An Enhanced Approach of Detection and Prevention of Black Hole Attack on AODV over MANET

Jayshree Gojiya
Student of M.tech (IT)
Department of Information & Technology
Charotar University of Science & Technology (CHARUSAT)

Amit Nayak
Assistant Professor
Department of Information & Technology
Charotar University of Science & Technology (CHARUSAT)

Bimal Patel
Assistant Professor
Department of Information & Technology
Charotar University of Science & Technology (CHARUSAT)

ABSTRACT

Mobile Ad-hoc network is a situate of portable nodes that correspond with wireless links and communication acknowledged out without any central control or fixed communication. The dynamic topology of MANETs allows nodes to join and leave the network at any point of time .this generic characteristic of MANET has rendered it vulnerable to security attacks. The black hole attack is one of such security risks. In this attack, a malicious node fallaciously advertise shortest path to the destination node with an intension to disrupt the communication In this paper, we intend a solution to the black hole attack in one of the most prominent routing algorithm, ad-hoc on demand distance vector (AODV) routing, for the MANETs. The anticipated scheme uses Watchdog mechanism to detect malicious node with usage of local information of intermediate node and propagates the information of black hole node to all other node in network the simulation results show the efficiency of anticipated scheme in presences of black hole node.

Keywords

ad hoc networks, black hole , AODV, security, routing**.**

1. INTRODUCTION

A mobile ad hoc network is a set of wireless mobile nodes that dynamically establishes the network in the absence of fixed communication. One of the individual features of MANET is, each node must be able to find out the optimal path to forward a packet. MANETs provide talented technology for civilian and military applications. One of the important research areas in MANET is starting and maintaining ad hoc network through the use of routing protocols. The increasing development in wireless local area networks has opened new limits in the field of telecommunication. MANET a composed of nodes that can communicate with each other without knowing their position [4]. There is no base station in these networks and nodes communicate in multi-hop pattern. These networks are needed in conditions where short-lived connectivity is required [4].

There are two well known secured-initiated on demand routing protocols include AODV and DSR. These protocols are based on plan of finding valid paths once they are needed by the source node. This procedure, known as route discovery engage the route request phase (RREQ) and route reply phase (RREP). All of these protocols construct a single-path route between a source node and a destination node. Whenever communication link breaks on the active route, each protocol has to raise a route discovery process can cause the performance badly. Single path protocols learn. Routes and select a single best route to reach each destination [1].

2. OVERVIEW OF AD HOC ON-DEMAND DISTANCE VECTOR ROUTING PROTOCOL

AODV stands for ad hoc on-demand distance vector routing protocol. AODV is a reactive protocol. AODV is a single path distance vector routing protocol in ad hoc wireless networks. This protocol mixes the route discovery mechanism in DSR with the approach of destination sequence number in DSDV [4]. Basically when there is one node that wants to communicate with another node that is not in range, it finds a route through the other nodes. It minimizes the number of broadcasts by creating rotes on-demand as oppose to all possible routes as in DSDV. AODV is a loop- free, single path, distance vector protocol based on hop-by-hop routing approach. There are two main procedures in AODV:

1. Route discovery
2. Route maintenance

1. Route Discovery

When source node wants to communicate with destination and if path is not available to destination then source node rebroadcast to its entire neighbor in the network. When intermediate node receives RREQ, they create link to previous node. They first of all check whether valid route to destination or present. If valid route is present then another condition is hold, i.e. intermediate node’s sequence number Should be at least as great as destination sequence number in RREQ packet. If both condition hold then that node generate RREP packet. If valid route is not present then RREQ is further forwarded. RREP contains IP address of source node as well as destination and destination sequence number once the node

Creates the forwarded route entry. If forwarded the RREP to destination node. The RREP is thus forwarded hop-by-hop to the source node. Once receives the RREP. It can utilize the path for the transmission of data packet [3].

2. Route Maintenance

As MANET is dynamic i.e. mobility and topology of nodes always change, link break occurs, when path breaks both nodes informs their end nodes about link failure who were using path by sending RERR. End nodes delete their entry from route table as path is no longer useful. If source nodes still want to communication with destination. If reinitiate RREQ broadcasting or path finding process or repair broken link [3]

