2011 International Conference on Computer and Software Modeling
IPCSIT vol.14 (2011) © (2011) IACSIT Press, Singapore

Detection and Removal of Cooperative and Multiple Black Hole Attack in Mobile ADHOC Networks

Mehdi Medadian [1], Ahmad Mebadi [2] and Khossro Fardad [1 +]

[1] Department of Computer Engineering Behbahan Branch, Islamic Azad University, Behbahan, Iran
[2] Department of Computer Engineering, Loghman Hakim University, Gorgan, Iran

Abstract. A mobile ad hoc network (MANET) is an autonomous network that consists of mobile nodes that communicate with each other over wireless links. In the absence of a fixed infrastructure, nodes have to cooperate in order to provide the necessary network functionality. One of the principal routing protocols used in Ad hoc networks is AODV (Ad hoc on demand Distance Vector) protocol. The security of the AODV protocol is threaded by a particular type of attack called 'Black Hole' attack. In this attack a malicious node advertises itself as having the shortest path to the destination node. If these malicious nodes work together as a group then the damage will be very serious. This type of attack is called cooperative black hole attack. To combat with black hole attack, it is proposed to wait and check the replies from all the neighboring nodes to find a safe route but this approach suffers from high delay. In this paper, an approach is proposed to combat the Cooperative/ Multiple Black hole attack by using negotiation with neighbors who claim to have a route to destination. the Simulation's results show that the proposed protocol provides better security and also better performance in terms of packet delivery than the conventional AODV in the presence of Black holes with minimal additional delay and Overhead.

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

1. Introduction

Wireless networks can be basically either infrastructure based networks or infrastructure less networks. The infrastructure based networks uses fixed base stations, which are responsible for coordinating communication between the mobile hosts (nodes). The ad hoc networks falls under the class of infrastructure less networks, where the mobile nodes communicate with each other without any fixed infrastructure between them. So the functioning of Ad-hoc networks is dependent on the trust and cooperation between nodes. Nodes help each other in conveying information about the topology of the network and share the responsibility of managing the network. Hence in addition to acting as hosts, each mobile node does the function of routing and relaying messages for other mobile nodes[1]. Routing protocols can be divided into proactive, reactive and hybrid protocols, depending on the routing topology. Security is a major concern in all forms of communication networks, but ad hoc networks face the greatest challenge due to their inherent nature of dependence on other nodes for transmission. As a result, there exist a slew of attacks that can be performed on an Ad hoc network. [1]. Recently, a lot of research has focused on the cooperation issue in MANET. Several related issues are briefly presented here. Researchers have proposed solutions to identify and eliminate a single black hole node [1]. Misbehavior detection and reaction are described in [3], by Marti, Giuli, Lai and Baker. The paper presents two extensions to the DSR algorithm: the watchdog and the path rater. The watchdog identifies misbehaving nodes by listening promiscuously to the next node transmission. This technique is imperfect due to collisions, limited transmit power and partial dropping. Buchegger and Le Boudec [4] present the CONFIDANT protocol. Each node monitor the behavior of its next hop neighbors in

+ Corresponding author. Tel.: + (989166726184); fax: +(986713331901).
E-mail address: (Medadian@Gmail.com).

