An Efficient Routing Protocol for Black Hole Attack prevention using Watch-dog methodology

Mrs. Chaitali Choudhary[1], Mrs. Monika Arya[2], Mr. Kaushal Sinha[3]

Associate Professor(BIT Durg)[1,2,3]
chaitali.choudhary@gmail.com, arya.akshara@gmail.com,
kaushal.sinha16@gmail.com

Abstract

Since an ad hoc network is a collection of infrastructure less & wireless mobile nodes, which act as a host as well as a router. Communication among nodes takes place in hop-to-hop fashion without a centralized administration. AODV is well-known on-demand reactive routing protocols for mobile ad hoc networks. But in existing AODV, there is lack of sufficient security provision against well-known attack "Black hole attack". Black hole nodes are those nasty nodes that show the same opinion to forward packet to destination but do not forward packet intentionally. This Paper presents a watch-dog mechanism for the AODV routing protocol to identify such misbehavior based on promiscuous listening. This method firstly notices a black hole node and then gives a fresh route avoiding this node. In lightly loaded, aggressive situation, our method gives better throughput as compared to a defenseless AODV protocol.

Keywords: *Mobile Ad hoc networks, routing, security, AODV, black hole attack, Prevention.*

1. Introduction

It is well known that there has been fantastic growth in the use of wireless communication over the last few years, from satellite transmission to home personal area networks (PANs-Bluetooth etc.). One side is advantages of wireless to transmit data among users in a common area while remaining mobile another side is the disadvantages of vulnerability. Nevertheless the range of transmitters or their nearness to wireless access points restricts distance between participants. Ad hoc networks moderate this problem by allowing out of range nodes to route data through intermediate nodes.

Ad hoc networks have a wide collection of military, commercial & educational applications and other emergency and disaster situations. Ad hoc networks are ideal in situations where installation of an infrastructure is not possible because the infrastructure is too expensive or too vulnerable, the network is to temporary, or the infrastructure was destroyed. A sensor network, which consists of several thousand small low-powered nodes with sensing capabilities, is one of the advanced applications of MANET's. Clearly, security is a vital issue in such areas.

However, recent wireless research indicates that the wireless MANET presents a large security problem than conventional wired and wireless networks. While most of underlying features make MANET's useful and popular. *First*, all signals go through bandwidth-constrained wireless links in a MANET, which makes it more prone to physical security threats than flexible landline networks. Possible link attacks range from passive eavesdropping to active interference. *Second*, mobile nodes are roaming independently and are able to move in any direction. In this case *denial of service* (DOS) can easily be launched if a malicious node floods the network with fake routing message. The other nodes may unknowingly propagate the messages. *Third, decentralized decision making* in the MANET relies on the cooperative participation of all nodes. The malicious node could simply block or modify the traffic traversing it by refusing cooperation to break the cooperative algorithm. Finally, an attacker could create a new type of DoS attack by forcing a node to replay packets to exhaust its energy.

In general, the wireless MANET is particularly vulnerable due to its elementary feature of open medium, dynamic topology, and absence of central authorities, distributed cooperation, and constrained capability. The existing security mechanisms for wired networks cannot be frankly applied in wireless MANET's. Theoretically there may be several type of attacks are possible but generally in practice Two types of attacks occurs first is *passive attacks* in which a node is driven its selfishness and *active attacks* in which a malicious node has the goal of interrupting normal network operation. Although a malicious node can deploy a variety of DoS attacks [1], [2], we only consider the attacks caused by the failing to perform packet forwarding while participating in routing. This problem is called as the black hole problem. Simulation in [3] shows that if 10%-40% of the nodes fail to forward packets (but participate in the routing protocol), this can cause a throughput degradation of about 16%-32%.

In this paper, we propose a mechanism based on promiscuous listening to detect misbehaving nodes. For a given node, the ratio between the number of dropped data packets and the number of successfully forwarded data packets by the node represents a metric to mark the node as either misbehaving or well behaving. If this ratio exceeds a threshold, the node is marked as misbehaving. If the ratio is below the threshold, the node is marked as well behaving. Upon detecting a misbehaving node, the detecting node tries to avoid the misbehaving node and route the packets along another path. This decision has been taken locally informing neither the sender nor the receiver, that is the misbehaving nodes can be avoided transparently from the sender and the receiver. The remaining of this paper goes as follows. In section2, we investigate some of currently proposed solutions for the routing misbehavior problem in ad hoc networks. Section 3, presents our watch-dog mechanism. Results from simulation using Network Simulator 2 (NS2) are presented in section 4. Section 5 concludes the paper.

