actually protect their attacks. These kind of malicious parties are called compromised nodes, as their actions compromise the security of the whole ad hoc network.

In black hole attack, 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. 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 [6, 7].

The method how malicious node fits in the data routes varies. Figure 1 shows how black hole problem arises, here node "A" want to send data packets to node "D" and initiate the route discovery process. So if node "C" is a malicious node then it will claim that it has active route to the specified destination as soon as it receives RREQ packets. It will then send the response to node "A" before any other node. In this way node "A" will think that this is the active route and thus active route discovery is complete. Node "A" will ignore all other replies and will start seeding data packets to node "C". In this way all the data packet will be lost consumed or lost.

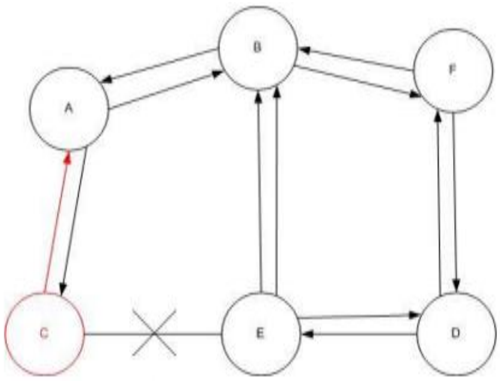

Figure 1: Black Hole Attack

In this paper, the proposed routing is based on DSR and is modified with detection algorithm. It is divided into two phases: Detection during route establishment and Detection during data forwarding. The silent feature of proposed scheme is its simplicity and effectiveness in detecting malicious nodes even when the network is highly dynamic. The rest of paper is organized as follows: Section 2 deals with the related works, Section 3 describes the methodology, Section 4 details the results and discussion, and section 5 concludes the paper.

2. Related Works

Hu et al.[8] presented a new protocol 'Ariadne' based on the DSR protocol for routing protection. Several authentication mechanisms such as digital signatures, MACs computed with pair-wise secret keys, or TESLA could be used with the proposed protocol. Hash chains are used to authenticate every route request protecting the network from overload, thus denial of service attacks are prevented. Attacks from compromised nodes from tampering with the uncompromised nodes are also prevented by the proposed method. Combinations of TESLA authenticators (MACs) are added by intermediate routers and a hashing technique to protect the discovered routes. The proposed method's security mechanisms are effective and can also be applied to wide variety of routing protocols.

Bhalaji et al.[9] analysed the black hole and cooperative black hole attack which is one of the new and possible attack in ad hoc networks. In this attack a malicious node advertises itself as having the shortest path to the node whose packets it wants to intercept. To reduce the probability it is proposed to wait and check the replies from all the neighbouring nodes to find a safe route. If these malicious nodes work together as a group then the damage will be very serious. This type of attack is called cooperative black hole attack. Our solution discovers the secure route between source and destination by identifying and isolating black hole nodes. In this paper, via simulation, the proposed solution are evaluated and compared it with standard DSR protocol in terms of throughput, Packet delivery ratio and latency.

Dadhania et al[10] investigated the performance of AODV and DSR in presence of black hole attack (malicious node) and without black hole attack with CBR (Constant Bit Rate) traffic under different scalable network mobility. Simulation was conducted to evaluate the effect and compare it with standard protocol in terms of throughput, Packet delivery ratio and End to End Delay. Extensive experiments using the network simulator-2 for 50 node ad hoc network was conducted. Results show that the AODV is more vulnerable to Black Hole attack than DSR.

In DPRAODV (Detection, Prevention and Reactive AODV) [11], they have designed a novel method to detect black hole attack: DPRAODV, which isolates that malicious node from the network. The agent stores the Destination sequence number of incoming route reply (RREPs) packets in the routing table and calculates the threshold value to evaluate the dynamic training data in every time interval as in [12]. The solution makes the participating nodes realize that, one of their neighbors is malicious; the node thereafter is not allowed to participate in packet forwarding operation. In normal AODV, the node that receives the RREP packet first checks the value of sequence number in its routing table. The RREP packet is accepted if it has RREP_seq_no higher than the one in routing table. DPRAODV does an addition check to find whether the RREP_seq_no is higher than the threshold value. The threshold value is dynamically updated as in every time interval. As the value of RREP_seq_no is found to be higher than the threshold value, the node is suspected to be malicious and it adds the node to the black list. As the node detected an anomaly, it sends a new control packet, ALARM to its neighbors. The ALARM packet has the black list node as a parameter so that, the neighboring nodes know that RREP packet from the node is to be discarded. Further, if any node receives the RREP packet, it looks over the list, if the reply is from the blacklisted node; no processing is done for the same. It simply ignores the node and does not receive reply from that node again. So, in this way, the malicious node is isolated from the network by the ALARM packet.

