Volume 3, Issue 5, May 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Dealing with Black Hole Attack in Mobile Ad Hoc Network (MANET)

Sonia [1]
Research scholar, S.K.I.E.T
Kurukshetra, Haryana, India

Abhishek Aggarwal [2]
Asst.Prof., S.K.I.E.T
Kurukshetra, Haryana, India

Abstract: The proliferation of Mobile Ad hoc Networks (MANETs) helps to realize the nomadic computing paradigm with ubiquitous access. Though they ensure self-maintainable, dynamic and temporary topology, the MANETS also suffer from constraints in power, storage and computational resources. In addition, the pervasiveness, ubiquity and the inherent wireless nature, warrant appropriate security provisions in these networks that becomes difficult to support, amidst the lack of sufficient resource strengths. As a result, the MANETs are more vulnerable to various communications security related attacks. In this paper we are addressing the problem of one of the popular security threat that is black hole attack. The nature of these networks and the limited processing capabilities of the nodes make them vulnerable to malicious attacks. These attacks are caused by malicious nodes that advertise the availability of the shortest route to the intended destination, thereby exploiting the functioning of the AODV protocol and retaining the data packets. AODV is principal routing protocol used in ad hoc network. The security of the AODV protocol is compromised by this particular type of attack called 'Black Hole' attack [1]. This leads to loss of critical and sensitive information being relayed across the network. We propose a technique that overcomes the shortcomings of this protocol, and makes it less vulnerable to such attacks by identifying the malicious node and isolating it from the network. We have developed a scheme. The scheme proposed to wait and check the replies from all the neighboring nodes to find a safe route.

Keywords: Ad hoc Networks, Routing Protocols, AODV, Black Hole Attack.

I. Introduction

MANETs [1] is a kind of point to point transmission type and is a group of mobile nodes communicate with each other by wireless. Each node among the MANETs not only works as a host but also need to play the role of router. While receiving data, nodes also need to help other nodes to forward packets, thereby forming a wireless local area network. However, the security of this particular network environment has many defects. In addition to the drawback of using radio wave to transmit in nature, there are still many problems, such as limited power, lower computing ability, and dynamic topology and so on. These problems make the security of MANET lower than cable network and produce many security Issues. The provision of security services for the above becomes all the more essential because of their potential in the military applications like interconnection between different units, event monitoring, contour detection and so on [2, 3,4]. Due to the lack of a central infrastructure and limited processing capabilities of individual nodes it is very difficult to have an elaborate ad hoc membership scheme taking into account the large size of these networks. In such circumstances even the presence of a small number of adversarial nodes can result in compromised routes leading to extremely high routing overhead and unacceptable end-to-end delays. One of the major attacks caused by tampering the route discovery process is the Black Hole attack [1]. In this kind of attack the malicious nodes in the network advertise the availability of a fresh enough route to the destination without checking their routing tables. In this process they always happen to be the first to reply to a route request and thus intercept the data packets being relayed in the network and retain them. Most important networking operations include routing and network management [6]. Routing protocols can be divided into proactive, reactive and hybrid protocols, depending on the routing topology. Proactive protocols are typically table-driven. Examples of this type include DSDV, WRP. Reactive or source-initiated on-demand protocols, in contrary, do not periodically update the routing information. It is propagated to the nodes only when necessary. Example of this type includes DSR; AODV and ABR. Hybrid protocols make use of both reactive and proactive approaches. Example of this type includes TORA, ZRP. Security is a major concern in all forms of communication networks, but ad hoc networks face the greatest challenge due to their inherent nature. As a result, there exist a slew of attacks that can be performed on an Ad hoc network. [1][5].

II. AODV AND BLACK HOLE ATTACK

A. OVERVIEW OF AODV

AODV is a reactive [2] routing protocol that does not require maintenance of routes to destination nodes. As its name indicates AODV is an on-demand routing protocol that discovers a route only when there is demand from mobile node. In ad hoc network first route discovery takes place, which means if a mobile node that wishes to communicate with other node first broadcast a RREQ (Route Request) message to find a fresh route to a desired destination node. Every neighbor node that receives RREQ broadcast first saves the path the RREQ was transmitted along its routing table. It then checks its routing table to see if it has a fresh enough route to the destination node provided in RREQ message. Destination sequence number attached to it indicates the freshness. If a node finds a fresh enough route it uncast a RREP (route reply) message back along the saved path to the source node or it rebroadcast the RREQ message otherwise. The same process continues until an RREP message from the destination node or an intermediate node that has a fresh route to the destination node received by the source node.

