ISSN 2319-2720
Volume 2, No.4, October - December 2013
International Journal of Computing, Communications and Networking
Available Online at http://warse.org/pdfs/2013/ijccn05242013.pdf

Secure Routing in Wireless Mobile Ad-hoc Network

Manuj Mishra[1], Kamlesh Kumar Gupta[2]
[1]Dept. CSE,ITM Group Of Institutions, Gwalior(M.P), manuj.mishra02@gmail.com
[2]Dept of IT,RJIT,Tekanpur,Gwalior, kamlesh_rjitbsf@yahoo.co.in

ABSTRACT

Mobile Ad-hoc network (MANET) has become particularly vulnerable to intrusion, as they operate in open medium, and use cooperative strategies for network communications. The black hole attack is one of such security risks. In this attack, a malicious node falsely advertise shortest path to the destination node with an intension to disrupt the communication. In this paper we proposed a approach to detection of black hole attack in AODV (Ad hoc on demand distance vector routing protocol), for MANET. The proposed method uses a last transmission time of a intermediate node which generate a first route reply. The simulation of a approach will show the efficiency of a proposed approach in terms of throughput and end to end dely.

.

Key words : Secured Routing, AODV, Ad-hoc network, Black Hole Attack, MANET

1. INTRODUCTION

MANET is a kind of wireless ad-hoc network and it is a self configuring network of mobile routers (and connected hosts) connected by wireless links – the union of which forms an random topology. The routers, the participating nodes act as router, are free to move randomly and handle themselves arbitrarily; thus, the network's wireless topology may change rapidly and randomly. Such a network may operate in a standalone fashion, or may be connected to the larger Internet [1].

Many routing protocols for mobile ad hoc networks have been proposed. A Survey of Secure Mobile Ad Hoc Routing Protocols in [2]. Up to now, the Internet Engineering Task Force (IETF) MANET working group produced four experimental Requests for Comments (RFCs) that specify four flat routing protocols: Ad Hoc on Demand Distance Vector (AODV), Optimized Link State Routing (OLSR), topology Dissemination Based on Reverse-Path Forwarding (TBRPF), and Dynamic Source Routing (DSR). Another routing protocol, Dynamic MANET On-Demand (DYMO), is currently in draft state.

However, none of these protocols specifies any security measures, effectively assuming that there are
no malicious nodes participating in routing operations. It is worth noting that in an open network
that is based on collaboration between nodes, like a MANET, to have a reliable infrastructure, security issues cannot overlooked[3].

Since the nodes are mobile, the network topology may change rapidly and unpredictably and connectivity among the terminal may vary with the time. The mobile nodes in the network dynamically establish routing among themselves as they move about, forming own network on the fly. The link capacity fluctuates in the mobile ad-hoc network. The nature of high bit error rates of wireless connection might be more profound in a MANET. Since there is no background network for the central control of the network operation, the control and management of the network is distributed among the terminals. The nodes involved in a MANET should collaborate amongst themselves.

Many routing protocols [7] for mobile ad hoc networks have been proposed. Routing in mobile ad-hoc network faced other problem and challenges compared to routing additional wired network. There are several well-known protocols in the literature that have been particularly developed to handle with the limitations imposed by ad hoc networking environments. The problem of routing in such environments is motivated by limiting factors such as rapidly changing topologies, high power consumption, low bandwidth, and high error rates [10].

Most of the existing routing protocols follow two different design approaches to deal with the inherent characteristics of ad hoc networks: the table-driven and the source-initiated on-demand approaches [3].

Based on this threat analysis and the recognized capabilities of the potential attackers, discuss a number of specific attacks that can object the function of a routing protocol in an ad hoc network.

Black Hole: A black hole [4] is a type of denial of service attack where the intension of the malicious node could be to hinder the path finding process or to intercept all data packets being sent to the destination node.

Location Disclosure: Location disclosure [8] is an attack that targets the confidentiality requirements of an ad hoc network.

Through the utilize of traffic analysis techniques, or with simpler probing and monitoring approaches, an attacker is

able to find out the location of a node, or even the structure of the whole network.

Replay: An attacker in replay attack [1] an attacker injects into the network routing traffic that has been captured previously.

Energy consummation: An attacker can attempt to consume batteries by requesting routes or forwarding unnecessary packets to a node [1].