a similar manner to watchdog. The information is given to the reputation system that updates the rate of the nodes. Based on the rating, the trust manager makes decisions about providing or accepting route information, accepting a node as part of a route and so on. When a neighbor is suspicious in misbehaving, a node informs its friends by sending them an ALARM message. Michiardi and Molva propose the CORE scheme and various related issues in [5]. In this scheme, every node computes a reputation value for every neighbor, based on observations that are collected in the same way as watchdog. Banal and Baker propose OCEAN [6], a scheme for robust packet-forwarding. OCEAN, similarly to previous schemes, is based on nodes' observations. In contrast to previous mechanisms, no rating is exchanged and every node relies on its own information, so the trust management is avoided. The rating is based on a counter that counts the positive and the negative steps a node performs and based on a faulty threshold, the node is added to a faulty list. Bracha Hod, in his thesis [7] highlights various aspects of cooperation enforcement and reliability, when AODV is the underlying protocol. Furthermore, it presents a scalable protocol that combines a reputation system with AODV that addresses reputation fading, second-chance, robustness against liars and load balancing. The proposed solution constructs different reputation properties and misbehaving reaction better suiting to AODV. The security of the AODV protocol is compromised by a particular type of attack called 'Black Hole' attack [1]. In this attack a malicious node advertises itself as having the shortest path to the node whose packets it want to intercept. The proposed approach to combat the Black hole attack is base on node's activity as example number of sent RREQ, number of sent RREP, number of received data and number of sent data packets. When an intermediate node reply RREQ packet, the voting process initiated about activity of replier.

2. Aodv Routing Protocol

The Ad Hoc On-Demand Distance Vector (AODV) routing protocol is an adaptation of the DSDV protocol for dynamic link conditions[2]. Every node in an Ad-hoc network maintains a routing table, which contains information about the route to a particular destination. Whenever a packet is to be sent by a node, it first checks with its routing table to determine whether a route to the destination is already available. If so, it uses that route to send the packets to the destination. If a route is not available or the previously entered route is inactivated, then the node initiates a route discovery process. A RREQ (Route Request) packet is broadcasted by the node. Every node that receives the RREQ packet first checks if it is the destination for that packet and if so, it sends back an RREP (Route Reply) packet. If it is not the destination, then it checks with its routing table to determine if it has got a route to the destination. If not, it relays the RREQ packet by broadcasting it to its neighbors. If its routing table does contain an entry to the destination, then the next step is the comparison of the 'Destination Sequence' number in its routing table to that present in the RREQ packet. This Destination Sequence number is the sequence number of the last sent packet from the destination to the source. If the destination sequence number present in the routing table is lesser than or equal to the one contained in the RREQ packet, then the node relays the request further to its neighbors. If the number in the routing table is higher than the number in the packet, it denotes that the route is a 'fresh route' and packets can be sent through this route. This intermediate node then sends a RREP packet to the node through which it received the RREQ packet. The RREP packet gets relayed back to the source through the reverse route. The source node then updates its routing table and sends its packet through this route. During the operation, if any node identifies a link failure it sends a RERR (Route Error) packet to all other nodes that uses this link for their communication to other nodes. Since AODV has no security mechanisms, malicious nodes can perform many attacks just by not behaving according to the AODV rules. A malicious node *M* can carry out many attacks against AODV. This paper provides routing security to the AODV routing protocol by eliminating the threat of 'Black Hole' attacks.

3. Black Hole Attack

A Black Hole attack [1][8] is a kind of denial of service where a malicious node can attract all packets by falsely claiming a fresh route to the destination and then absorb them without forwarding them to the destination. Cooperative Black hole means the malicious nodes act in a group[7]. When the source node wishes to transmit a data packet to the destination, it first sends out the RREQ packet to the neighboring

nodes. The malicious nodes being part of the network, also receive the RREQ. Since the Black hole nodes have the characteristic of responding first to any RREQ, it immediately sends out the RREP. The RREP from the Black hole reaches the source node, well ahead of the other RREPs. Now on receiving the RREP from the Black hole node, the source starts transmitting the data packets. On the receipt of data packets, the Black hole node simply drops them, instead of forwarding to the destination.