Mittal et al[13] developed the routing protocol which can deal with single and cooperative black hole attack and also without degrading the performance of such networks. The approach provides a feasible solution for the Black hole node detection within the network by making use of "reputation tables" and assigning reputation values to the participating nodes. It improved the routing security of the existing association based DSR protocol using the concept of reputation of nodes value, by identifying and isolating black hole nodes working in a group.

3. Methodology

3.1. Dynamic Source Routing (DSR)

The Dynamic Source Routing (DSR) protocol is a on-demand routing protocol. DSR protocol maintains the route cache to store the route to the mobile node it is aware [14, 15]. This protocol composed of two major phases: route discovery and route maintenance. Whenever any node has the data to send, first it checks the route cache for the route to the destination. If it has the unexpired route, then it use it otherwise initiate a route discovery process by broadcasting the RREQ (Route Request) packet which contains the source address and destination address. Whenever any intermediate node receives the RREQ, and it does not have the route to the destination it adds its own address in the route record and forward to its neighbor. RREP (Route Reply) is generated whenever RREQ reaches to destination node or intermediate node which has the route to destination in its route cache. Route maintenance mechanism is used to detect whether the path to the destination exist or not. Route maintenance uses the route error message and acknowledgement. Route error (RERR) message is initiated whenever the destination's data link layer recognize any transmission error.

DSR is suited for small to medium sized networks as its packet overhead can scale all the way down to zero when all nodes are relatively stationary [16]. The packet data overhead will increase significantly for networks with larger hop diameters as more routing information will need to be contained in the packet headers. The DSR protocol is composed of two main mechanisms that work together to allow the discovery and maintenance of source routes in the ad hoc network:

- **Route Discovery** is the mechanism by which a node S wishing to send a packet to a destination node D obtains a source route to D. Route Discovery is used only when S attempts to send a packet to D and does not already know a route to D.

- **Route Maintenance** is the mechanism by which node S is able to detect, while using a source route to D, if the network topology has changed such that it can no longer use its route to D because a link along the route no longer works. When Route Maintenance indicates a source route is broken, scan attempt to use any other route it happens to know to D, or it can invoke Route Discovery again to find a new route for subsequent packets to D. Route Maintenance for this route is used only when S is actually sending packets to D.

3.2. Proposed modification in the DSR

The proposed routing is based on DSR with modification for detection of black hole attack. It is divided into two phases: Detection before route establishment and avoidance of malicious nodes during data forwarding. The salient feature of proposed scheme is its simplicity and effectiveness in detecting malicious nodes in dynamic scenarios.

This algorithm has been designed based on the concept that malicious node may drop the packet or modify the packet. The DSR is modified to contain new header called Trap Header (TH). During detection phase, the nodes first sources the entire two hop neighbor node id's and sends trap packet with TH consisting of invalid data destination to its two hop neighbors. If the receiving node states that it has the route to the invalid destination in its cache, and has forwarded the data packet to next hop then the node is assumed to be a black hole malicious node. This information about the maliciousness is stored in the nodes. During route discovery, the nodes cross check the routes in its cache and if the route consists of a malicious node, the node invalidates that route and starts a fresh route discovery avoiding the malicious node. Thus, the proposed mechanism mitigates the black hole attack by a simple mechanism of trapping the malicious nodes and avoiding it in any of the routes during transmitting data packets.

4. Results and Discussion

The proposed DSR is simulated to evaluate its performance and compared with traditional DSR. The experiments are conducted for varying speed of the mobile nodes. The speed is varied from 10 Kmph to 90 Kmph and studied for the network performance. The black hole attack misbehaviour is defined as either drop the packets or not to forward the packet in the specified time interval. DSR routing protocol parameters were set as shown in Table 1.

Table 1: DSR Routing Parameters Used

Parameters	Values
Route expiry time	300 second
Request table size	64
Maximum transmission attempt	16
Timeout value for non-propagating requests	0.03 second
Gratuitous route reply timer	1 second
Maintenance hold off time during route maintenance	0.25 second
Maintenance acknowledgement time	0.5 second

Several performance metrics are used to compare the proposed DSR protocol with the existing one. The following metrics were considered for the comparison were

Packet Delivery Ratio(PDR): It is the ratio of the number of packets received and the number of packets sent.

Average End to End delay: It gives the mean time (in seconds) taken by the packets to reach their respective destinations.

Table 2(a, b and c) tabulates the Number of hops to destination, end to end delay and packet delivery ratio obtained for the proposed DSR and DSR. Figure 2 to Figure 4 shows the same.