Blackmail: This attack is relevant against routing protocols that use mechanisms for the recognition of malicious nodes and transmit messages that attempt to blacklist the delinquent. An attacker may fabricate such reporting messages and try to isolate legal nodes from the network [11].

2. AODV Routing protocol and Black Hole attack

The AODV protocol makes use of route request (RREQ) messages flooded in the network in order to discover the paths required by a source node. An intermediate node that receives a RREQ reply to it using a route reply message only if it has a route to the destination whose subsequent destination sequence number is greater or equal to the sequence number contain in the RREQ [4]. This effectively means that an intermediate node reply to a RREQ only if it has a fresh route to the destination. Or else, an intermediate node broadcasts the RREQ packet toward its neighbors until it reaches the destination. The destination uncast a RREP back to the node that initiated the route discover by transmitting it to the neighbor from which it received the RREQ. As the RREP is propagate back to the source, all intermediate nodes put up forward route entry in their tables. The route maintenance process utilizes link-layer notifications, which are intercepted by nodes adjacent the one that caused the error. These nodes generate and forward route error (RERR) messages to their neighbors that have been using routes that include the broken link. Following the reception of a RERR message a node initiates a route discovery to re-establish the failed paths.

AODV is a collaborative protocol [5] and allow nodes to allocate the information they hold about other nodes. RREQ messages need not necessarily reach the destination node during the route discovery process. If an intermediate node already knows a route toward the destination, it does not forward the RREQ any further and generates a RREP message. This enables earlier replies and limits the flooding of RREQs when flooding is not required.

Route discovery is susceptible in AODV, which an adversary can develop to perform a black hole attack on mobile ad-hoc network. In this attack, a malicious node falsely advertise excellent path (e.g., shortest path or more stable path) to the destination node during the path finding process. The intension of the malicious node could be to hamper the path-finding process or to interrupt all data packet being sent to the destination node concerned.

Use either SI (MKS) or CGS as primary units. (SI units are strongly encouraged.) English units may be used as secondary

3. Black Hole Attack in AODV Routing

A black hole [1][4], is a type of denial of service attack where the intension of the malicious node could be to obstruct the path finding process or to intercept all data packets being sent to the destination node. In this attack the malicious node pay attention to a route request packet in the network, and respond with claim of having a particularly short route to the destination node, even if it have not any such route. As a result, the malicious node easily false route network traffic to it and then drops the packets transitory to it.

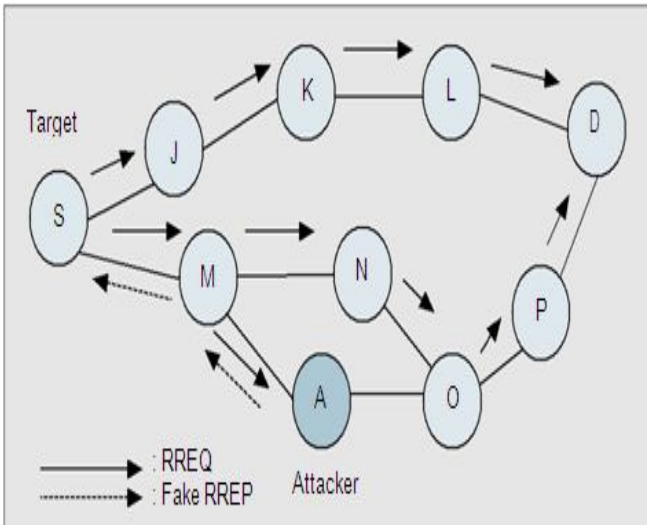

Figure 1 Black hole attack in AODV

Figure 1 shows an example of a black hole attack, where attacker A sends a fake RREP to the source node S, claim that it has a suitably fresher route than other nodes. Since the attacker's advertised sequence number is higher than other nodes' sequence numbers, the source node S will choose the route that passes through node A.

4. LITERATURE SURVEY

Various techniques have proposed in MANET to detect and prevent black hole attack. In paper [6], proposed technique intrusion detection using anomaly detection (IDAD) use host base scheme. Network based intrusion detection schema cannot be engaged to MANET where there is no central device that monitor traffic flow, network based intrusion detection system lying on data centric point of a network such as router and switches but host based intrusion detection system are installed on hosts so that they can oversee the activities of a host and users on the hosts.