B. BLACK HOLE ATTACKS

A black hole attack is a kind of Denial of service attack in mobile ad hoc networks. In this attack, a malicious node sends [4] a fake RREP packet to the source node that has initiated a route discovery, in order to show itself as a destination node or an intermediate node to the actual destination node. In such a case the source node would send all of its data packets to the malicious node the malicious node then absorbs all the packets and drops them fully or sometimes partially. As a result source and destination node will not be able to communicate *with each other.*

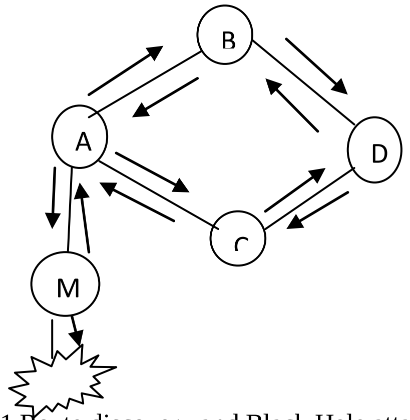


Fig.1 Route discovery and Black Hole attack by malicious node M

Consider the case in fig. 1 where A is the source node D is the destination node and M is the malicious node here node A starts with the route discovery process then the node M advertises itself as having a valid shortest route to the destination, even though the route is fake with the purpose of intercepting packets. Moreover a malicious node does not need to check its routing table when sending a spurious message; its response is more likely to reach the source node first. This makes the source node think that the route discovery process is complete, ignore all other reply messages and begin to send data packets. As a result, all the packets through the malicious node are simply absorbed discarded and then lost. The malicious node could be said to form a black hole in the network.

III. PROPOSED SOLUTION AGAINST BLACK HOLE ATTACK

We propose a solution that is an enhancement of the basic AODV routing protocol, which will be able to avoid black holes. To reduce the probability it is proposed to wait and check the replies from all the neighboring nodes to find a safe route. According to this proposed solution before sending the data the source node or requesting node has to wait till other replies with next hop details from the other nearby nodes. After receiving the first request it sets timer in the ETT (expired timer table). It will store the 'Sequence number', and the time at which the packet arrives, in a 'accumulate Route Reply Table' (ARRT). The time for which every node will wait is proportional to its distance from the source. It calculates the 'timeout' value based on arriving time of the first route request. After the timeout value, it first checks in ARRT whether there is any repeated next hop node. If any repeated next hop node is present in the reply paths it assumes the paths are correct or the chance of malicious paths is limited.

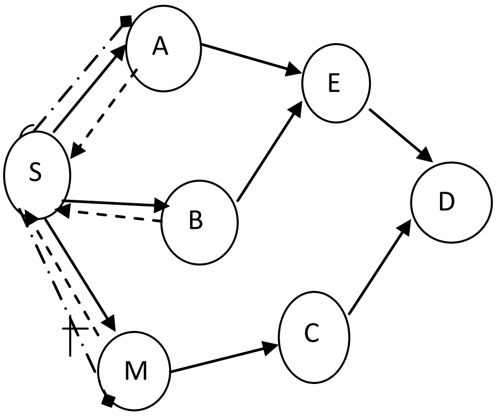
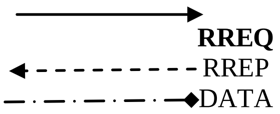


Figure 2. Solution to Black hole



C. Working principal of proposed solution

In fig 2, SN (source node) wants to transmit to DN (destination node) .so it first start route discovery process by broadcasting the route request (RREQ) to all neighbors. Here node A, node, nodeM receives this request. The malicious node M has no intention to transmit the DATA packets to the destination node DN but it wants to intercept/collect the DATA from the source node SN. So it immediately replies to the request as (M – C). Instead of transmitting the DATA packets immediately through M, SN has to wait for the reply from the other nodes. After some time it will receive the reply from node A as (A – E), and node B as (B – E).

According to this proposed solution it first check the path that contains repeated next hop node to the destination. If there is no repeated node select random path and transmits the data through that path.

Table1: Routing information table

Source node(SN)	From node	Through node	Destination node(DN)
SN	M	C	DN
SN	A	E	DN
SN	B	E	DN

IV. Algorithm for the proposed solution

Algorithm to deal with black hole attack

```
Notations
SN: source node; DN: destination node
NHN: next hop node; IN: intermediate node
RREQ: route request;  RREP: route reply
ARRT: accumulate route reply
RIT: routing information table
ETT: expired timer table
SN starts route discovery by broadcasting            RREQ
IN: receives route request
while(destination node(DN))
{
   receives(RREQ) from source
 if(INaddr==RREQ.DNaddr)
{
  send route reply (RREP) to source
else if (INaddr exists in RREQaddr)
 neglect the route request(RREQ)
else
check any route to the destination in RIT
then send RREP to source
SN: receives (RREP)
{
get(present time value)
set(timer value)//proportional to the distance from the source
total time=present time value+ timer value
while(present time value<=total time)
{
record (seq.no.,arrival time)in ARRT
increment the entry in ARRT
}
   }
}
check repeated next hop node(NHN)
{
 select repeats NHN(RREP)ARRT
route DATA as route is secure
}
```

```
else
randomly select the RREP from ARRT
rout DATA through this randomly selected route
```