2. Related Research Work

In this section, we survey some of the current attempts at solving the problem of routing misbehavior in ad hoc networks.

Sergio Marti [3] introduced Watchdog and Path rater techniques with Dynamic source Routing (DSR) [4] that improve throughput in a MANET by identifying misbehaving nodes that agree to forward packets but never do so. Watchdog is used to identify misbehaving nodes, and Path rater to help routing protocol to avoid these nodes.

The CONFIDANT scheme [5] utilizes the concept of reputation. Each node keeps track of a black-list of misbehaving nodes. Detection of a misbehaving neighbor and/or reception of a warning message from trusted peers against a node would add the misbehaving node to the black-list. A node will not service a request coming from a black-listed node. Also a packet is routed so that to avoid black-listed nodes in its path. Reliance on trust, the ability of malicious nodes to blackmail a legitimate node and the un-scalability of the global distribution of the black-list are some limitations of this scheme.

H.Deng, W.Li and D.P.Agrawal [6] proposed a solution for single black hole problem for ad hoc on-demand distance routing protocol. In this method source node do not send packet to the destination node after receiving the route reply packet, but source node finds one or more route to the intermediate node that replays the RREQ message to check whether the route from the intermediate node to the destination node exits or not. This methods increases the routing overhead and is only solves the problem of single black hole node.

In CORE scheme [7], each node keeps track of reputation values of its neighbors only. The scheme uses more complex reputation systems. A node attains a negative reputation only when its neighbor detects its misbehavior and this negative value is kept local to the detecting neighbor. A misbehaving node will eventually be isolated from the network when all its neighbors detect its misbehavior and thus stop forwarding packets to/from it. With mobility in mind, one would expect this mechanism to fail if the misbehaving node's neighbors continuously change allowing for a new chance for the malicious node to drop more packets. The authors did not present information on the performance of this scheme. It should be noted that all the above schemes fail in the case of multiple colluding nodes. For example, for this scheme if two colluding nodes are neighbors, one of them would behave normally keeping a path through the other node to drop packets.

3. The AODV Watch Dog Algorithm

A. AODV Routing Protocol

There are three types of routing messages in the Ad hoc On-demand Distance Vector (AODV) [8] routing protocol: Route Request (RREQ), Route Reply (RREP) and Route Error (RERR). AODV adopts a proactive scheme to establish routes among nodes. If node A wants to communicate with another node B and it has no active route to it, it issues a RREQ message for node B. The RREQ message contains the address of B, the address of A, a sequence number unique per node per RREQ message, and the number of hops traversed by the RREQ message so far. Node A broadcasts the RREQ message. Upon reception of an RREQ message, a neighboring node C checks to see if it has an active route to B. If it does, it replies to node A with an RREP messages containing the address of node B, the number of hops (as the routing metric) to B and a sequence number for the route. If node C does not have an active route to B, it either creates or updates its route to A using the information it gets from the RREQ message. Node C then broadcasts the RREQ message after incrementing the message's number of traversed hops. If the RREQ message reaches the destination B, B issues an RREP message containing its current sequence number and uni-cast it to the source of the RREQ. Each intermediate node on the path that the RREP message traverses to A creates a route to B if it does not have one, and forwards the RREP message using its route to A. If it has an active route to B, the intermediate node examines the RREP's sequence number and number of hops. A node updates its route if the new route has a larger sequence number or it has the same sequence number but with less number of hops. It then forwards the RREP message. Otherwise, the node drops the RREP message. When node A receives the RREP message, it creates a route to B using the fields in the RREP message.

