ROUTING MECHANISM USING DSDV PROTOCOL TO PREVENT BLACKHOLE ATTACK IN MANET

B.R.JEYANTHI*

J.NALINI*

ABSTRACT

Mobile ad hoc network (MANET) is a collection of mobile nodes that communicate with each other without any fixed infrastructure or a central network authority. From a security design perspective, MANETs have no clear line of defense; i.e. no built-in security. Thus, the wireless channel is accessible to both legitimate network users and malicious attackers. A black hole attack is a severe attack that can be easily employed against data routing in MANETs. A black hole is a malicious node that can falsely reply for any route requests without having an active route to a specified destination and drops all the receiving data packets. In this paper we investigated the effects of Black Hole attacks on the network performance. We simulated black hole attacks in Network Simulator 2 (ns-2) and to detect the Black hole attacks in the network .In this novel scheme for Detecting Black hole Attacks in MANETs is introduced. The DBA-DSDV protocol detects and avoids the black hole problem before the actual routing mechanism is started to catch the malicious nodes. Simulation results are provided, when black hole nodes are present in the network.

Keywords—*DestinationSequenceDistanceVector(DSDV),Mobile Ad Hoc Network,Black hole Attack.*

* **Member IEEE**

I. INTRODUCTION

Mobile Ad-Hoc Networks are autonomous and decentralized wireless systems. MANETs consist of mobile nodes that are free in moving in and out in the network. Nodes are the systems or devices i.e. mobile phone, laptop, personal digital assistance, MP3 player and personal computer that are participating in the network and are mobile. These nodes can act as host/router or both at the same time. They can form arbitrary topologies depending on their connectivity with each other in the network. These nodes have the ability to configure themselves and because of their self configuration ability, they can be deployed urgently without the need of any infrastructure. Internet Engineering Task Force (IETF) has MANET working group (WG) that is devoted for developing IP routing protocols. Routing protocols is one of the challenging and interesting research areas. Many routing protocols have been developed for MANETS, i.e. AODV, DSDV, DSR etc.

B.R.JEYANTHI is with the PSN College of Engineering & Technology, Tirunelveli, TN 627152 IND phone: 7708829595; e-mail: jeyanthi.ammu@ gmail.com.

J.NALINI, AssistantProfessor/Head, was with Department of Electronic and communication, PSN College of Engineering and Technology, Triunelveli, TN 627152 IND.

Manuscript received December 11 2012, This work was submitted in International Conference on Emerging Trends in Engineering and Technology, ICETET-2013

.

Security in Mobile Ad-Hoc Network is the most important concern for the basic functionality of network. The availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met. MANETs often suffer from security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. These factors have changed the battle field situation for the MANETs against the security threats. The MANETs work without a centralized administration where the nodes communicate with each other on the basis of mutual trust. This characteristic makes MANETs more vulnerable to be exploited by an attacker inside the network. Wireless links also makes the MANETs more susceptible to attacks, which make it easier for the attacker to go inside the network and get access

to the ongoing communication . Mobile nodes present within the range of wireless link can overhear and even participate in the network.

MANETs must have a secure way for transmission and communication and this is a quite challenging and vital issue as there is increasing threats of attack on the Mobile Networks. Security is the cry of the day. In order to provide secure communication and transmission, the engineers must understand different types of attacks and their effects on the MANETs. Wormhole attack, Black hole attack, Sybil attack, flooding attack, routing table overflow attack, Denial of Service (DoS), selfish node misbehaving, impersonation attack are kind of attacks that a MANET can suffer from. A MANET is more open to these kinds of attacks because communication is based on mutual trust between the nodes, there is no central point for network management, no authorization facility, vigorously changing topology and limited resources. In this paper our focus is on black hole attacks.

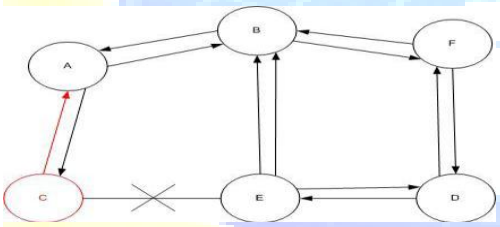

Fig 1 Example of black hole attack

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 .The method how malicious node fits in the data routes varies. Fig. 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 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. This paper focus on detecting black hole nodes (i.e. malicious nodes) in the network.

II. DSDV :PROPOSED MITIGATION SCHEME

The DSDV is designed to identify and isolate the black hole nodes present in the MANET. Destination sequenced distance vector routing is adapted from the conventional Routing Information Protocol (RIP) to ad hoc networks routing. It adds a new attribute, sequence number, to each route table entry of the conventional RIP. Using the newly added sequence number, the mobile nodes can distinguish stale route information from the new and thus prevent the formation of routing loops. In proposed technique a sequence of packets are sent between the wireless nodes in the ad hoc network. Each node will send packets with the specific range of frequency between the nodes where the range of frequencies are given built in. In ad hoc network any foreign nodes can easily become a member of that network and can transmit data with the node. When foreign node tries to communicate with other nodes in the network packets are sent between the nodes, but foreign node can send packet only with the different frequencies which is been not standardized in that network. When frequencies differs for a particular period of time then that node is been declared as a malicious node. When node is declared as a malicious node automatically members in that network will not use that node to send data or packets to destination. Using this technique malicious node can be found easily. Since sequence of packets are transmitted continuously, packet verification can be done. Back up path is found easily when dedicated link is failed to reach the destination. Latency can been reduced to an extend Data loss can be reduced to a greater extend.

