Advances in Wireless and Mobile Communications.
ISSN 0973-6972 Volume 10, Number 5 (2017), pp. 859-869

http://www.ripublication.com

Development of Modified Reactive Protocol to diminish Blackhole Attack using Diffe-hellman and BT-AODV in MANETs

Dinesh[1], Ajay Kumar[2] and Rajiv Mahajan[3]

[1]Research Scholar, Department of Computer Applications, I.K.G. PTU, Jalandhar, India

[2]Associate Professor, Department of ECE, Beant College of Engg. & Tech., Gurdaspur, India.

[3]Professor, Department of CSE, Golden College of Engg. & Tech., Gurdaspur, India.

Abstract

Mobile ad-hoc wireless networks (MANETs) are self configured, self organized, short lived, dynamic networks which can be deployed anywhere, anytime within limited area without any infrastructure setup. MANETs are becoming popular due to prolific use of easily available, cheaper mobile devices and advancement in wireless technologies. The peculiar and distinctive characteristics of MANET like unpredictable node movement, no centralized control, and stringent constraints of resources make security a challenging issue in MANET. In this paper, we have focused on AODV, most promising routing technique of MANET which is vulnerable to black hole problem. Black hole is an unsolved hazard to functionality of routing behavior and network mechanism of MANET caused due to faulty and misbehaving node. Our paper proposes an effective solution to diminish bad effect of black hole and find trusted secure route using Diffe-Hellman and Backtrace-AODV method. Extensive simulation results show that our proposed method performs very well in thwarting black holes from MANET. Our proposed solution performs well than normal AODV with less packet loss and more mean hop.

Keywords: Ad-Hoc on Demand Distance Vector Routing Protocol (AODV), Black hole attack, Routing protocol

I. INTRODUCTION

Mobile ad hoc network is a wireless network of mobile nodes with no infrastructure like access point which reduces deployment time and set up cost of network. Nodes in MANET[1,2] are free to move anywhere in any direction due to changing network topology. The every node in ad hoc network forwards packets for other nodes to discover routes acting as a router. Any two nodes in network communicate directly with each other if both nodes are in transmission range otherwise they need the help of other nodes to forward packets to communicate. The main objective of a routing protocol is to find and maintain routes due to link breakages and forged routes. There are three categories of routing protocols used in MANET such as table driven routing protocols, reactive (or on-demand) protocols and hybrid protocols depending upon routing table updation mechanism. The three most widely used routing protocols in Manet are Dynamic Source Routing Protocol (DSR) [17], Destination Sequenced Distance Vector Routing Protocol (DSDV)[16], Adhoc On demand Distance Vector Routing Protocol (AODV) [15]. These routing protocols are highly vulnerable to security threats [3],[4],[5],[6],[7],[8] which can disturb routing mechanism. Mobile ad hoc networks have various security threats such as modification attack, replay attack, black hole attack, spoofing attack, wormhole attack. In this paper, we address the issue of black hole attack on AODV routing protocol and propose a technique to avoid black hole and find secure route between sending node and destination node.

The paper is organized as follows: section I will talk about introduction of MANETs and their security issues, section II discusses the Black Hole attack, section III covers the related work, section IV discusses about proposed work, section V discusses results and discussions and final conclusion is described in section VI.

II. BLACK HOLE ATTACK

A Black hole attack struggle the route by producing the routing message and afterward either listens or drop the packets, representing a conceivable risk to security properties. A Black hole attack changes sequence number and hop count of values of