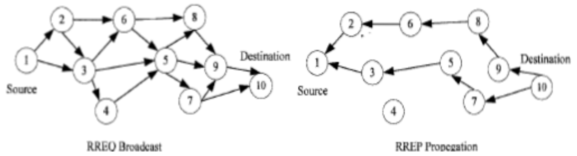


Figure 1. Route Discovery

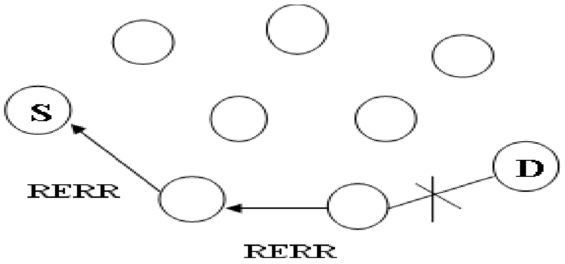


Figure 2. Route Maintenance

3. REVIEW OF LITERATURE

Security issues in MANETs have always been a hot topic and many research articles are available in the literature that deals exclusively the black hole problem. Lu et al. [5] proposed SAODV which may be considered as an extension to the AODV. On receiving a RREP packet, the source node verifies a secure path to the destination node by sending SRREQ packets. The SRREQ contains a secret code (a random number). After receiving at least two such packets, the destination node responds back with SRREP packets. The SRREP also contains a secret code (a random number). When the source node receives at least two such packets, it chooses the shortest among them as a secure path to the destination node for data transmission. However, it contains several disadvantages. The throughput of the network decreases as it increases the delay. In some cases, it may be catastrophic and introduce a depletion of routes in the network. Deng et al. [6] also propose a method which verifies security of the path after receiving a RREP packet. It requires each node to send back the next hop information also when it sends back the RREP packet. After receiving the RREP packet, the source node sends a Further Request packet to the next hop of the intermediate node. Only the next hop can send back a Further Reply packet. The source node decides a secure route on the basis of this Further Request packet and declares the malicious node as black hole. The drawback of this approach is an increased delay in the network.

Alem and Xuan [7] propose a solution Intrusion Detection using Anomaly Detection (IDAD). It uses host- based Intrusion Detection System (IDS) scheme to monitor the activities of a host. An anomaly activity is detected on the basis of audit data which is collected and is given to the IDAD system. It compares every activity of a host with the audit data on the fly and isolates a host (node) if any of its activity resembles an activity in the audit data. However, there are several drawback of this method. It requires extra memory, slows down the system and is impractical to implement in some hostile scenario.

Pushpa [8] presents a modified approach of AODV which is based on trust and gives equal weight to both route trust and node trust for the route selection process. Continuous evaluation of node's performance and collection of neighbor node's opinion value about the node are used to calculate the trust relationship of this node with other nodes. Mediation et al. [9] present a routing protocol to combat black hole attack in MANET. It is a trust based method where the sender takes opinion of the neighbors of the node (say, node *A*) which replied with a RREP packet, i.e., advertises the shortest route to the destination. This opinion along with a rule base determines whether node *A* is malicious. Mahmood and Khan [10] present a survey of methods to combat black hole attack on AODV routing protocol.

4. PROPOSED SCHEME FOR BLACK HOLE DETECTION AND PREVENTION

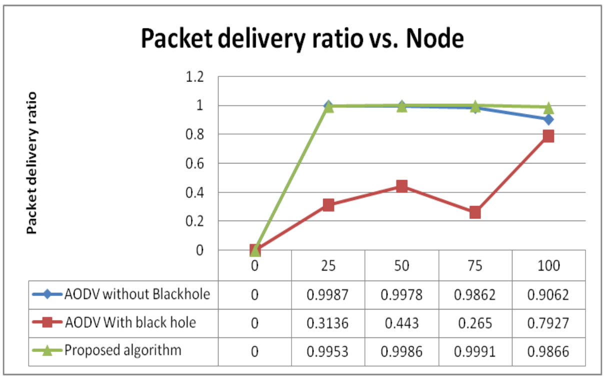
In proposed system we have merged two techniques for detection and prevention of black hole. In which, each and every node observes the other node into the network using watchdog mechanism. First source node broadcast RREQ for finding the best route towards the destination. Intermediate node process the RREQ based on, its originator or it does not know the destination location so that it further broadcast RREQ. At that time source node observes the intermediate node and increment the credit value. Credit value increases based on RREQ broadcast or forward data packet. Credit value decreases based on receive route reply RREP or drop the data packet. Attacker node never broadcast RREQ message so we consider this issue for our proposed work. When credit value reached at the zero intermediate node itself modify RREQ message and add the malicious node ID in modify RREQ. so that each and every node remove the entry of malicious node for prevention technique. Based on this scheme it prevents black hole attacker and increase the parameter like throughput, routing overhead and PDR

5. SIMULATION AND RESULT

we have setup experiment in which we have taken two network simulation scenarios in which first we have checked the behavior of normal AODV protocol under various performance parameters and second we have checked the behavior of AODV protocol under some malicious behavior

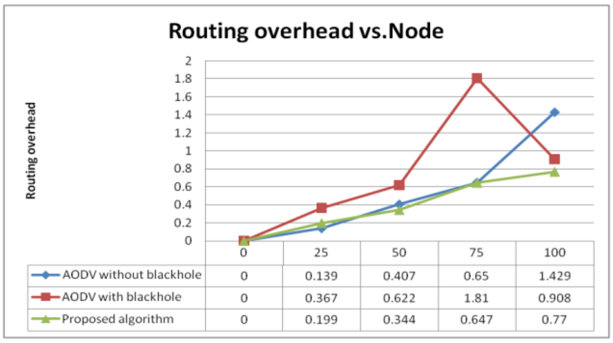
Simulation parameters are given in following Table 1.