Table 2: Results of the experiments

Table 2(a): Values of No. of hops to destination

Mobility	No of hops to destination	
	DSR	Proposed DSR
10 Kmph	2.7	2.9
30 Kmph	3.2	3.6
50 Kmph	3.5	3.8
70 Kmph	3.9	4.1
90 Kmph	4.2	4.4

Table 2(b): Values of the end to end delay

Mobility	End to End Delay	
	DSR	Proposed DSR
10 Kmph	0.0514	0.0464
30 Kmph	0.0608	0.0582
50 Kmph	0.0684	0.0618
70 Kmph	0.0726	0.0638
90 Kmph	0.0784	0.0692

Table 2(c): Values of Packet Delivery Ratio

Mobility	Packet Delivery Ratio (PDR)	
	DSR	Proposed DSR
10 Kmph	0.9278	0.9432
30 Kmph	0.9148	0.9326
50 Kmph	0.8842	0.9014
70 Kmph	0.8621	0.8942
90 Kmph	0.8544	0.8824

It is observed that the number of hops for the proposed DSR is slightly more than the DSR as shown in figure 2. This is due to avoiding the malicious nodes in the network, while transmitting data packets to the destination. As the increase is negligible, when compared to DSR, the increase can be ignored.

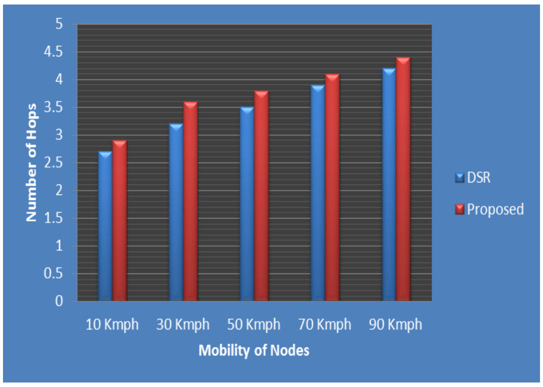

Figure 2.Number of Hops to Destination

The end to end delay in the proposed DSR is considerably less and it is observed that with the increase in number of nodes, the delay in DSR increases by 13.3%. Though, the number of hops from the source to destination increases, the end to end delay is less in the proposed DSR as shown in figure 3.

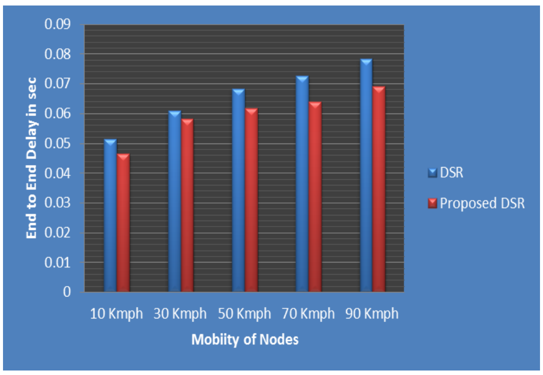

Figure 3. End to End Delay

The PDR improves with the use of modified DSR in the range of 1.57 % to 3.28% as shown in figure 4. It is observed from the tables and figures that the proposed DSR performance better than DSR in the presence of black hole attack.

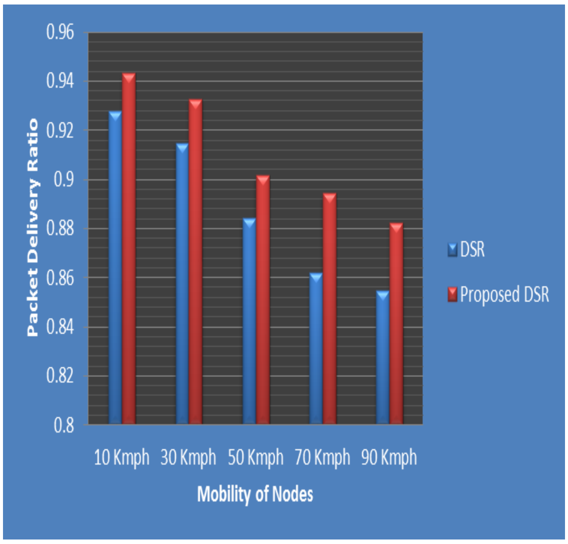

Figure 4. Packet Delivery Ratio

5. Conclusion

MANET networks are systems of mobile ad hoc networks which are presented dynamically and self-organized in temporary topologies. Internal attacks are typically more severe attacks, since malicious insider nodes already belong to the network as an authorized party and are thus protected with the security mechanisms the network and its services offer. The DSR routing is modified to include a Trap Header to identify malicious nodes. Experimental results demonstrate that the proposed DSR performance better than DSR in the presence of black hole attack under dynamic conditions.