IDAD assumes every activity of a user or a system can be recognized from normal activities. IDAD needs to be

provided with a pre collected set of anomaly activities, called audit data. IDAD system capable to compare every activity of a host with the audit data, if any activity of a host match the activity listed in the audit data, the IDAD system separate the particular node from the network. The drawback of this technique is that, here needs the extra memory to make IDAD system. In paper [8], introduce the use of DRI (Routing Information) to keep track of past routing information among mobile nodes in the network and cross checking of RREP message from intermediate node by source node. The main disadvantage of this technique is that mobile node has to maintain an extra database of precedent routing knowledge in addition to routine work of maintaining their routing table. In paper [9], discussed the survey of methods of detecting the black hole attack. CONFIDANT protocol works as an expansion to reactive source routing protocols like DSR [12]. The fundamental idea of the protocol is that nodes that does not forward packets as they are supposed to, will be recognized and expelled by the other nodes. Thereby, a disadvantage is, if a node is found to be intolerable then all the routes which consists of this node will be deleted.

5. THE PROPOSED SCHEME FOR BLACK HOLE DETECTION

In this paper we proposed a approach to detection of black hole attack in AODV (Ad hoc on demand distance vector routing protocol), for MANET. The proposed method uses a last transmission time of a intermediate node which generate a first route reply. The simulation of a approach will show the efficiency of a proposed approach in terms of throughput and end to end dely.
In proposed algorithm, initially a sender broadcasts RREQ packet to its entire intermediate node. If route reply is directly from the destination node or destination node is in direct transmission range of sender node then route is assume to be safe and send the packets from source to destination node.

If route reply from any intermediate node then as the node which generate the first route reply , here check the last transmission time (Ltt) of the node (time gap between RREQ arrived and generate RREP) with transmission time(Tt) (minimum time needed for route reply). If the intermediate node which generate the first route reply is black hole node then it will not check its own routing table after getting a route reply packet then its last transmission time will be less then transmission time and if the intermediate node is the trusty node then it will check in own routing table then its last transmission time will be equal or greater then transmission time. So b using the last transmission time we can detect a black hole node in the network.

Algorithm to detect black hole attack

EVENT Node "S" have Data for node "D"

Notations:
Step1: Source sends RREQ to all intermediate neighbors.

Step2: Source receives the RREP packet.

Step3: if (RREP packet comes directly from Destination) or (Destination node is in direct transmission range of Sender node).
{
Send all data to this node; // Route is assume to be safe
}
Step4: Else if route reply come from some intermediate node
{
If (Ltt<Tt)
Then
Node is malicious node;
Discard this route and broadcasts some ALARM packet to all intermediate node to isolate this node from the network;
Else
Node is a trusty node; // Route is assume to be safe
Send data packets through this path;
}
Step 5: End

6. SIMULATION AND RESULTS

Performance of proposed trust based AODV routing protocol is analyzed by the ns-2 simulator [13]. MANET environment (Table 1) is fully formed using this network simulator. In the simulation the number of node is 20, 30, 40 and 50, node's mobility characteristic is random movement. Routing decision in this environment is carried out by both AODV and modified AODV protocols. Results are traced out from this simulation. Finally, they are presented in the form graph for the comparison of these protocols.

Table 1 Scenario specification

Parameter	**Value**
Simulation duration	30 sec.
Simulation area	1500 meter ×1500 meter
N0. of nodes	20, 30, 40, 50
Maximum segment size	512 bytes
Data rate	2 mbps
Radio range	250 meter
Traffic type	CBR
Mobility	Random way point

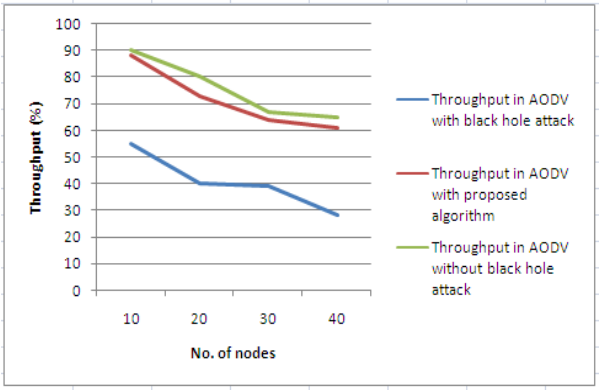

Figure 2 Impact of black hole on network Throughput and throughput in proposed algorithm under black hole attack

In Figure 2 representing the impact of black hole attack on network throughput. The throughput of network is decreased due to the impact of black hole but the proposed algorithm giving the good throughput with black hole attack.

