A Detection and Prevention Algorithm for Single and Cooperative Black hole Attacks in AODV MANETs

Saeed K. Saeed **Noureldien A. Noureldien**

Department of Computer Science

University of Science and Technology

Omdurman, Sudan

e-mail: saeed_kl@hotmail.com **e-mail: noureldien@hotmail.com**

***Abstract*— A mobile ad-hoc network (MANET) is a new generation of wireless networks that is used in many applications. MANETs have much vulnerability such as mobility, unsecure boundaries, lack of central management, that have been exploited by attackers to launch different types of attacks. One well known attack is the Black Hole Attack, which absorbs packets before reaching its destination. As one of the vital MANET attacks, the black hole attack has been studied extensively, and many detection and prevention techniques have been proposed. In this paper, a new detection and prevention algorithm for single and cooperative black hole attacks in MANET that employ Adhoc On-demand Distance Vector (AODV) is proposed. The developed algorithm benefits from the two previously proposed detection techniques; the sequence number scheme, and cooperative black hole attack scheme in AODV MANETs. The simulation results show that the proposed algorithm works and improves the security of AODV MANTETs against black hole attack.**

Keywords- MANET attacks; Black hole attack; Black hole attack detection; single Black hole attack; Cooperative black hole attack.

I. INTRODUCTION

MANET's are composed of equivalent nodes that communicate over wireless links without any central control and can move randomly and have the capability to self-manage without any need to predefined infrastructure.

The nodes can cooperate to communicate with each other via sending data packets from source to destination through intermediate node(s). Packet routing is done using a routing protocol such as AODV, which is the most popular routing protocol.

MANET's are facing great security challenges due to the vulnerabilities initiated from; the wireless transmission media, the high dynamic topology of nodes, the limited nodes resources, and the lack of central management.

These attacks can prevent the transmission or reduce the performance of the network. One of these attacks is the Black Hole Attack in which one or more malicious node drops all the data packets in the network. As a result the data packets do not reach the destination node and the data will be lost.

To defend a black hole attack there are a lot of techniques that have been proposed either to detect or to prevent black hole attack.

In this paper, we discuss some of the most common current detection techniques with a special focus on the sequence number scheme and the detection of cooperative black hole attack scheme, and then a new algorithm that is capable for detection and prevention of single and cooperative black hole attack is proposed.

The rest of this paper is organized as follows: Section 2 reviews the current black hole attack detection techniques. Section 3 is dedicated to the proposed new algorithm. Section 4 shows the simulation results of the proposed algorithm. Section 5 represents conclusion and future work.

II. CURRENT DETECTION TECHNIQUES

There are many secure routing protocols, and schemes, which can detect the black hole attack; this section discusses some of these techniques.

A. Neighborhood-based and Routing Recovery Scheme

Guan et al. [1] designed a method to deal with the black hole attack based on the neighbor set information; this method consists of two parts: detection and response. The detection procedure has two major steps; in the first one each node collects neighbor set information. The second step determines whether if there is a black hole attack or not. In response procedure, the source node sends a control packet called Modify Route Entry (MRE) to the Destination node in

 ISBN: 978-1-61208-427-5

order to form a correct path by modifying the routing entries of all of the intermediate nodes from source to destination.

B. Detection Based on Path Based Method

A path based scheme is proposed in [2]. In this method, a node is used to monitor the next hop nodes in the current route path. First, the monitoring node calculates the digest value for every packet that wants to be sent, and add this digest into a buffer called FwdPktBuffer. After sending the packet the node overhears, when the next hop forwards this packet that is overheard, the digest value will be released from the FwdPktBuffer. Finally, every node calculates the forwarding rate of its next hop and compares it with a threshold. If it is lower than the threshold, that node is marked as malicious.

This technique does not increase the overhead because it does not send additional control packets and also it does not require encryption of the control packets to avoid the security primitive attacks.