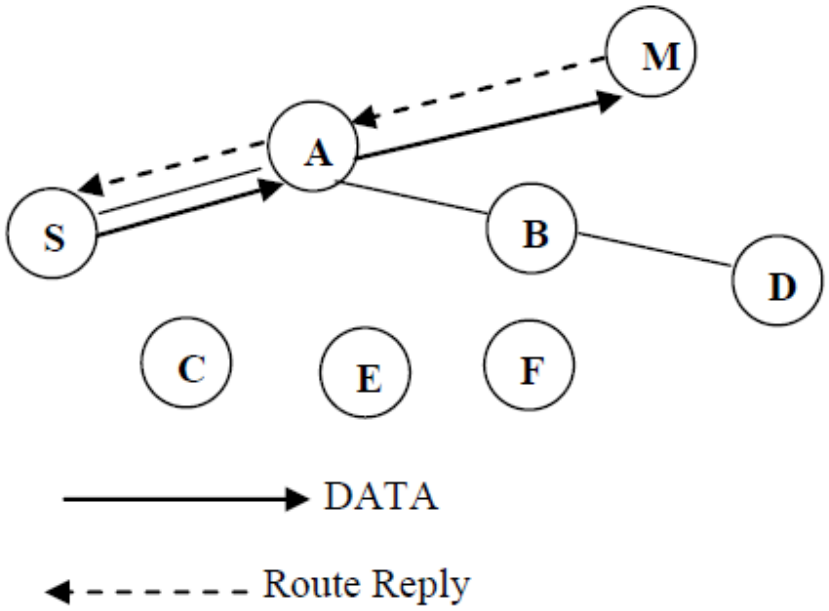

Fig. 1: Black hole Attack

a routing message to get route wrongly and afterward drops all packets of data which should reach receiver D. Black hole problem is shown in Fig.1. Here, Originating node S should send data with route S-A-B-D. But, due to blackhole M, S will send all data packets to M through A. An attacker node mimics a destination node by sending a wrong reply of route (RREP) to source that initiates a discovery for generating route between source and destination. The Black Hole node has two properties [9]: (1) Attacker exploits routing mechanism of AODV protocol and promotes itself as having shortest and best path to a receiving node and (2) Attacker deprives all traffic from source S to receiver D. The malicious node dependably sends reply of route (RREP) to source S when it gets route of request (RREQ) without performing normal routing behaviour of AODV. While keeping very high Destination Sequence Number (DSN), AODV considers reply of route (RREP) as fresh. Therefore, route of reply (RREP) sent by backhole node is treated as fresh. In this way, malicious nodes become successful in infusing Black hole attacks [9].

III. RELATED WORK

Tamilselvan et.al [10] proposed a technique for identification of black hole node. In their solution, they have modified AODV routing protocol. Source node does not send data packets when it receives the route reply (RREP) message, rather it waits for other route reply messages coming from adjoining nodes to find the safe route to send data

packets. Source node selects the most trusted node by investigating the various route reply messages. This technique has the limitation of delay.

M.A Shurman et.al [11] proposed a method to avoid black hole nodes. In this method, source node will wait for route reply (RREP) messages from more than two adjoining nodes and checks the authenticity of adjoining nodes sending route reply (RREP) messages. Source node searches for shared nodes from different route reply (RREP) messages and supposes route is safe if it finds shared node in route reply (RREP) messages from neighbouring nodes. Delay is weakness of in their method.

H. Weerasinghe et al. [12] proposed a method that consists of data routing information (DRI) table which contains 0 and 1 value for 'false' and 'true' values respectively. In their method, with DRI table and cross checking techniques, they can find that reply is from malevolent node or not by checking route reply message.

H. Deng et al. [13] proposed a solution where intermediate node give information about next hop node with route reply message. When source receives reply of route (RREP) message with information of next hop node, it sends a request to next hop node to find if there is any path between intermediate node and destination node. Then, based on reply from next hop node, source checks safety of particular route. Their method cannot identify cooperative black hole attack.

M.Khalili et.al [14] proposed a solution based on hash chain technique. Their solution checks the change in sequence number and hop count in the selected path. In this technique, an extra field is added with route request message (RREQ) and route reply (RREP) message when intermediate node receives route request (RREQ) and route reply (RREP). Two fields hash-RREQ and hash-RREP are added with route request, route reply messages and a random number is chosen to find hash function.

H. Xia et. al. [18] has proposed TeAOMDV protocol to diminish bad effect of grey-hole and black-hole in AOMDV protocol in MANETs.

A. Baadache et. al. [19] has proposed an approach based on authenticated end to end acknowledgement to detect black hole mobile nodes in ad-hoc wireless network.

D. Singh et. al. [20] has proposed ESTA routing protocol to enhance security of AODV protocol to diminish blackhole effect in routing behavior of wireless MANET.

IV. PROPOSED SCHEME

A novel technique is proposed to avoid the occurrence of blackhole problem in MANETs. Although many techniques proposed by different authors are available to prevent the blackhole problem, some of these methods are reviewed in research literature.

