Rajesh J. Nagar, Kajal S. Patel / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 2, Issue 1,Jan-Feb 2012, pp.1116-1120

Securing AODV Protocol against BlackholeAttacks

Rajesh J. Nagar*, Kajal S. Patel**

*(Department of Information Technology, Gujarat Technological University, India)
**(Department of Computer Engineering, Gujarat Technological University, India)

Abstract—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.The nodes 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. The MANETS sufferfrom constraints in power, storage and computational resources.In addition, the pervasiveness, ubiquity and the inherentwireless nature, warrant appropriate security provisions inthese networks that becomes difficult to support, amidst the lackof sufficient resource strengths. As a result, the MANETs aremore vulnerable to various communications security relatedattacks.In this paper, therefore, we attempt to focus on analyzing andimproving the security of one of the popular routing protocol forMANET's viz. the Ad hoc On Demand Distance Vector (AODV)routing protocol. Our focus specifically, is on ensuring thesecurity against the Blackhole Attacks. We proposemodifications to the AODV protocol and justify the solutionwith appropriate implementation and simulation using NS-2.33.Our analysis shows significant improvement in Packet DeliveryRatio (PDR) of AODV in presence of Blackhole attacks, withmarginal rise in average end-to-end delay.

***Index Terms*—AODV, Blackhole attack, MANET, Routing protocols, Security.**

I. INTRODUCTION

At present, the study of MANETs has gained a lotof interest of researchers [1]. A Mobile Adhoc Network(MANET), as the name suggests, is a self-configuringnetwork of wireless and hence mobile devices that constitute anetwork capable of dynamically changing topology. Thenetwork nodes in a MANET, not only act as the ordinarynetwork nodes but also as the routers for other peer devices[2].

The idea of adhoc networking is sometimes also calledinfrastructure less networking [1], since the mobile nodesin the network dynamically establish routing amongthemselves to form their own network "on the fly." Someexamples of the possible uses of ad hoc networking include students using laptop computers to participate inan interactive lecture, business associates sharinginformation during a meeting, soldiers relayinginformation for situational awareness on the battlefield,and emergency disaster relief personnel coordinatingefforts after a hurricane or earthquake. Many differentprotocols have been proposed to solve the multihoprouting problem in ad hoc networks, each based ondifferent assumptions and intuitions.

We attempt revisiting the routing protocols applicable inMANETs, in this research exercise and investigate whether itis possible to strengthen the existing attempts on devisingsecure routing protocols for MANETs. The network layer in MANETs is susceptible to variousattacks viz. eavesdropping with a malicious intent, spoofingthe control and/or data packets transacted, maliciousmodification/alteration of the packet contents and theDenial-of-service (DoS) attacks viz.Wormhole attacks,Sinkhole attacks, Blackhole attacks.Amongst these, in this paper, we attempt in analyzing andimproving the security of the routing protocol AODV [4]against the Blackhole attacks.

The rest of this paper is organized as follows. In Section 2, we briefly describe the different types of routing protocols with its descriptions and detail note on AODV routing protocol. Section 3 discusses about blackhole attack. Section 4 presents the related work in literature, Section 5 we discuss our solution to AODV algorithm. Finally, we conclude in Section 6 with future scope.

II. ROUTING PROTOCOLS

The primary goal of routing protocols in ad-hoc network isto establish optimal path (min hops) between source anddestination with minimum overhead and minimumbandwidth consumption so that packets are delivered in atimely manner. A MANET protocol should functioneffectively over a wide range of networking context fromsmall ad-hoc group to larger mobile Multihop networks.As fig 1 shows the categorization of these routingprotocols.

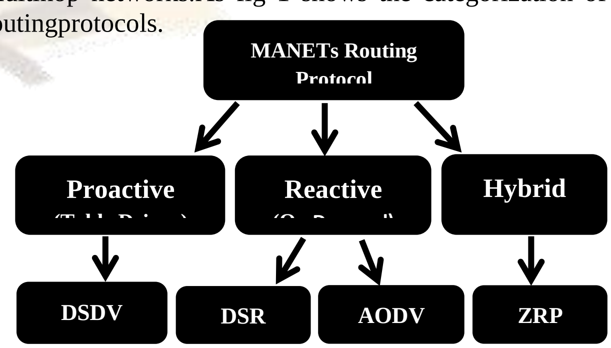


Fig 1. Hierarchy of Routing Protocols

Routing protocols can be divided into proactive, reactiveand hybrid protocols, depending on the routingtopology. Proactive protocols are typically table-driven.Examples of this type include Destination SequenceDistance Vector (DSDV). 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 Dynamic

Source Routing (DSR) and Ad Hoc On-Demand Distance Vector (AODV). Hybrid protocols make use of both reactive and proactive approaches. Example of this type includes Zone Routing Protocol (ZRP).