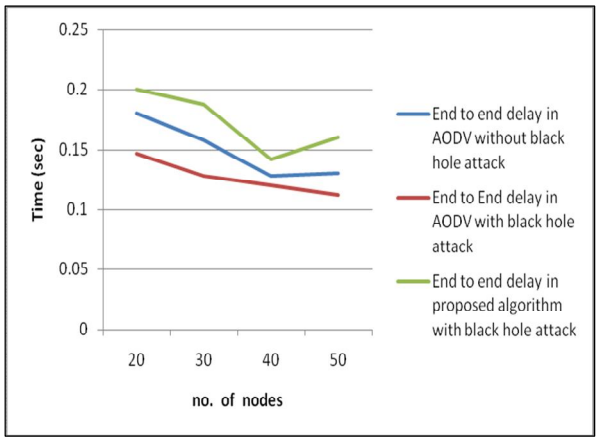

Figure 3 Impact of black hole on network End-to-End delay and End-to-End delay in proposed algorithm under black hole attack.

From the figure 3 it can be observed that, there is slight increase in the average end-to-end delay without the effect of black hole, as compared to the effect of black hole attack, This is due to the immediate reply from the malicious node i.e. the nature of malicious node here is it would not check its routing table.

7. CONCLUSION

In this paper, we have analyzed and describe the condition to detect the single black hole in the network. We have used AODV routing protocol and we have make it more secure routing protocol and detected the black hole attack using last transmission time. Security of our approach is better than AODV's security. Here we are saving memory requirement for detection of black hole attack.

REFERENCES

1. C. Siva Ram Murthy and B.S. Manoj, **—Ad Hoc Wireless Networks: Architectures and Protocols, Prentice Hall (2004).**
2. Loay Abusalah, Ashfaq Khokhar and Mohsen Guizani, **—A Survey of Secure Mobile Ad Hoc Routing Protocols,IEEE Communications Surveys & Tutorials,** Vol 10, No. 4 pp. 78-93 (2008).
3. D. P. Agrawal and Q.-A. Zeng, **Introduction to Wireless and Mobile Systems, Brooks/Cole Publishing**, Aug. 2002.
4. Songbai Lu, Longxuan Li, Kwon-Yan Lam and Lingvan Jia **—SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack International Conference on Computational Intelligence and Security**, pp 421-425 (2009).
5. Devid Cerri, Alessandro Ghioni, CEFRIEL-Politecnico di Milano **—Securing AODV: The A-SAODV secure Routing Prototype,‖ IEEE Communication Magzine**, pp 120-125 (2008).
6. 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 Communicatio**n, pp 672-676 (2010).
7. Patroklos G. Argyroudis and Donal O'Mahony, **—Secure Routing for Mobile Ad-hoc Network, IEEE Communication Surveys & Tutorials**, pp 2-21 (2005).
8. H. Weerasinghe and H. Fu, "**Preventing cooperative black hole attacks in mobile ad-hoc networks: simulation, implementation and evaluation," International Journal of Software Engineering and Its Application**s, Vol. 2, No. 3 (2008) pp. 39-54.
9. P. Raj and P. Swadas, "**A dynamic learning system against black hole attack in AODV based MANET," IJCSI International Journal of Computer Science**, Vol. 2, (2009) pp. 54-59
10. J.-F. Raymond, **—Traffic Analysis: Protocols, Attacks, Design Issues and Open Problems, Proc. Wksp. Design Issues in Anonymity and Unobservability, Berkeley**, CA, July 2000, pp. 7–26.
11. M. Sayee Kumar, S. Selvarajan, S. Balu, **—ANODR based anomaly detection for black hole and route disrupt attacks, International Conference on Computing, Communication and Networking** , pp 1-5 (2008).
12. Nidhi Sharma, Sanjeev Rana and R.M. Sharma, **—Provisioning of Quality of Se Service in MANETs Performance Analysis &Comparison (AODV AND DSR), ‖ International Conference on Computer Engineering and Technology,** pp 243-248 (2010).
13. http://www.isi.edu/nsnam/ns/