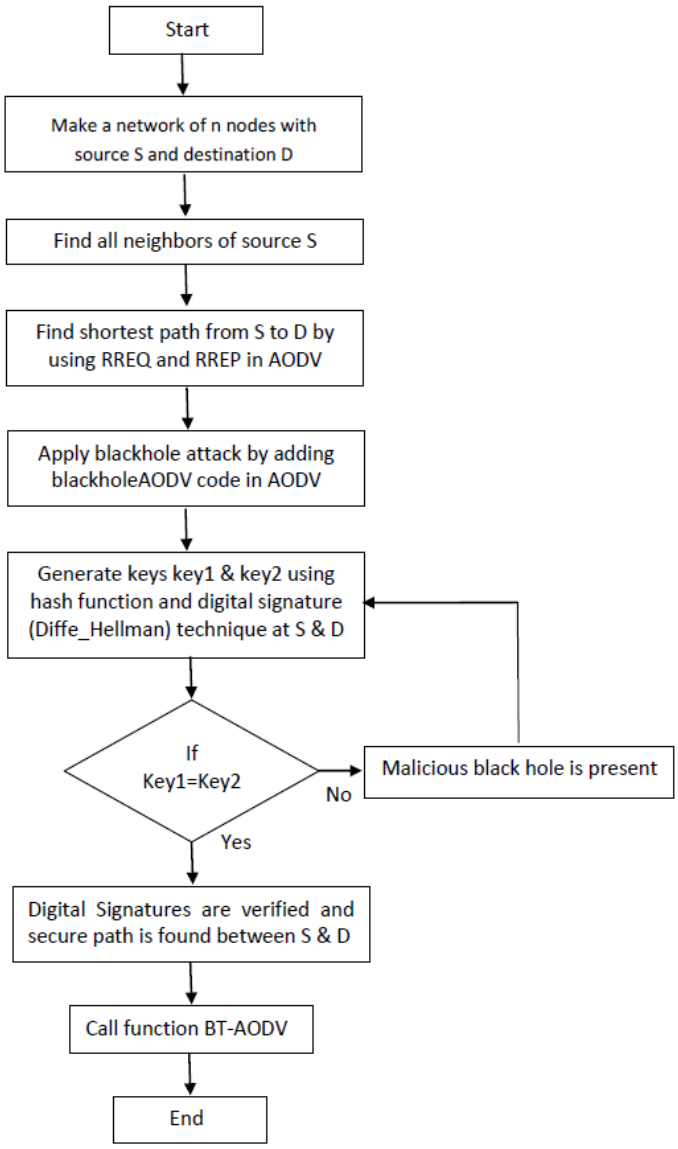

Fig. 2 : Detection Method

In our proposed work, we have modified AODV routing technique which is used as reactive routing in MANET. For detecting black hole in MANET, we have used digital signatures along with hash function. Digital signatures are applied in our solution by Diffe-Hellman method. In AODV, originating node S sends RREQ (route request) control packets to all neighbours which further sends RREQ (route request) to its neighbours in search of destination node D. Header of destination node D stores two columns contains ids of selected path and 2nd column contains digital signatures. Destination D compares digital signature of last node. If digital signatures are same, then node is true node otherwise node is malicious one. Here, we have generated

session keys using Diffe-Hellman and hash function. At destination D a session key is produced with node-id and node claiming to be destination D. If there is no black hole, then both keys match. The proposed detection method is shown in Fig. 2 and we have used backtrace-AODV protocol to avoid black holes in our solution. AODV protocol is having a problem of missed RREP (route reply message). Our reactive protocols are mostly dependent on a single RREP message In our method, we have used backtrace-AODV algorithm to remove this flaw of reactive protocols like AODV. In this method, destination D does not send single RREP, but sends backtrace route request to source S for best route to source S. In high node movement environment of MANET, our algorithm works effectively in case of damaged RREP message. BT-AODV mechanism will definitely enhance routing mechanism of AODV. Proposed BT-AODV mechanism algorithm is shown in Fig. 3.

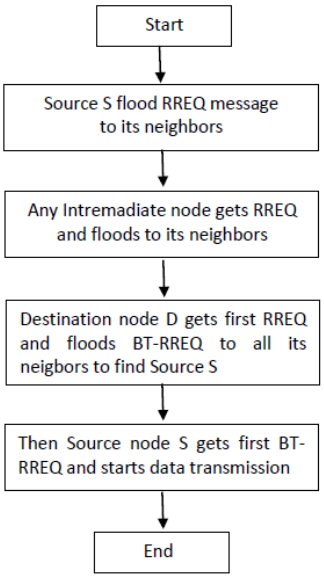

Fig. 3: Backtrace-AODV

V. RESULTS AND DISCUSSIONS

In this section, proposed method has been implemented and results are presented. We have used two metrics for evaluation of proposed method.