A. Proactive Routing Protocol

In a network utilizing a proactive routing protocol, every node maintains one or more tables representing the entire topology of the network. These tables are updated regularly in order to maintain up-to-date routing information from each node to every other node. To maintain the up-to-date routing information, topology information needs to be exchanged between the nodes on a regular basis, leading to relatively high overhead on the network. On the other hand, routes will always beavailable on request. Many proactive protocols stem fromconventional link state routing, including the OptimizedLink State Routing protocol (OLSR).

B. ReactiveRouting Protocol

Reactive routing protocols [1] are on-demand protocols.These protocols do not attempt to maintain correct routinginformation on all nodes at all times. Routing informationis collected only when it is needed, and routedetermination depends on sending route queriesthroughout the network. The primary advantage ofreactive routing is that the wireless channel is not subjectto the routing overhead data for routes that may never beused. While reactive protocols do not have the fixedoverhead required by maintaining continuous routingtables, they may have considerable route discovery delay.Reactive search procedures can also add a significantamount of control traffic to the network due to queryflooding. Because of these weaknesses, reactive routing isless suitable for real-time traffic or in scenarios with ahigh volume of traffic between a large numbers of nodes.

C. Hybrid Routing Protocol

Wireless hybrid routing is based on the idea of organizingnodes in groups and then assigning nodes differentfunctionalities inside and outside a group [1]. Bothrouting table size and update packet size are reduced byincluding in them only part of the network (instead of thewhole); thus, control overhead is reduced. The mostpopular way of building hierarchy is to group nodesgeographically close to each other into explicit clusters.Each cluster has a leading node (cluster head) tocommunicate to other nodes on behalf of the cluster. Analternate way is to have implicit hierarchy. In this way,each node has a local scope. Different routing strategiesare used inside and outside the scope. Communicationspass across overlapping scopes. More efficient overall routing performance can be achieved through thisflexibility. Since mobile nodes have only a single omnidirectionalradio for wireless communications, this type ofhierarchical organization will be referred to as logicalhierarchy to distinguish it from the physically hierarchicalnetwork structure.

D. An Overview of AODV Routing Protocol

AODV routing protocol is based on DSDV and DSRalgorithm and is a state-of-the-art routing protocol thatadopts a purely reactive strategy: it sets up a route ondemandat the start of a communication session, and usesit till it breaks, after which a new route setup is initiated[2]. This protocol is composed of two mechanism (1)Route Discovery and (2) Route Maintenance. AODV usesRoute Request (RREQ), Route Reply (RREP) controlmessages in Route Discovery phase and Route Error(RERR) control message in Route Maintenance phase.The header information of this control messages can beseen in detail in [3].

In general, the nodes participating in the communicationcan be classified as source node, an intermediate node ora destination node. With each role, the behavior of a nodeactually varies. When a source node wants to connect to adestination node, first it checks in the existing route table,as to whether a fresh route to that destination is availableor not. If a fresh enough route is available, it uses thesame. Otherwise the node initiates a Route Discovery bybroadcasting a RREQ control message to all of itsneighbours. This RREQ message will further be forwarded(again broadcasted) by the intermediate nodes to theirneighbors. This process will continue until the destinationnode or an intermediate node having a fresh route to thedestination. At this stage eventually, a RREP controlmessage is generated. Thus, a source node after sending aRREQ waits for RREPs to be received. Fig. 2 depicts thetraversal of control messages.