C. Detection Based on Learning Automata

Taqi and Abdorasoul [3] proposed a black hole attack detection mechanism that uses a machine learning automata is proposed. The machine operates in a random environment and tries to adapt itself to this environment according to feedback received from this environment. The machine has a finite set of potential actions, where each action has a specific probability. This probability is updated according to feedbacks. The feedbacks may reward or punishment. If the machine performs an action in the correct manner it will get rewarded, otherwise it will get punished. Action probabilities affect the selecting of the future action. The main objective of this is that automata should learn how to select the best action from the finite set of actions. Therefore, the best action is the one that maximizes the probability of getting reward from the environment.

Each node has a list of its direct neighbors and gives a value of trust and a confidence degree to each one of those neighbors. The initial value of trust is 1. This means each node in the network is trust in all of its neighbors. So any node has normal behavior in the network. The value of the trust will be updated after receiving feedback from the network. Each node dedicates a learning automaton to compute the degree of confidence of each neighbor. According to this degree, the node will decide if it will send packets through that node or not.

D. Detection Using Fuzzy Logic

Jagpreet [4] have proposed a system that isolates the malicious node from the network. Every node in the network decides if the behavior of its neighbors was malicious or not. If a node decides a neighbor is malicious it will broadcast an alarm packet in the network with the IP address of the malicious node which is not allowed to participate in any future communication.

The fuzzy system integrates with AODV routing protocol. It consists of four components: Fuzzy Parameter Extraction, Fuzzy Computation, Fuzzy Verification Module and Alarm Packet Generation Module. The Fuzzy Parameter Extraction module extracts the required analysis parameters from the network traffic. Then pass these parameters to a fuzzy computation module, which in turn applies some of fuzzy rules and membership functions to calculate the fidelity level of the node. The verification module determines the behavior of the node by comparing the value of fidelity level with the threshold if it was less than the threshold level in fuzzy it will broadcast an alarm packet with the IP address of this malicious node to the whole of the network. This system beside the detection of the black hole, it also isolates it from the network.

E. Detection Using Anomaly Detection

Fantahun, and. Zhao [5] proposed a host-based Intrusion Detection System (IDS) scheme. The scheme assumes that, every activity of a system can be monitored and anomaly activities of an intruder can be identified from normal activities. Hence, by identifying anomalous activities of an adversary, it is possible to detect a possible intrusion and isolate the adversary. To do so an anomaly detection system needs to be provided with a pre-collected set of anomalous activities, called audit data.

Once the audit data is collected and given to the system, the system will be able to compare every activity of a host with the audit data on the fly. If any activity of a host resembles the activities listed in the audit data, the anomaly detection system isolates the particular node by forbidding further interaction. It does not trust on peer nodes.

F. Enhance Black-Hole AODV (EBAODV)

Rachh et al. [6] proposed an Enhance Blackhole AODV solution (EBAODV). In this solution, what is called leader nodes are created first, these nodes are responsible for detection of malicious nodes.

After sending the first Routing Request message (RREQ) a timer is started. If a RREP is received before the timer is expired, then one stale packet will be send to the destination. To ensure that the stale packet is received by the destination, the source node must received acknowledgement (ACK) from the destination. When the source node receives the acknowledgement it sends the original packet.

When the source node has not received any ACK, it means packets are dropped. If the number of dropped packets is more than a threshold, then the leader nodes will send block messages that contains the id of the blackhole node to all neighbors and the source node must start again a new RREQ to discover another route.

G. Feedback Solution

Singh [7] proposed a feedback technique which examines the malicious nodes from the amount of packets sent by this

 ISBN: 978-1-61208-427-5

node, this amount in the most of the cases equal zero. After detecting the malicious nodes, the method was adopted to avoid the recipients of the packets that are coming from these detected nodes. The packets coming to the neighbors of the black hole nodes are propagated back to the source, and the source node has to follow another route to the destination. This method decrease packet loss in the network comparatively. But this method cannot detect the collaborative black holes.

H. Detection Technique for Single Black hole Attack Using Sequence Number

Singh and Manpreet [8] have proposed a method to find the secure route and prevent the black hole nodes (malicious nodes) in MANETs. This is done by checking whether there is a large difference between the sequence number of the source node and the intermediate node who has sent back the first RREP or not.

The detection method builds a table to store RREPs messages received in response to source RREQ. The method compares the sequence number in RREPs with that of the resource node, if there is a significant difference, the method considers that RREP is originated from a malicious node and remove it from the table. The RREP with a reasonable difference is considered to be from a legitimate node and the route defined by that RREP is used by the source node.