Packet loss: Packet loss is defined by formula

$$\text{Packet loss} = \frac{\text{No. of packets sent by source} - \text{No. of packets received by destination}}{\text{Stop time} - \text{Start time}}$$

Mean Hop: Mean Hop is given by formula

$$\text{Mean Hop} = \frac{\text{Total no. of packets forwarded}}{\text{Total no. of packet sent by source}}$$

For carrying out simulation experiments, we have used network simulator 2 and different values of simulator parameters as shown in Table 1

Table 1: Simulation Parametres

Simulator	NS2 (Ver. 2.34)
Number of Black Hole nodes	10
Number of Mobile Nodes	30 to 100
Simulation Time	100 seconds
Topology	800m * 800m
Traffic	CBR(Constant Bit Rate)
Packet Size	512 bytes
Radio Propagation Range	250m
MAC Protocol	IEEE 802.11
Mobility Model	Random Way Point
Routing Protocol	AODV
Antenna Type	Omni directional
Channel Type	Wireless Channel

Table 2: Number of Mobile Nodes and Mean Hop

Number of Nodes	MH without Blackhole	MH with Blackhole	MH with Proposed System
30	0.5959	0.1948	0.2642
40	0.7971	0.00001	0.3987
50	0.8683	0.0003	0.6313
60	0.78	0.0004	0.4249
70	0.8517	0.511	0.7177
80	0.8343	0.0009	0.566
90	0.919	0.0006	0.5637
100	0.8352	0.2934	0.5719

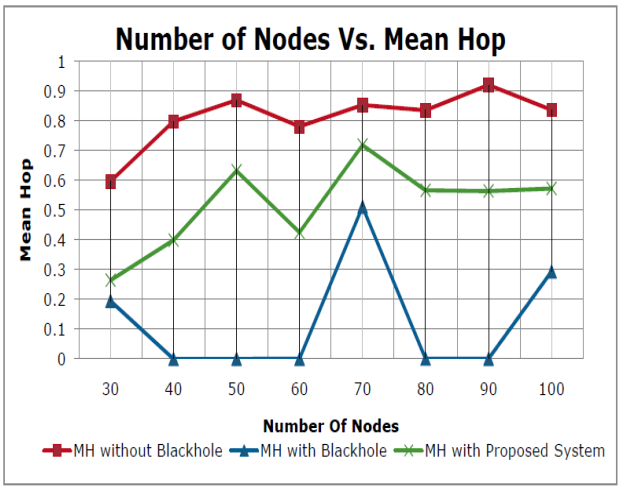

Fig. 4: Mean Hop Vs No. of Mobile Nodes

Table 3: Number of Mobile Nodes and Packet Loss

Number of Nodes	PL without Blackhole	PL with Blackhole	PL with Proposed System
30	232.8	264.01	256.61
40	209.42	264.01	245.73
50	229.86	264.01	239.96
60	200.36	264.01	252.84
70	207.59	264.01	247.48
80	206.98	264.01	238.01
90	218.75	264.01	246.92
100	223.52	264.01	240.1

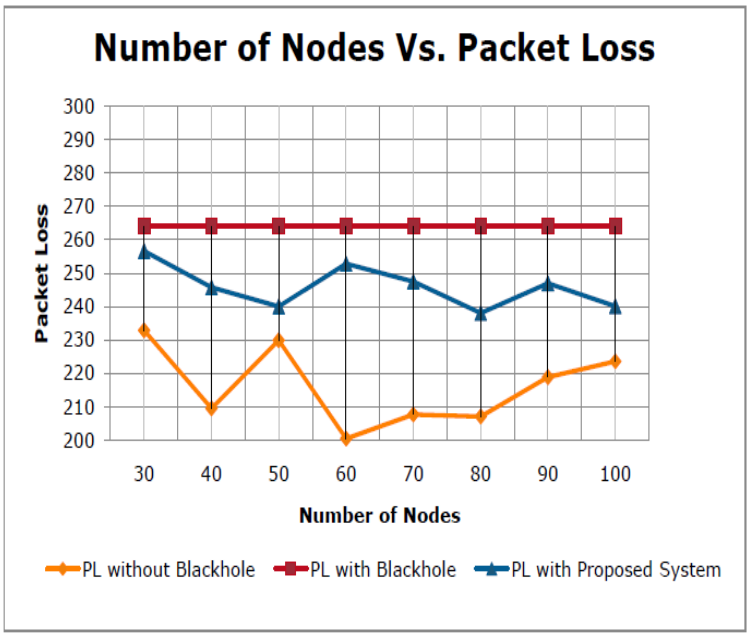

Fig. 5: Number of Mobile Nodes Vs Packet Loss

We have found from Fig. 4 and Table 2 that Mean hop is dropped by 84.56% under black hole attack from malicious node and Mean hop has improved by 48.41% by applying our proposed solution. Also, we have evaluated from Fig. 5 and Table 3 that packet loss of AODV protocol is increased by 22.13% under black hole problem. But, when we have applied our proposed solution, packet loss is dropped by 8.35 %.