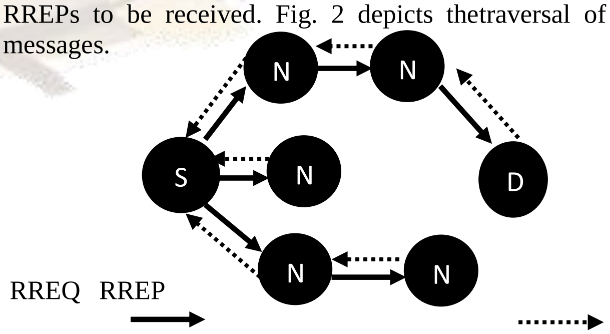


Fig 2. Traversal of Control Messages

III. BLACKHOLE ATTACK

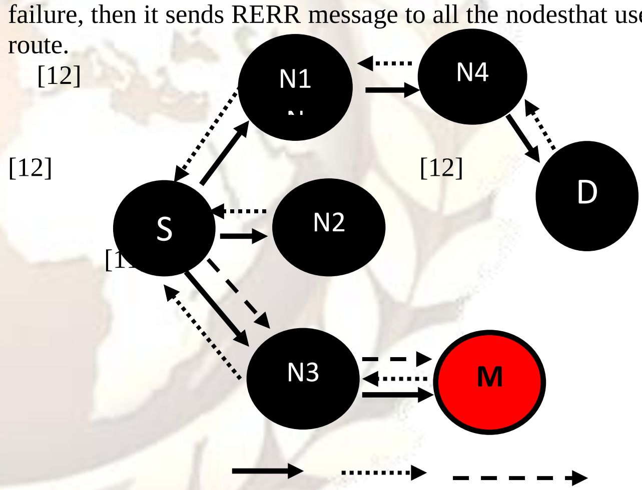
Routing protocols are exposed to a variety of attacks.Black hole attack is one such attack and a kind of Denial Of Service (DoS)in which a malicious node makes use of the vulnerabilities of the route discovery packets of the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept [3]. This attack aims at modifying the routing protocol so that traffic flows through a specific node controlled by the attacker. During the Route Discovery process, the source node sends RREQ packets to the intermediate nodes to find fresh path to the intended destination. Maliciousnodes respond immediately to the source node as these nodes do not refer the routing table. The source node assumes that the route discovery process is complete, ignores other RREP messages from other nodes and selects the path through the malicious node to route the data packets. The malicious node does this by assigning ahigh sequence number to the reply packet. The attackernow drops the received messages instead of relaying themas the protocol requires.

As an example, consider the following scenario in fig. 3.We illustrate a typical scenario of the protocol packetexchanges, depicting the generation and traversal ofRREQ and RREP control messages. The node S isassumed to be the source node desiring to communicatewith node D. Thus, as per the explanation earlier, node Swould generate the RREQ control message and broadcastit. The broadcasted RREQ control message is expected tobe received by the nodes N1, N2 and N3. Assuming thatthe node N3 has a route to node D in its route table, thenode N3 would generate a RREP control message andupdate its routing table with the accumulated hop countand the destination sequence number of the destinationnode.

Destination Sequence Number [11] is a 32-bit integerassociated with every route and is used to decide thefreshness of a particular route. The larger the sequencenumber, the fresher is the route [4]. Node N3 will nowsend it to node. Since node N1 and node N2 do not have aroute to node D, they would again broadcast the RREQcontrol message. RREQ control message broadcasted bynode N3 is also expected to be received by node M(assumed to be a malicious node). Thus, node M beingmalicious node, would generate a false RREP controlmessage and send it to node N3 with a very highdestination sequence number, that subsequently would besent to the node S.However, since, the destination sequence number is high,the route from node N3 will be considered to be fresherand hence node S would start sending data packets tonode N3. Node N3 would send the same to the malicious node. The RREQ control message from node N1, would eventually reach node D (destination node), which would generate RREP control message and route it back. However, since the node S has a RREP control message with higher destination sequence number to that route, node S will ignore two genuine RREP control messages. If any link is disconnected during the transfer of packets then RERR control message is generated.

For every RREP control message received, the sourcenode would first check whether it has an entry for thedestination in the route table or not. If it finds one, thesource node would check whether the destinationsequence number in the incoming control message ishigher than one it sent last in the RREQ or not. If thedestination sequence number is higher, the source nodewill update its routing table with the new RREP controlmessage; otherwise the RREP control message will bediscarded.

In *Route Maintenance phase*, if a node finds a link breakor failure, then it sends RERR message to all the nodesthat uses the route.



RREQ RREP Data Packet

[ ] – DestinationSequence Number
S – Source Node D- Destination Node
M – Malicious Node

Fig 3. Protocol Packet Exchanges

IV.RELATED WORK

There indeed have been numerous attempts published inthe literature that aim at countering the Black attacks. Wesurvey them in the following.