The method was implemented by adding a new function to AODV protocol called Pre_ReceiveReply (Packet P) and added a new table C_RREP_T, a timer M_WAIT_T and a variable M_Node to the data structures in the basic AODV. The time M_WAIT_T is initialized to be the half value of RREP_WAIT_TIME, i.e., the time for which the source node waits for RREP control messages before regenerating RREQ.

The source node analyses all the stored RREPs from C_RREP_T table and discards the RREPs having very high destination sequence number. Then the source node selects a reply having highest destination sequence number of the C_RREP_T table.

The major drawback of this method is that; when the source node received RREPs from two or more collaborated malicious nodes, then the function will fail to get a legitimate RREP since the collaborative attackers keep sending similar sequence numbers. So this technique fails to detect cooperative black hole nodes.

I. Detection Technique of Cooperative Black Hole Attack

Munjal et al. [9] proposed a method to detect multiple black hole nodes that working collaboratively as a group to launch a cooperative black hole attack. The technique maintains a Routing Information Table (RIT) at each node in addition to the Routing Table of the AODV protocol. The method considers a node that has an entry in the RIT table as a trusted node. RIT table contains the fields {Node ID, From, Through}, where From Node stands for source nodes that broadcast RREQs, and Through Node stands for nodes that forward data packets.

The technique suggests that each source node builds a table for trusted nodes that are exchanged RREQ or data packets with the source node.

The source node starts to send RREQ and then wait for destination replies, all intermediate nodes update their RITs by adding an entry referred to the destination. Also the source node updates the RIT as well. When a node receives a RREP message, it checks its Trust table, if the sending node was recorded as a trustee the RREP is accepted, otherwise the source node makes a further request (FRREQ) to its neighbors.

This technique leads to a delay as a result of trust table checking and exchanging of further requests and further replies.

J. BDSR Scheme to Avoid Black Hole Attack

Po-Chun et al. [10] designed a novel solution named Bait DSR (BDSR) or Fake RREQ scheme to prevent the collaborative black hole attacks. The proposed mechanism is composed of proactive and reactive method to form a hybrid routing protocol, and the major essence is the DSR on-demand routing. In this solution in the beginning of routing phase, the source node sends bait RREQ packet before starting route discovery.

The target address of bait RREQ is random and non-existent destination. The malicious nodes are easily expelled from the initial phase, because the bait RREQ is able to attract the forged RREP from the black hole node. In author's mechanism, the generator of RREP is recorded in the RREP's additional field. Therefore the source node can recognize the location of an attacker from the reply location of the RREP. All of the response set by the adversaries should be dropped. After the initial phase, the authors employ the original DSR route discovery procedure. If the data delivery rate is lower than the pre-defined threshold value, the boot procedure will be triggered again to examine the uncertainly suspicious nodes.

K. Detection Using Watchdog

Marti et al. [11] proposed a method that uses the node promiscuous mode. This method allows a node to intercept and read each network packet that arrives in its entirety. Promiscuous mode means that if a node A is within the range of node B, it can overhear communication to and from B even if those communications do not directly involve A.

The watchdog works as follows, node A listens to the transmission of B to make sure that B forwards to C. If the packet overheard from B matches that stored in the buffer, it means that B really forwards to the next hop, and it then removes the packet from the buffer. However, if there's no matched packet after a certain time, the watchdog increments the failures counter for node B. If this counter exceeds the threshold, A concludes that B is misbehaving and reports to the source node S. The watchdog is implemented by

 ISBN: 978-1-61208-427-5

maintaining a buffer of recently sent packets and comparing each overheard packet with the packet in the buffer to see if there is a match. If so, the packet in the buffer is removed and forgotten by the watchdog, since it has been forwarded on. If a packet has remained in the buffer for longer than a certain timeout, the watchdog increments a failure tally for the node responsible for the forwarding of the packet. If the tally exceeds a certain threshold, it determines that the node is misbehaving and sends a message to the source notifying it of the misbehaving node. The watchdog technique has advantages and weaknesses.