VI. CONCLUSION

Black hole attack is one of the conceivable attacks in MANETs. We proposed a novel approach to minimize a blackhole attack in terms of packet loss, mean hop. The proposed two techniques provided better results than the existing techniques. The Simulations of proposed techniques using differ_hellman and BT-AODV have been done in network simulator 2 and is found required security from blackhole attack with minimum packet loss and better mean hop. In future work, we can extend our approach for large network.

REFERENCES

[1] Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt, Piet Demeester, “An Overview of Mobile Ad Hoc Networks: Appliactions and Challenges”, Department of Information Technology ,Ghent University, Belgium.

[2] Mohit Kumar, Rashmi Mishra, "An Overview of MANET: History, Challenges and Application",Indian Journal of Computer Science and Engineering (IJCSE), 2012,Vol.3.

[3] Wenjia Li, Anupam Joshi, "Security Issues in Mobile Ad Hoc Networks- A Surevy", Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore County.

[4] Aarti, Dr. S.S. Tyagi, "Study of MANET: Characteristics, Challenges, Application and Security Attacks", International Journal of Advanced Research in Computer Science and Software Engineering, Vol.3, Issue5, May 2013.

[5] Pravin Ghosekar, GirishKatkar, Dr.Pradip Ghorpade, "Mobile Ad Hoc Networking: Imperatives and Challenges", IJCA Special Issue on "Mobile Ad-hoc Networks" MANETs, 2010.

[6] Jiahong Weng, "Security Issues in Mobile Ad Hoc Networks-A Survey"

[7] Nishu Garg, R.P. Mahapatra, "MANET Security Issues", IJCSNS International Journal of Computer Science and Network Security, Vol.9, No.8, August 2009.

[8] Kuldeep Sharma, Neha Khandelwal, Prabhakar.M , "An Overview of security Problems in MANET",2012.

[9] Ochola EO, Eloff MM, "A Review of Black Hole Attack on AODV Routing in MANET", School of Computing, University of South Africa, Pretoria, South Africa.

[10] L. TamilSelvan, V. Sankaranarayanan, "Prevention of Black hole Attack in MANET", The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications(AusWireless 2007) Aug. 2007,pp. 27-30.

[11] M. A. Shurman, S. Park and S. M. Yoo, "Black hole attack in Mobile Ad Hoc Networks", In Proceedings of the 42nd annual Southeast conference(ACMSE), April 2004,pp. 96-97

[12] H. Weerasinghe, H. Fu, "Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation", Proceedings of the Future Generation Communication and Networking,Vol. 2, 2007, pp. 362-367

[13] Hongmei Deng, Wei Li, and Dharma P. Agrawal, "Routing Security in Wireless Ad-hoc Network", IEEE Communications Magazine, Issue 40,2002, pp. 70-75.

[14] M. Khalili, H. Taheri, S. Vakilinia, "Preventing black hole attack in AODV

through use of hash chain", in Proc. of 19th Iranian Conference Electrical Engineering (ICEE), Iran, 2011, pp. 1-6.

[15] C. E. Perkins and E. M. Royer, " Ad Hoc On-Demand Distance Vector Routing", Proc. 2nd IEEE Workshop Mobile Computer Systems and Applications New Orleans, LA, Feb. 1999, pp. 90-100.

[16] C. E. Perkins and Pravin Bhagwat, "Highly Dynamic Destination-Sequenced Distance-vector Routing (DSDV) for Mobile Computers", SIGCOMM, vol. 24 Issue 4 October 1994, pp. 234-244.

[17] D. B. Johnson, D.A. Maltz, and Y.C. Hu, "The Dynamic Source Routing Protocol for Mobile Ad-hoc Network (DSR)", IETF RFC Internet Draft, July 2004.

[18] H. Xia, J. Yu, C.L. Tian, Z.K. Pan, E. Sha 2016 "Light-weight trust-enhanced on-demand multi-path routing in mobile ad hoc networks", Journal of Network and Computer Applications 62, pp. 112–127.

[19] A. Baadache, A. Belmehdi 2014 "Struggling against simple and cooperative black hole attacks in multi-hop wireless ad hoc networks", Computer Networks, pp. 173-184.

[20] D. Singh, A. Singh 2015 "Enhanced Secure Trusted AODV (ESTA) Protocol to Mitigate Black hole Attack in Mobile Ad Hoc Networks", Future Internet, pp. 342-362.