4. The Proposed Method

In this paper, an approach has been proposed to combat black hole attack in AODV routing protocol. In this approach any node uses number rules to inference about honesty of reply's sender. Following codes show the proposed approach. Following codes show the proposed approach.

```
Node_function (packet,time)
{
    IF time is start of simulation THEN
        BEGIN
            Initialize quarantine list;  Initialize activity table of neighbors;  This table has following fields:
            (Node id, number of received data, number of sent data, number of sent rrep )
        END
    IF packet is data THEN
        BEGIN
            INCREMENT number of received data for sender of packet
            IF this node isn't destination THEN
                BEGIN
                    GET next node which it isn't in quarantine list
                    IF find next node for forwarding THEN
                        BEGIN
                            FORWARD packet to next node
                            INCREMENT number of sent data to next node
                        END
                    ELSE
                        SEND error packet to source
                END
            ELSE
                RECIEVE packet
        END
    IF packet is rrep THEN
        BEGIN
            INCREMENT number of received rrep for sender of packet
            IF next isn't in quarantine list THEN
                BEGIN
                    IF sender of rrep has not been good node THEN
                        CREATE an opinion request packet broadcast to neighbors of rrep's
                        sender
                        SET a timer for process responses
                        CREATE a temporary list to save responses
                    FORWARD packet
                END
            ELSE
                DISCARD packet
        END
    IF packet is opinion request THEN
        BEGIN
            CHECK if this node has any opinion about requested node
            IF this node have any opinion THEN
                BEGIN
                    EXTRACTactivities of the requested node from activity table (including number
                    of received data, number of sent data, and number of  sent rrep)
                    CREATE response packet including the required information
                    FORWARD response packet
                END
            ELSE
                FORWARD        packet
        END
    IF packet is response packet THEN
        BEGIN
            IF this node is sender of the opinion request packet THEN
```

```
                    BEGIN
                        EXTRACTinformation from packet (including number of received data, number
                        of sent data, number of sent rrep)
                        SAVE the extracted information in temporary list

                    END
                ELSE
                    FORWARD     packet
            END
        IF time is timer expiration THEN
            BEGIN
                INSPECT all information in the temporary list to judge about node
                IF ((sum of sent rrep's is high) and (sum of sent data is low) and (sum of  received data is high)) or
                high number of     the voters announce this node as a attacker)
                 THEN
                    BEGIN
                        ADD attacker to quarantine list
                        REMOVE all routes to this node in routing table
                        ALARM this node is a attacker
                    END
            END
        IF packet is an alarm THEN
            BEGIN
                ADD attacker to quarantine list
                REMOVE all routes to this node in routing table
                ALARM this node is an attacker
                FORWARD packet
            END
}
```

Activities of a node in a network show its honesty. To participate in data transfer process, a node must demonstrate its honesty. Early of simulation, all nodes are able to transfer data; therefore they have enough time to show its truth (Though every node can be an effect less one). If a node is the first receiver of a RREP packet, it forwards packets to source and initiates judgment process on about replier. The judgment process is base on opinion of network's nodes about replier. The activities of a node are logged by its neighbors. These neighbors are requested to send their opinion about a node. When a node collects all opinions of neighbors, it decides if the replier is a malicious node. The decision is base on number rules. The following rules used in this paper to judge about honesty of a node in network. This judgment is base on node's activity in network.

Rule1: If a node delivers many data packets to destinations, it is assumed as an honest node.
Rule2: If a node receives many packets but don't sent same data packets, it's possible that the current node is a misbehavior node.
Rule3: When the rule2 is correct about a node, if the current node has sent number RREP packets; therefore surely the current node is misbehavior.
Rule4: When the rule2 is correct about a node, if the current node has not sent any RREP packets; therefore the current node is a failed node.

5. Conclusions

In the following figures AODV is standard AODV with no malicious function; AAODVn is AODV with n malicious nodes. The proposed method is named MAODV.