A Watchdog has the advantage that it can detect misbehavior at the forwarding level and not just the link level. Watchdog's weaknesses are that it might not detect a misbehaving node in the presence of ambiguous collisions, receiver collisions, limited transmission power and false misbehavior alarm.

L. Detection Based on Collaborative Bayesian Watchdogs

Authors in [12], have proposed a detection technique based on the message passing mechanism between a group of collaborating Bayesian watchdogs by allowing to every watchdog to publishing both self and neighbor reputations. The standard watchdog monitors packets have been transmitted/ received by its neighbors, counts the packets that need for retransmission, and calculates the trust level for any one of the neighbors as the ratio of packets retransmitted to packets that need to retransmission. If a node retransmits all the packets that it should have retransmitted, it will be given the value 1 as a trust level. If there is a node has a trust level lower than the tolerance threshold, the watchdog will consider this node as a black hole.

III. A PROPOSED NEW DETECTION AND PREVENTION ALGORITHM FOR BLACK HOLE ATTACKS IN AODV MANETS

Our proposed black hole detection and prevention technique is based on the sequence number scheme [8] and cooperative black hole attack scheme in AODV MANETs [9].

The Sequence Number Scheme as explained in section II.H, suffers from collaborative black hole attack; whiles the proposed technique for detecting cooperative black hole attacks, discussed in section II.*I* causes a high overhead over the original AODV.

Our proposed detection technique aimed to take advantages of the two schemes and to avoid their drawbacks, to be able to detect single and cooperative attackers without significant delay over normal AODV.

The algorithm donates a table for each node to store received RREPs after the node sends a RREQ, besides a table for trusted nodes. Then after, the source node scans the RREPs table looking for a trusted node that is registered in the trusted nodes table. If such a node is found, then the route defined by that RREP is used.

If the scan fails to find a trusted node, then the sequence number scheme applies to RREPs table entries. Entries with very high sequence numbers will be deleted. If a RREP with an adequate sequence number is found, then the RREP source node is considered a trusted node and added to trusted table and the route defined is used.

Thus, the proposed algorithm defines the following pre-setting:

- At each node a W-TIME timer was set.
- At each node an RREP_TABLE was built to store received RREPs during W-Time.
- At each node a TRUST-TABLE was built to store trusted nodes.

Then, the algorithm works as follows:

1) The source node sends it's RREQ and wait for W-TIME, storing all received RREPs in RREP_TABLE.

2) IF a RREP from a node in the TRUST_TABLE is found in RREP_TABLE, use that RREP route, then call normal AODV and terminates;

3) Otherwise While RREP_TABLE is not empty do

a) If a RREP have a very high sequence number, then delete the RREP route from RREP_TABLE // applying sequence number scheme

b) IF a RREP have a suitable sequence number, then add that RREP node for the TRUST_TABLE, use that RREP route, then call normal AODV and terminates;

4) IF RREP_TABLE is empty go to step 1

This algorithm applies both the Sequence Number Scheme in step 3.a, and the Trust Table technique used in the detecting cooperative black hole attack method in preprocessing stage and in steps 2 and 3.b.
Step 3.a and Step 5, ensures the avoidance of cooperative black hole attack.

The developed algorithm was implemented by adding the TRUST_TABLE, RREP_TABLE, a timer W_TIME and a Boolean variable NOT_ROUTE to the data structures in the basic AODV.

To implement the algorithm a new function to AODV protocol called Pre_ReceiveReply (Packet P) is added in aodv.cc before ReceiveReply (Packet P).

The pseudo code of the new Pre_ReceiveReply (Packet P) function is shown in Figure 1.

 ISBN: 978-1-61208-427-5

```
Pre_ReceiveReply (Packet P)
  {
    While (NOT_ROUTE = true) do
     {
        Send RREQ;
        While (W_TIME)
                Store all received RREPs in
                 RREP_TABLE;
       i=0;
       While ( RREP_TABLE is not empty)
         If (RREP_TABLE[i] is in TRUST_TABLE
         {
            NOT_ROUTE = False;
             Use that RREP route;
             Call normal AODV;
             Exit;
           }
          Else
           i++;
       }/**while
      i=0;
       While (RREP_TABLE is not empty)
       {
           If ( RREP_TABLE[i].Dest_Seq_no >>>
           Src_Seq_No) then
                 {
                   delete(RREP_TABLE[i]);
                   i++;
                 }
           else
            {
               Add RREP_TABLE[i]node to the
                        TRUST_TABLE,
              NOT_ROUTE = False
               use that RREP route,
               call normal AODV;
               exit;
             }
        }//while
    }
}
```

Figure 1. Proposed Algorithm

The Pre_ReceiveReply (Packet P) function implements our proposed detection algorithm.