D. Maintance of route:

After selecting the route between the source and the destination and during data transmission, if any node participating in the route moves, then the node that tries to send data will detect a link break. Then it tries to salvage the packet, that is, it searches in its cache to find an alternate route to reach the destination. If there is any route, then it will send data through that new route. Otherwise, it creates a 'Route Error' packet and sends it to the source node to indicate the failure of the link. When forwarding the route error packet, the intermediate nodes remove the cache entries corresponding to the node, which moved and then forward the packet. On receiving the error packet, the source node also removes the entries corresponding to the node and tries to find another route to the destination in its cache.

V. Conclusion and future work

MANET has the ability to deploy a network where a traditional network infrastructure environment cannot possibly be deployed. Security of MANET is one of the important features for its deployment. In our thesis we have analyzed the behavior and challenges of security threats in mobile ad hoc networks with solution finding technique. In this paper, we have studied the routing security issues of MANETs, described the black hole attack that can be mounted against a MANET, and proposed a feasible solution for it on the top of AODV protocol to avoid the black hole attack, and also prevented the Network form further malicious behavior. Proposed method can be used to find the secured routes and prevent the black hole nodes in the MANET.

VI. Future scope

Wireless Ad-Hoc networks are widely used networks due to their flexible nature i.e. easy to deploy regardless of geographic constraints. These networks are exposed to both external and internal attacks as there is not centralized security mechanism. A lot of research work is still need in this area.

As future work, research work intend to develop simulations to analyze the performance of the proposed solution based on the various security parameters like mean delay time, packet overhead, memory usage, mobility, increasing number of malicious node, increasing number of nodes and scope of the black hole nodes and also focusing on resolving the problem of multiple attacks against AODV.

References

[1] Hongmei Deng, Wei Li, and Dharma P. Agarwal, "Routing Security in Wireless Ad Hoc Networks", University of Cincinnati, IEEE Communications magazine, October 2002.

[2] RFC 2501, http://www.faqs.org/rfcs/rfc2501.html.

[3] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J.Dixon, and K. Nygard, "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks," 2003 International Conference on Wireless Networks (ICWN'03), June 2003.

[4] H. Weerasinghe and H. Fu, "Preventing Cooperative Black Hole Attacks in Mobile Ad hoc Networks: Simulation Implementation and Evaluation," IEEE International Conference on Communication, 2007.

[5] M.G. Zapata, N. Asokan. Securing Ad hoc Routing Protocols. ACM WiSe, September 2002.

[6] C K. Toh, Ad Hoc Mobile Wireless Networks: Protocols and Systems, Prentice Hall, January 2002.

[7] Elizabeth M. Royer, Chai-Keong Toh, "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks",IEEE Personal Communications, Vol. 6, No. 2, pp. 46-55, April 1999. http://users.ece.gatech.edu/~cktoh/royer.html.

[8] S. Marti, T. J. Giuli, K. Lai and M. Baker, "Mitigating Routing Misbehavior in Ad Hoc Networks", Proc. 6th Annual Int'l.Conf. Mobile Comp. and Net, Boston, MA. pp. 255-265. August 2000.

[9] Vesa Kärpijoki, "Security in Ad hoc Networks," http://www.tcm.hut.fi/Opinnot/Tik-110.501/2000/papers/karpijoki.pdf.

[10] V. Karpijoki, "Security in Ad Hoc Networks", Seminar on Net Work Security, HUT TML 2000.

[11] C.E. Perkins, S.R. Das, and E. Royer, "Ad-Hoc on Demand Distance Vector (AODV)", March 2000, http://www.ietf.org/internet-drafts/draft-ietf-manet-aodv-05.txt

[12] Lidong Zhou, Zygmunt J. Haas, "Securing Ad Hoc Networks", IEEE network, special issue, November/December 1999.

[13] Yi-Chun Hu, Adrian Perrig, "A Survey of Secure Wireless Ad Hoc Routing", IEEE Security and Privacy May/June 2004.

[14] Yih-Chun, Adrian Perrig, David B. Johnson, "Ariadne: A secure On-Demand Routing Protocol for Ad Hoc Networks", 2002