III .METHODS

A. NODE CREATION

In thismethod the nodes are deployed randomly in the network and each node send the HELLO message to their neighbors containing the node's id, message, port no and the hop count.

B. NEIGHBOUR ESTABLISHING

In this method the source node discover the route to the destination by broadcasting the RREQ message to their neighbors and the corresponding destination will unicast the RREP to the source node. Along with the primary path it also find one back up route for the same destination with unique path.

C. FINDING SHORTEST PATH

In this method all the nodes are connected the network , to send a hello message to all the system then only about the system connection. To create a table for those network it will gives the network details this is the one method to find the shortest path.

D. OPTIMIZED BLACKHOLE DETECTION

This method is very important to this paper, first to find the shortest path , and to send a hello message to all the systems, then only know, how many system are connected to the network . and then the system distance also known .in this module the backup route is periodically checked by sending the ACK message in the backup route. If the route is not exist then it again the finds the alternate backup route for the same source and destination. ,another way is using this dsdv protocol.

E. *FINDING ALTERNATE PATH*

This method is used to find the alternate path , because the hacked routes are identified that is reason for finding the alternate path. Which is used to transmit the securily.

IV.THE DSDV PROTOCOL

We consider a collection of mobile computers,(nodes) which may be far from any base station. The computers (nodes) exchange control messages to establish multi-hop paths in the same way as the Distributed Bellman-Ford algorithm. These multi-hop paths are used for exchanging messages among the computers (nodes).Packets are transmitted between the nodes using routing tables stored at each node. Each routing table lists all available destinations and the number of hops to each destination. For each destination, a node knows which of its neighbors leads to the shortest path to the destination. We need to maintain the consistency of the routing tables in a dynamically

varying topology. Each node periodically transmits updates. This is done by each node when significant new information is available.

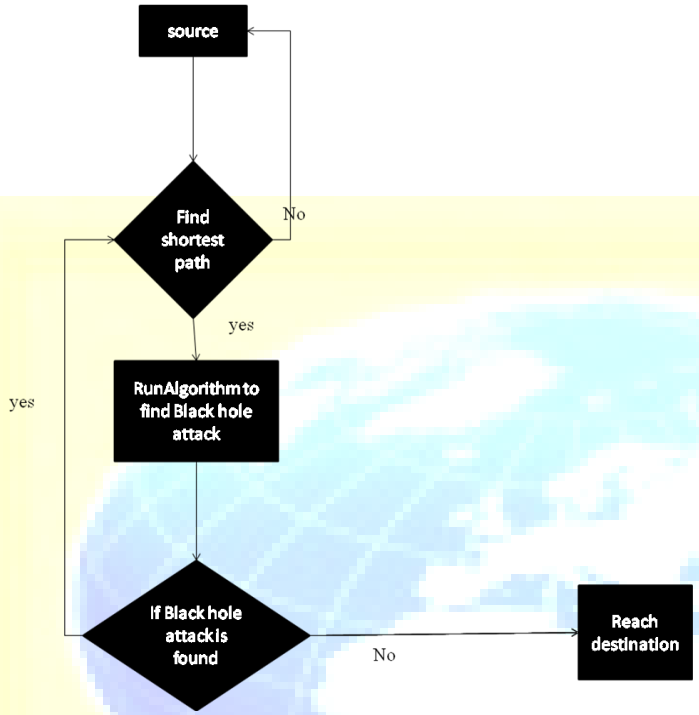

Fig 2 Flow chart diagram for DSDV protocol

V. KEY GENERATION

key is generated to provide security during the transmission. For key generation RSA algorithm is used. RSA involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key. The keys for the RSA algorithm are generated the following way:

Choose two distinct prime numbers p and q.

For security purposes, the integer's p and q should be chosen uniformly at random and should be of similar bit-length. Prime integers can be efficiently found using a primarily test. Compute n = pq. n is used as the modulus for both the public and private keys.

Compute φ(pq) = (p − 1)(q − 1). (φ is Euler's totient function). Choose an integer e such that 1 < e < φ(pq), and e and φ(pq) share no divisors other than 1 (i.e., e and φ(pq) are coprime). e is released as the public key exponent. e having a short bit-length and small Hamming weight results in more efficient Encryption. However, small values of e (such as e = 3) have been shown to be less secure in some settings. Determine d (using modular arithmetic) which satisfies the congruence relation d e \equiv 1\pmod {\varphi(pq)}.Stated differently, ed − 1 can be evenly divided by the totient (p − 1)(q − 1). This is often computed using the extended Euclidean algorithm. d is kept as the private key exponent.