Simulator	Ns 2.35
Routing Protocol	AODV
Number of Nodes	100
Packet Size	512
Pause Time	2.0
Maximum Speed	50
Simulation Time	100
Topology	500 × 500
Traffic	CBR
Seed	1.0
Maximum Connection	8
Data Rate	4.0
Mobility Model	Random Way



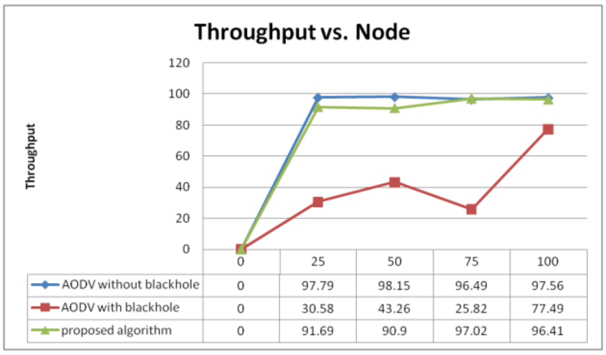
	0	25	50	75	100
AODV without Blackhole	0	0.9987	0.9978	0.9862	0.9062
AODV With black hole	0	0.3136	0.443	0.265	0.7927
Proposed algorithm	0	0.9953	0.9986	0.9991	0.9866

Figure 5.graph of PDR for AODV, black hole and proposed system



	0	25	50	75	100
AODV without blackhole	0	0.139	0.407	0.65	1.429
AODV with blackhole	0	0.367	0.622	1.81	0.908
Proposed algorithm	0	0.199	0.344	0.647	0.77

Figure 4.graph of routing overhead for AODV,black hole and Proposed system



	0	25	50	75	100
AODV without blackhole	0	97.79	98.15	96.49	97.56
AODV with blackhole	0	30.58	43.26	25.82	77.49
proposed algorithm	0	91.69	90.9	97.02	96.41

Figure 5.graph of throughput for AODV, black hole and proposed system.

6. CONCLUSION

MANET is an emerging area as it has great potential in various diverse areas, e.g., military, disaster management, intelligent transportation system, monitoring, public safety. However, it poses a greater security risk in comparison to conventional wireless and wireless networks due to its inherent characteristics, e.g., the open medium, dynamic network topology, autonomous terminal, lack of centralized monitoring, lack of management point Mobile. In this paper, we discuss black hole problem which is severe security risk in routing. We propose a method which is combination of watchdog mechanism and credit based technique in which we can take advantage of both for in which watchdog mechanism uses local information of routing table so it decreases the extra overhead so using these two technique we have tried to improve the results which we can see in graph .The simulation results show effectiveness of proposed method.

7. REFERENCES

[1] Hrishabha Raj Jain, Sanjay Kumar Sharma, “Improved Energy Efficient Secure Multipath AODV Routing for MANET”, IEEE international conference on advances in engineering & technology research (ICRETR-2014) August 01-02, 2014. .

[2] G. Varaprasad, Shivashankar, “Designing Energy Routing Protocol With Power Consumption Optimization in MANET”, IEEE TRANSACTION Vol. 2, no. 2, June-2014

[3] Uma Rathore Bhatt*, Priyanka Jain, Raksha Upadhyay, “Enhance AODV- An Energy Efficient Routing Protocol For MANET”, IEEE-2013.

[4] Alireza Shamsoshoara, Dr. Yousef Darmani, “Enhance Multi-Route Ad Hoc On-Demand Distance Vector Routing” Iranian Conference On Electrical Engineering(ICEE), IEEE-2015.

[5] Songbai Lu, Longxuan Li , Kwon-Yan Lam and Lingvan Jia “ SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack,” Proceedings of International Conference on Computational Intelligence and Security, 2009, pp. 421-425

[6] Hongmei Deng, Wei Li and Dharma P. Agrawal, “Routing Security in Wireless Ad Hoc Networks,” IEEE Communication Magazine, Vol. 40, 2002, pp. 70-75

[7] Yibeltal Fantahun Alem and Zhao Cheng Xuan, “Preventing Black Hole Attack in Mobile Ad-Hoc Networks Using Anomaly Detection,” International Conference on Future Computer and Communication, 2010, pp. 672-676.

[8] A. Menaka Pushpa, “Trust Based Secure Routing in AODV Routing Protocol”, IEEE, 2009

[9] M. Medadian, M. H. Yektaie, A. M. Rahmani, “Combat with Black Hole Attack in AODV Routing Protocol in MANET”, AH-ICI 2009, First Asian Himalayas International Conference on Internet, November 2009, pp. 1-5.

[10] R.A. Raja Mahmood and A.I. Khan, “A Survey on Detecting Black Hole Attack in AODV-based Mobile Ad Hoc Networks”, Proceedings of International Symposium on High Capacity Optical Networks and Enabling Technologies, 2007, pp. 1-6.