Each node maintains a routing table containing an entry for each destination it knows about. An AODV routing table entry contains the destination node address, the address of the next hop, the number of hops to reach the destination via this route, and the destination's sequence number associated with this route. AODV has two modes of route maintenance: periodic hello messages and link layer feedback. In the former, nodes exchange hello messages periodically. The absence of a specified number of consecutive hello messages indicates that a node is either down or out of wireless range. A link layer feedback is generated in case of a missing ACK or a missing CTS message after a specified number of retries. Either of these conditions causes a node to either try a local route repair by sending an RREQ message if the node is closer to the destination than the source or to broadcast an RERR message containing the broken node address and, in the case of link layer feedback, the destination's address that the node was trying to reach. Each node receiving this RERR message will bring down its route to the mentioned destination if the route goes through the source of the RERR message and broadcast the RERR message if there are nodes that use this route. For each routing table entry, each node keeps a precursor list of upstream nodes using the route entry. Finally, each routing table entry expires after some specified amount of time if it was not used for this time.

B. Routing Attack(Black Hole Attack)

Black hole attack [6] is an active insider attack; the attacker consumes the intercepted packets without any forwarding

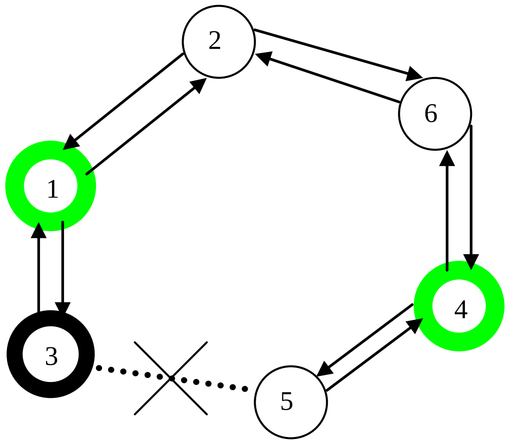

Figure 1: The Black hole problem

Based on original AODV protocol, any intermediate node may respond to the RREQ message if it has fresh enough route, which is checked by the destination sequence number contained in the RREQ packet. In the above figure node 1 is source node where as node 4 is destination node. Source node broadcasts route request packet to find a route to destination node. Here node 3 acts as black hole. Node 3 also sends a route reply packet to the source node. But a route reply from node 3 reaches to source node before any other intermediate node. In this case source node sends the data packet to destination node through node 3. But as the property of black hole node, the very node does not forward further and dropped it. But source node is not aware of it and continues to send packet to the node 3. In this way the data, which have to be reached to the destination fails to reach there? There is no way to find out such kind of attack. These nodes can be in large number in a single MANET, which makes the situation more critical.

C. The Watch-dog Mechanism

In my proposed solution, each node maintains two tables, one is called pending packet table and another one is called node-rating table. In pending packet table, each node keeps track of the packets it sent. It contains a unique packet ID, the address of the next hop to which the packet was forwarded, address of the destination node, and an expiry time after which a still-existing packet in the buffer is considered not forwarder by the next hop.

In node rating table, each node keeps rating of nodes, which are adjacent to it (means nodes are within its communication range). This table contains the node address, a counter of dropped packets observed at this node and a counter of successfully forwarded packets by this node. The fourth field of the above node rating table is calculated by the ratio of data forwarding failure and successfully forwarded packets, if this ratio is greater than a given threshold value then this node misbehave value will be 1(means it is considered as a misbehave node), otherwise it is considered as a valid node. An expired packet in the pending packet table causes the packet drops counter to increment for the next hop associated with the pending packet table entry.

Each node listens to packet that are within its communication range, and only to packets belonging to its domain. Then it verifies each packet and prevent forged packet. If it observes a data packet in its pending packet table, then it removes this data packet from pending packet table after authenticating the packet. If it observes a data packet that exits in its pending packet table with source address different from the forwarding node address, then it increments the packet forwarding value in the node-rating table.

For deciding whether a node is misbehaving or act as a legitimate one, depend on the selection of threshold value. For example if we take a threshold value of 0.2. This means that as long a misbehaving node is forwarding twice packets as it drops it will not be detected. If we take a lower value of threshold then it will increase the percentages of false positives. After detecting a misbehaving node, a node will try to do local repair for all routes passing through this misbehaving node. If local repair process fails, then it will not send any RERR packet upstream in the network. This process tries to prevent a misbehaving node from dropping packets, and also prevent black-mailing of legitimate nodes. To avoid constructing routes, which traverse misbehaving nodes, nodes drop/ignore all RREP messages coming from nodes currently marked as misbehaving. To stop misbehaving node to act actively in a network, the entire packet originating from this node has been dropped as a form of punishment.