IV. SIMULATION AND RESULTS

To test the performance of the developed algorithm, three scenarios are simulated. The first scenario simulates the network under the normal AODV (called Normal-AODV), the second scenario simulates the network under both single and cooperative black hole attacks (called Blackhole-AODV), and the last scenario simulates the network that implements proposed algorithm (called Modified-AODV-black hole).

The Network Simulator (NS2.35) was used as a network simulation tool. The Tool Command Language (TCL) was used to implement the simulation with 25 mobile nodes. All simulation time is set to 100 Sec. Table (I) shows the simulation environment that used in all experiments scenarios.

TABLE 1: THE SIMULATION ENVIRONMENT

Simulator	NS-2 v. 2.35
Transmission Protocol	UDP
CBR Packet Payload (data)	1000 bytes
Channel bit rate (data)	20 Mbps
Number of nodes	25 nods
Routing Protocol	AODV
Traffic Model	CBR
Terrain	1186 x 584 meter
Malicious nodes	3 nodes
MAC type	802.11
Simulation Time	100 Sec

To evaluate the performance of the developed algorithm, packet delivery ratio and throughput are used as measurement criteria. To represent and illustrate results the Xgraph tool is used.

Figures 2 and 3 show the simulation results. Where the green color represents the Normal-AODV, the red color represents the Blackhole-AODV, and the blue color represents the Modified-AODV-black hole.

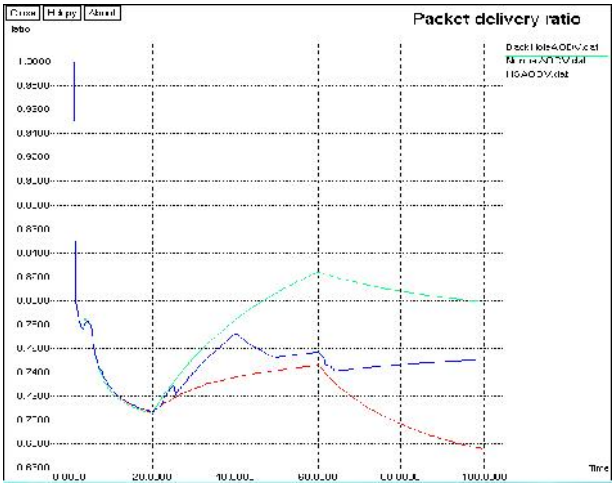

Figure 2. Throughput

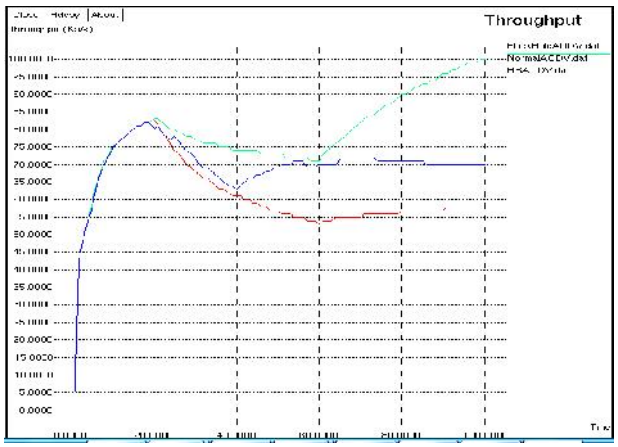

Figure 3. Packet Delivery Ratio

A. Discussion

From Figure 2, the throughput of Modified-AODV-black hole started normally, then the performance decline due to the start of the developed algorithm the waiting period in which it receives and stores RREPs. The algorithm then executes making the performance moderate between the Normal-AODV and the Black Hole-AODV.