In [5], the authors discuss a protocol that requires theintermediate nodes to send RREP message along with the next hop information. When the source node get thisinformation, it sends a RREQ to the next hop to verifythat the target node (i.e. the node that just sent back theRREP packet) indeed has a route to the intermediate nodeand to the destination. When the next hop receives aFurther Request, it sends a Further Reply which includesthe check result to the source node. Based on informationin Further Reply, the source node judges the validity of theroute. In this protocol, the RREP control packet ismodified to contain the information about next hop. Afterreceiving RREP, the source node will again send RREQto the node specified as next hop in the received RREP.Obviously, this increases the routing overhead and end-to-enddelay. In addition, the intermediate node needs tosend RREP message twice for a single route request.

In [6], the authors describe a protocol in which the sourcenode verifies the authenticity of a node that initiatesRREP by finding more than one route to the destination.When source node receives RREPs, if routes todestination shared hops, source node can recognize a saferoute to destination.

Sanjay Ramaswamy, et al [7] proposed a method foridentifying multiple black hole nodes. They are first topropose solution for cooperative black hole attack. Theyslightly modified AODV protocol by introducing datarouting information table (DRI) and cross checking.Every entry of the node is maintained by the table. Theyrely on the reliable nodes to transfer the packets.

Latha Tamilselvan, Dr. V Sankaranarayanan[8] proposeda solution with the enhancement of the AODV protocolwhich avoids multiple black holes in the group. Atechnique is given to identify multiple black holescooperating with each other and discover the safe route byavoiding the attacks. It was assumed in the solution thatnodes are already authenticated and therefore canparticipate in the communication. It uses Fidelity tablewhere every node that is participating is given a fidelitylevel that will provide reliability to that node. Any nodehaving 0 value is considered as malicious node and iseliminated.

Hesiri Weerasinghe [9] proposed the solution whichdiscovers the secure route between source and destinationby identifying and isolating cooperative black hole nodes.This solution adds on some changes in the solutionproposed by the S.Ramaswamy to improve the accuracy.This algorithm uses a methodology to identify multipleblack hole nodes working collaboratively as a group toinitiate cooperative black hole attacks. This protocol is aslightly modified version of AODV protocol byintroducing Data Routing Information (DRI) table andcross checking using Further Request (FREQ) and FurtherReply (FREP). Most of the papers have addressed theblack hole problem on the protocol such as AODV.

V. THE PROPOSED SOLUTION

The solution that we propose here is basically onlymodifies the working of the source node without alteringintermediate and destination nodes by using a methodcalled Prior_ReceiveReply. In this method three thingsare added, a new table RR-Table(Request Reply), a timerWT (Waiting Time) and a variable MN-ID (MaliciousNode ID) to the data structures in the default AODVProtocol.

Algorithm: Prior-ReceiveReply Method

DSN – Destination Sequence Number, NID – Node ID,MN-ID – Malicious Node ID.

Step 1: (Initialization Process)
Retrieve the current time and add the current time with waiting time

Step 2: (Storing Process)
Store all the Route Replies DSN and NID inRR-Table. Repeat the above process until the time exceeds

Step 3: (Identify and Remove Malicious Node)
Retrieve the first entry from RR-Table, If DSN is much greater than SSN thendiscard entry from RR-Tableand store its NID in MN-ID

Step 4: (Node Selection Process)
Sort the contents of RR-Table entries accordingto the DSNSelect the NID having highest DSN among
RR-table entries

Step 6: (Continue default process)
Call ReceiveReply method of defaultAODV Protocol

The above algorithm starts from the initialization process, first set the waiting time for the source node to receive the RREQ coming from other nodes and then add the current time with the waiting time. Then in storing process, store all the RREQ Destination Sequence Number (DSN) and its Node Id in RR-Table until the computed time exceeds. Generally the first route reply will be from the malicious node with high destination sequence number, which is stored as the first entry in the RR-Table.

Then compare the first destination sequence number with the source node sequence number, if there exists much more differences between them, surely that node is the malicious node, immediately remove that entry from the RR-Table. This is how malicious node is identified and removed. Final process is selecting the next node id that has the higher destination sequence number, is obtained by sorting the RR-Table according to the DSEQ-NO column, whose packet is sent to

ReceiveReply method in order to continue the default operations of AODV protocol.