4. The Results

We use the NS2 [9], [10] simulator to build a module for our AODV watch-dog mechanism. The module inherits from the AODV module already integrated in NS2. It adds the two tables: the pending packet buffer and the node ratings table. It also uses the support to tap MAC layer packets. The number of nodes simulated is 50 nodes moving in an area of 2000x1000 meters squared with speed between 0 and 10 m/s and using the random waypoint mobility model. Each simulation run is for 1000 seconds. We vary the pause times of the nodes between 0 seconds (high mobility), 100 seconds, 200 seconds, 300 seconds, 400 seconds, 500 seconds (medium mobility), 600 seconds, 700 seconds, 800 seconds, 900 seconds and 1000 seconds (low mobility). We use CBR traffic generators with 16 packets/second and 512 bytes packet size. We use 10 number of CBR traffic sources. Finally, we vary the number of misbehaving nodes between 0, 3 and 5 nodes. We measure the throughput, the total number of received packet per unit time. We also measure the packet delivery ratio, the ratio between the number of packets received by the CBR sink at the final destination and the number of packets originated by the CBR sources.

The throughput and packet delivery ratio (PDR) at different pause times and different number of misbehaving nodes has been measured when the number of CBR sources is 10. For a lightly loaded network, the effect of the watch-dog mechanism is to improve the throughput and packet delivery ratio in the existence of misbehaving nodes, while retaining the approximately same throughput and packet delivery ratio as the defenseless AODV in the case of 0 misbehaving nodes.

5. Conclusion

The mobile Ad hoc Network is an emerging research area with practical application, but they are vulnerable in many settings to nodes that misbehave when routing packets. In general, routing security in wireless networks appears to be a nontrivial problem that cannot easily be solved. It is impossible to find a general idea that can work efficiently against all kinds of attack, since every attack has its own distinct characteristics.

In this paper we analyze extension to AODV to mitigate the effect of routing misbehavior in ad hoc networks- the watch-dog mechanism. We show that this technique increases throughput by 16% to 20% and packet delivery ratio by 8% to 20% in the presence of 8% misbehaving nodes in a network with moderate mobility.

6. REFERENCES

[1] Jin Taek Kim, Jeong-Ho Kho, Chang-Young Lee, Do-Won Lee, Cheol-Soo Bang, Geuk Lee, “A Safe AODV (Ad Hoc on-Demand Distance Vector) Security Routing Protocol”, Proceedings of the 2008 International Conference on Convergence and Hybrid Information Technology - Pages 115-118.

[2] Y.C.Hu, D.B.Johnson and A .Perrig, “Sead: Secure efficient distance vector routing in mobile wireless ad hoc networks”, in fourth IEEE Workshop on Mobile Computing System and Applications, pp 3-13, june 2002.

[3] S. Marti, T. J. Giuli, K. Lai, and M. Baker, “Mitigating routing misbehavior in mobile ad hoc networks,” in Mobile Computing and Networking, pp. 255–265, 2000.

[4] David B.Johnson and Dravid A. Maltz. Dynamic Source routing in ad hoc wireless networks. Technical report, Carneigie Mellon University, 1996.

[5] S.Buchegger and J.Y.L.Boudec. Performance analysis of CONFIDANT protocol: Cooperation of nodes, In Preceeding of IEEE workshop on MobiHOC, Lausanne, June2002

[6] Hongmei Deng, Wei Li, and Dharma P. Agarwal, “Routing Security in Wireless Ad Hoc Networks,” University of Cincinnati, IEEE Communication magazine, October 2002.

[7] P.Michiardi and R.Molva, “Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks,” in Proceedings of Sixth IFIP conference on security communications, and multimedia (CMS 2002), Portoroz, Slovenia, 2002.

[8] C.E. Perkins, S.R.Das, and E.Royer, “Ad-hoc Demand Distance vector (AODV)”, Mobile Ad Hoc Networking Working Group, IETF Internet Draft, http:/www.ietf.org/internet-draft/draft-ietf-manet-aodv-05.txt March 2000.

[9] The Network Simulator – ns-2 http://www.evanjones.ca/ns2

[10]www.esnips.com/doc/2fe839f5-6e38-4c0d-92b1-33ff81a2066a/ns2-manual