Figure 3 represents the packet delivery ratio (PDR) versus Time. The performance is similar to throughput. The PDR in the proposed algorithm started normally as well, then decreased because the source node might have just one trusted node or no trusted nodes in the TRUST_TABLE. Then, the Modified-AODV-blackhole performance moderates between the Normal-AODV and the Blackhole-AODV. This means that, the proposed algorithm enhance and improve the performance of the network under black hole attack.

V. Conclusion and Future Work

In this paper, a new detection and prevention algorithm to single and collaborative black hole attack was developed and tested. The simulation results show that the developed solution improves the security and resistance of MANETs to single and collaborative black hole attack.

Currently, we are working on comparing the performance of the developed algorithm with the previously proposed techniques, the sequence number and cooperative black hole attack schemes.

References

[1] S. Guan, J. Chen, and U. Pooch, “Detecting Black-hole Attack in Mobile Ad Hoc Networks,” Proc. the 5th European Conference on Personal Mobile Communicationse,, Apr. 2003, pp. 490-495, doi: 10.1049/cp:20030303.

[2] J. CAI, Y. Ping, C. Jialin, W. Zhiyang, and L. Ning, “An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network,” Proc. IEEE 24th International Conference on Advanced Information Networking and Applications, 2010, pp. 775-780, doiI:10.1109/AINA.2010. 143.

[3] M. Taqi, and G. Abdorasoul, “Detecting Black Hole Attack in Wireless Ad Hoc Networks Based On Learning Automata,” Proc. the 6th International Conference on Computer Sciences and Convergence Information Technology (ICCIT), Nov. 2011 , pp 514 – 519.

[4] K. Jagpreet, “Fuzzy Logic based Intrusion Detection System against Blackhole Attack on AODV MANET,” International Journal of Computer Application (IJCA), Special Issue on Network Security and Cryptography (NSC), 2011. pp. 28-35, doi::10.5120/4331-024.

[5] Y. Fantahun, and X. Zhao, “Preventing Black hole Attack in Mobile Ad-hoc Networks using Anomaly Detection,” Proc. International Conference on Future Computer and Communication, Wuhan, May 2010, pp. 672-676, doi: 10.1109/ICFCC.2010.5497455.

[6] A. Rachh, V. Yatin, and R. Tejas, "A Novel Approach for Detection of Blackhole Attacks," IOSR Journal of Computer Engineering (IOSR-JCE), Mar-Apr. 2014 . vol 16, issue 2, pp. 69-74.

[7] H. Singh, "An approach for detection and removal of Black hole in MANETS," International Journal of Researh in IT& Management (IJRIM), June 2011. Vol 1, issue 2, pp. 78-87.

[8] H. Singh and S. Manpreet,"Securing MANETs Routing Protocol under Black Hole Attack," International Journal of Innovative Research in Computer and Communication Engineering, June 2013 . vol 1, issue 4, pp. 808- 813.

[9] K. Munjal, V. Shilpa, B. Aditya, "Cooperative Black Hole Node Detection by Modifying AODV," International Journal of Management, IT and Engineering (IJMIE), August 2012. Vol 2, issue 8, pp. 484-501.

[10] T. Po-Chun, J. Chang, Y. Lin, H. Chao, and J. Chen, “Developing a BDSR Scheme to Avoid Black Hole Attack Based on Proactive and Reactive Architecture in MANETs,” Proc. the 13th international conference on Advanced Communication Technology, Seoul, 2011, pp. 775-780.

[11] S. Marti, T. Giuli, K. Lai, and M. Baker, “Mitigating routing misbehavior in mobile ad hoc networks,” Proc. the 6th International Conference on Mobile Computing and Networking (MobiCom’00), 2000, pp. 255-265, doi:10.115/ 345910.345955.

[12] M. Serrat-Olmos, H. Enrique, C. Juan-Carlos, T. Carlos, and M. Pietro, “Accurate Detection of Black Holes in MANETs using Collaborative Bayesian Watchdogs,” Proc. Wireless Days (WD), IFIP International Conference, 2012, pp. 1-6, doi:10.1109/WD.2012.6402811.

 ISBN: 978-1-61208-427-5