VI .PERFORMANCE EVALUATION

NS2 has been used as the simulation tool.A MANET with 50nodes is designed and the choice of malicious nodes in the network is random.A source node and a destination node are selected and about 500 data packets of 64 bytes each are transmitted from source to destination.The simulation parameters are captured in Table 1.

Table 1: Simulation Parameters

Parameter	Setting
Terrain dimension	1000m*1000m
Number of nodes	50
MAC Protocol	IEEE802.11
Radio range of nodes	250m
Traffic type	CBR
Network layer	DSDV

routing protocol	
Simulation time	10minutes
Data rate(MBPS) mobility model	Random way point
Speed	Random (0-80m/s)
Packet size	64bytes
Pause time	Random(0-80s)

In this paper the performance of QAR and AC are analyzed through the parameters, throughput, Packet Delivery Ratio, drop, and energy consumption in the network based on time

VII. SIMULATION RESULT

We have simulated the proposed model along with the previously used model. The proposed is measured based on the following performance metrics :

• ***Packet delivery ratio*:** This represents the ratio between the number of packets originated by the "application layer" CBR sources and the number of packets received by the CBR sink at the final destination .

• ***Network throughput:***

This represents the average rate of successful message delivery over a communication channel and can be measured as bits per second (bps).

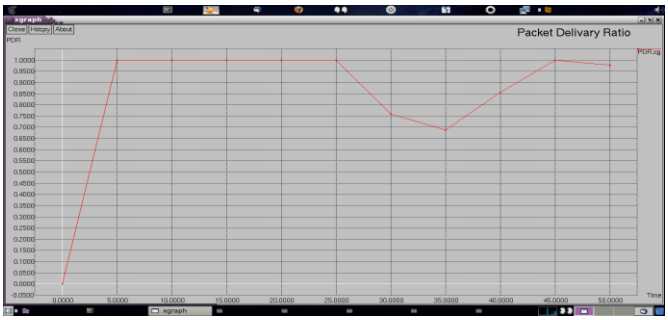

Fig 3: Packet Delivery Ratio

VIII . CONCLUSION

As a result based on Optimized Black hole Detection method we can detect black hole attack and the DSDV protocol is to find the shortest distance between the source and the destination also the simulation results show well its effectiveness in the detection of such attacks and the packet delivery ratio .The DSDV performs better than that of the DSR protocol. The cryptographic techniques are used to provide the security for the packet.

IX. FUTURE ENHANCEMENT

In future, we plan to extend the proposed scheme so that it can handle the case of cooperative black hole attacks in MANETs as well.

X.REFERENCES

[1]Thosar T.P surana k.a, Rathi S.B and Snehal Meharte "A Mechanism To Detect Blackhole Attack On Routing Protocol AODV In MANET", World Research Journal of Telecommunications Systems vol -1,Issue1, 2011.

[2] Marjan Kuchaki Rafsanj, Zahra Zahed Anvari , Shahla Ghasemi " Methods of Preventing and Detecting Black/Gray Hole Attacks on AODV-based MANET" IJCA Special Issue on "Network Security and Cryptography",vol-2,Issue-3,2010.

[3] Yaser khamayseh, Abdulraheem Bader, Wail Mardini, and Muneer BaniYasein "A New Protocol for Detecting Black HoleNodes inAdHocNetworks"International Journal of Communication Networks and Information Security Vol. 3, 2009.

[4] Semih Dokurer , Y. M. Erten , Can Erkin Acar "Performance analysis of ad-hoc networks underblack hole attacks" International Journal of Communication Networks and Information Security Vol. 2, 2008.

[5] Baadache.A, and Belmehdi.A, "Avoiding blackhole and cooperative blackhole attacks in wireless ad hoc networks," Intl. Journal of Computer Science and Information Security, Vol. 7, No. 1, 2007.

[6]Jain.S,Jain.M, Kandwal.H, "Advanced Algorithm for Detection and Prevention of Cooperative Black and Grayhole Attacks in Mobile Ad Hoc Networks", Intl. Journal of Computer Applications 1(7):37–42, Published by Foundation of Computer Science,2006.

[7] Rahul Rishi, Dheer Dhwaj Barak, Yudhvir Singh, Prabha Rani "Mobility Analysis of Blackhole Node Attacks inMobile Adhoc Networks" International Journal of Technical Research(IJTR)Vol 1,Issue 1,2005.

[8]Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto "Detecting Blackhole Attack on AODV-basedMobile Ad Hoc Networks by Dynamic LearningMethod" International Journal of Network Security, Vol.5, 2004.

[9] Khokhar R.H, Ngadi A.N, Mandala.A, "A review of current routing attacks in mobile ad hoc networks", Intl. Journal of Computer Science and Security, vol. 2, Issue-3, 2003.

[10] Royer E.M,Toh.C, "Review of current routing protocols for ad hoc mobile wireless networks", IEEE Personal Communications,2002