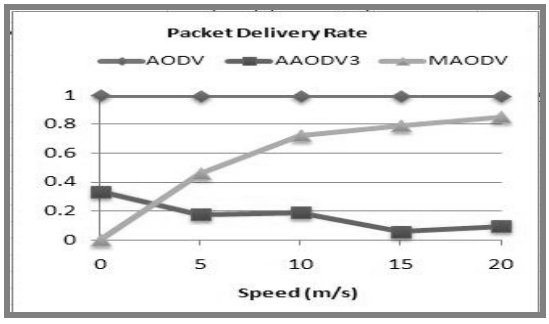

Fig. 1: Packet delivery ratio with increasing speed

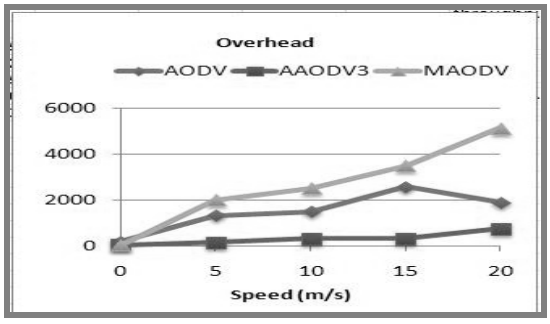

Fig. 2: Overhead with increasing speed

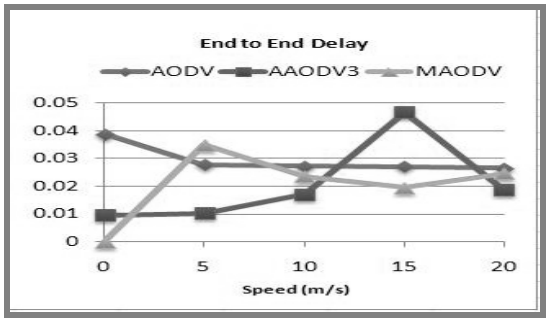

Fig. 3: End to end delay with increasing speed

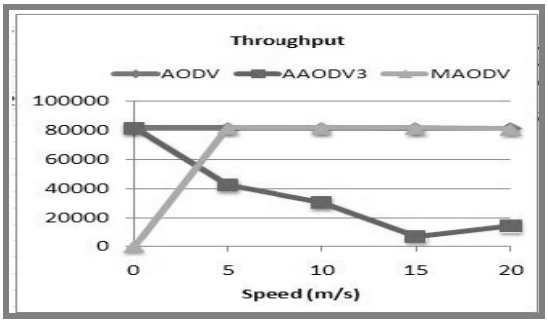

Fig. 4: Throughput with increasing speed

6. Acknowledgements

In this paper the routing security issues of MANETs, are discussed. One type of attack, the black hole, which can easily be deployed against the MANET, is described. The percentage of packets received through the proposed method is better than that in AODV in presence of cooperative black hole attack. The solution is simulated using the Global Mobile Simulator and is found to achieve the required security with minimal delay & overhead. Future works may be concentrated on ways to reduce the delay in the network.

7. References

[1] H. M. Deng, W. Li and Dharma P. Agarwal, Routing Security in Wireless Ad Hoc Networks. University of Cincinnati, *IEEE Communication Magazine*,Vol.40, no.10, October 2002.

[2] 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.

[3] S. Marti, T. J. Giuli, K. Lai, and M. Baker. Mitigating routing misbehavior in mobile ad hoc networks. In mobile Computing and Networking (MOBICOM), pages 255–265, 2000. Available on: citeseer.ist.psu.edu/marti00mitigating.html.

[4] S. Buchegger and J. Y. Le Boudec. A robust reputation system for mobile adhoc networks.Technical Report IC/2003/50, EPFL-DI-ICA, July 2003.

[5] P. Michiardi and R. Molva. Preventing denial of service and selfishness in adhoc networks. *In Working Session on Security in Ad Hoc Networks*. Lausanne, Switzerland, June 2002.

[6] S. Bansal and M. Baker. Observation-based cooperation enforcement in ad hoc networks, July 2003. Available on: http://arxiv.org/pdf/cs.NI/0307012.

[7] B. Hod. Cooperative and Reliable Packet-Forwarding On Top of AODV. www.cs.huji.ac.il/~dolev/pubs/reliable-aodv.pdf, 2005.

[8] H. S, Chen, Z. Z. Ji and M. Z. Hu. A Novel Security Agent Scheme for Aodv Routing Protocol Based on Thread State Transition. *Asian Journal of Information Technology*. 5 (1):54-60, 2006.