References

[1] Zhao, Z., Hu, H., Ahn, G. J., and Wu, R. Risk-aware response for mitigating MANET routing attacks. IEEE Conference In Global Telecommunications (GLOBECOM 2010), December 2010, pp. 1-6.

[2] Mohapatra, P., Li, J., and Gui, C. QOS in Mobile Ad hoc Networks. IEEE Wireless Communications, June 2003, 10(3), pp. 44-52.

[3] Buchegger, S., Boudec, J.-Y.L. Nodes bearing grudges: Towards routing security, fairness, and robustness in Mobile ad hoc networks, In Proceedings of the Tenth Euromicro Workshop on Parallel, Distributed and Network-based Processing, IEEE Computer Society, Canary Islands, Spain, January 2002, pp. 403–410.

[4] Padmavathi, D. G., and Shanmugapriya, M. A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks. International Journal of Computer Science and Information Security(IJCSIS), 2009, 4(1&2), pp.1-9.
[5] Papadimitratos, P. and Haas, Z.J. Securing the Internet Routing Infrastructure, IEEE Communications Magazine, October 2002, 40(10), pp. 60-68.
[6] BrachaHod, Cooperative and Reliable Packet-Forwarding On top of AODV, www.cs.huji.ac.il/~dolev/pubs/reliable-aodv.pdf, 2005.
[7] Sanjay Ramaswamy, Huirong Fu, ManoharSreekantaradhya, John Dixon and Kendall Nygard. Prevention of Cooperative Black Hole Attack in Wireless AdHoc Networks, In Proc. of International Conference on Wireless Networks, 2003.
[8] Hu, Y. C., Perrig, A., and Johnson, D. B. Ariadne: A Secure On-Demand Routing Protocol for Ad hoc Networks. Wireless Networks, 2005, 11(1-2), pp. 21-38.
[9] Bhalaji, N. and Shanmugam, A. Defense Strategy Using Trust Based Model to Mitigate Active Attacks in DSR Based MANET. Journal of Advances In Information Technology, May 2011, 2(2), pp. 92-98.
[10] Dadhania, P., and Patel, S. Performance Evaluation of Routing Protocol like AODV and DSR under Black Hole Attacks. Performance Evaluation, International Journal of Engineering Research and Applications(IJERA), 2013, 3(1), pp. 1487-1491.
[11] Payal N. Raj, Prashant B. Swadas. DPRAODV: A Dyanamic Learning System Against Blackhole Attack In AODV Based MANET. IJCSI International Journal of Computer Science Issues, 2009, Vol. 2, pp. 54-59.
[12] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kat, Abbas Jamalipour, and Yoshiaki Nemoto, “Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method”, International Journal of Network Security, Nov. 2007, 5(3), pp. 338-346,
[13] Mittal, S., and Taluja, H. Analysis of Cooperative Black Hole Attack Using Dynamic Source Protocol. International Journal of Advanced Research in Computer Science and Software Engineering(IJARCSSE), August 2012, 2(8), pp. 139-142.
[14] Hu, Y., and Maltz, D. The Dynamic Source Routing Protocol (DSR) for Mobile Ad hoc Networks for IPv4. RFC 4728, February 2007, pp. 2-100.
[15] Broch, J., Johnson, D. B., and Maltz, D. A. The Dynamic Source Routing protocol for Mobile Ad hoc Networks, 1998.
[16] Bouhorma, M., Bentaouit, H., and Boudhir, A. (2009, April). Performance comparison of ad-hoc routing protocols AODV and DSR. International Conference on Multimedia Computing and Systems’2009(ICMCS'09), 2-4 April 2009, pp. 511-514.

Bio data for Authors

Mr. K. Mahamuni received the B.Sc. (Computer Science) degree from the Bharathidasan University Tiruchirappalli, in 1992. He received his MCA and M.Phil (Computer Science) Degrees from Manonmaniam Sundaranar University, Tirunelveli in 1995 and 2001, respectively. He is working as an Assistant Professor, Department of Computer Applications, Government Arts College (Autonomous), Salem, TamilNadu, Salem, India. He is currently pursuing the Ph.D. degree with the Department of Computer Science, Periyar University, Salem, TamilNadu, India. His research interests include Mobile Computing and Wireless Networking.

Dr. C. Chandrasekar received his Ph.D., degree from Periyar university. He is working as an Associate Professor, Department of Computer Science, Periyar University, Salem, TamilNadu, India. His areas of interest include Wireless networking, Mobile Computing, Image Processing, Data mining, Computer Communications and Networks. He is a research guide at various universities in India. He has published more than 80 technical papers at various National & International conferences and 50 journals. He is a senior member of ISTE and CSI.