In addition, the proposed solution maintains the identityof the malicious node as MN-Id, so that in future, it candiscard any control messages coming from that node.Now since malicious node is identified, the routing tablefor that node is not maintained. In addition, the controlmessages from the malicious node, too, are not forwardedin the network. Moreover, in order to maintain freshness,the RR-Table is flushed once a route request is chosenfrom it. Thus, the operation of the proposed protocol isthe same as that of the original AODV, once themalicious node has been detected.

The main benefits of modifying the AODV protocol is (1)The malicious node is identified at the initial stage itselfand immediately removed so that it cannot take part infurther process. (2) With no delay the malicious node areeasily identified i.e. as we said before all the routes hasunique sequence number. Generally the malicious node has the highest Destination Sequence number and it isthe first RREP to arrive. So the comparison is made onlyto the first entry in the table without checking otherentries in the table. (3) No modification is made in otherdefault operations of AODV Protocol (4) Betterperformance produced in little modification and (5) Lessmemory overhead occurs because only few new things areadded.

Table 1: Content of RR-table with malicious node

RNO	DSEQ-NO	NODE-ID
1	9876543210	N3
2	11	N2
3	12	N1

Table 2: Content of RR-table without malicious node and sorted according to DSEQ-NO.

RNO	DSEQ-NO	NODE-ID
1	12	N1
2	11	N2

VI. CONCLUSION

In this paper we have mentioned the AODV protocol andBlack hole attack in MANETs. We have proposed afeasible solution for the black hole attacks that can beimplemented on the AODV protocol. The Proposedmethod can be used to find the secured routes and preventthe black hole nodes in the MANET. As future work, weintend to develop simulations to analyze the performanceof the proposed solution based on the various securityparameters like packet delivery ratio (PDR), mean delaytime, packet overhead, memory usage, mobility, increasing number of malicious node, increasing numberof nodes and scope of the black hole nodes.

REFERENCES

[1] Imrich Chlamtac, Marco Conti, Jennifer J.-N. Liu "Mobile ad hocnetworking: imperatives and challenges", School of Engineering,University of Texas at Dallas, Dallas, TX, USA, 2003.

[2] Gianni A. Di Caro, Frederick Ducatelle, Luca M. Gambardella. "Asimulation study of routing performance in realistic urbanscenarios for MANETs". In: Proceedings of ANTS 2008, 6thInternational Workshop on Ant Algorithms and SwarmIntelligence, Brussels, Springer, LNCS 5217, 2008

[3] C. Perkins. "(RFC) request for Comments-3561", Category:Experimental, Network, Working Group, July 2003.

[4] Satoshi Kurosawal, Hidehisa, Nakayama, Nei Kato, AbbasJamalipour and Yoshiaki Nemoto. "Detecting Blackhole Attackon AODV-based Mobile Ad Hoc Networks by Dynamic LearningMethod." In: International Journal of Network Security, Vol. 5,No.3, pp.338–346, Nov. 2007.

[5] H. Deng, W. Li, and D. P. Agrawal. "Routing Security in AdhocNetworks." In: IEEE Communications Magazine, Vol. 40, No. 10,pp. 70-75, Oct. 2002.

[6] M. A. Shurman, S. M. Yoo, and S. Park, "Black hole attack in wireless ad hoc networks." In: Proceedings of the ACM 42ndSoutheast Conference (ACMSE'04), pp 96-97, Apr. 2004.

[7]. Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, JohnDixon, and Kendall Nygard, "Prevention of Cooperative BlackHole Attack in Wireless Ad Hoc Networks", 2003 InternationalConference on Wireless Networks (ICWN 03), Las Vegas,Nevada, USA.

[8]Tamilselvan, L. Sankaranarayanan, V. "Prevention of BlackholeAttack in MANET",JournalOfNetworks ,Vol.3,No.5,May2008.

[9] Hesiri Weerasinghe and Huirong Fu, Member of IEEE, PreventingCooperative Black Hole Attacks in Mobile Adhoc Networks:Simulation mplementationAndEvaluation,IJSEA,Vol2,No.3,July2008.

[10] Nital Mistry, Devesh C Jinwala, Member, IAENG, Mukesh Zaveri,"Improving AODV Protocol against Blackhole Attacks",Proceedings of the International MultiConference of Engineersand Computer Scientists 2010 Vol II, IMECS 2010, March 17-19, 2010, Hong Kong.