ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 7, July 2014

Secure Routing In Mobile Adhoc Networks (MANET)

Muralidharan.R [1] , Sampathkumar.J [2], Palanisamy.P.N [3]

[1]Student, Department of ECE, Mahendra college of Engineering, Salem – 636106, India.

[2] AP, Department of ECE, Mahendra college of Engineering, Salem – 636106, India.

[3]AP, Department of ECE, Mahendra college of Engineering, Salem – 636106, India.

ABSTRACT: A black hole attack on a MANET refers to an attack by a malicious node, which forcibly acquires the route from a source to a destination by the falsification of sequence number and hop count of the routing message. A selective black hole is a node that can optionally and alternately perform a black hole attack or perform as a normal node. Several IDS (intrusion detection system) nodes are deployed in MANETs in order to detect and prevent selective black hole attacks. The IDS nodes must be set inorder to perform the so-called ABM (Anti-Blackhole Mechanism) function, which is mainly used to estimate a suspicious value of a node according to the abnormal difference between the routing messages transmitted from the node. When a suspicious value exceeds a threshold, an IDS nearby will broadcast a block message, informing all nodes on the network, asking them to cooperatively isolate the malicious node.

KEYWORDS: Mobile ad hoc networks, Intrusion detection system, Black hole attack

I. INTRODUCTION

In a wireless mobile ad hoc network (MANET), there are no basic network devices, such as routers or access points; data transfer among nodes is realized by means of multiple hops, and rather than just serving as a single terminal, every mobile node acts as a router to establish a route. When a source node intends to transfer data to a destination node, packets are transferred through the intermediate nodes, thus, searching for and quickly establishing a route from a source to a destination node is an important issue for MANETs. The currently available routing protocols are mainly categorized into proactive routing protocols and reactive routing protocols. In a proactive routing protocol, every node proactively searches for routes to other nodes, and periodically exchanges routing messages, in order to ensure that the information in the routing table is up-to-date and correct, such as DSDV (Destination Sequence Distance Vector) and OLSR (Optimized Link State Routing Protocol). Each node in a MANET is limited to a certain power and bandwidth, thus, continuous transmission of routing messages would lead to congestion of the network. In a reactive routing protocol, a route is searched and established only when two nodes intend to transfer data; and therefore, it is also called an on-demand routing protocol, such as AODV (Ad hoc On-Demand Distance Vector) or DSR (Dynamic Source Routing). A source node generally broadcasts a route request message to the entire network by means of flooding, in order to search for and establish a route to the destination node.

MANETs are generally used for communication during natural disasters, on the battlefield, and business conferences, which illustrate the importance of guaranteed safety of data transfer between two nodes, thus, more secure routing protocols have been recently proposed. Most secure routing protocols are designed to prevent hazards to safety properties, such as: (1) identity authentication and non-repudiation; (2) availability of resources; (3) Integrality; and (4) confidentiality and privacy. By forging a routing message, a black hole attack is intended to scramble the route, and then, further eavesdrop or drop the packets, posing a possible threat to safety properties (2), (3), and (4). Due to its easy-to-operate behaviour, a black hole attack is common in MANETs, making it very important to efficiently prevent black hole attacks.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 7, July 2014

II. RELATED WORK

Black hole attacks have serious impact on routing algorithms, which uses sequence numbers to determine whether a message is fresh, and selects the shortest route of minimum hops, such as AODV or DSR. Dokurer et al., revised the AODV routing protocol to reduce opportunities for a black hole node to acquire a route, namely, the source node drops the first returned RREP, or the first two returned RREPs, but selects any subsequent RREP packets, because RREP replies by a black hole node are generally the first or the second one to arrive at the source node, thus, method is very useful to prevent a black hole node being located nearby a source node.

In this paper, IDS nodes are deployed in MANETs to identify and isolate black hole nodes. An IDS node observes every node's number of broadcasted RREQs, and the number of forwarding RREQs in AODV, in order to judge if any malicious nodes are within its transmission range. Once a black hole node is identified, the IDS node will send a block message through the MANET to isolate the malicious node.

Tamilselvan et al. [4] also proposed a revised AODV routing protocol, called PCBHA (Prevention of a Co-operative Black Hole Attack), in order to prevent cooperative black holes. First, it provides each legal user with a default fidelity level, and after broadcasting a RREQ, a source node waits to receive returned RREPs from the neighboring nodes, and then selects a neighboring node of a higher fidelity level, which exceeds the threshold value, for passing the data packets. The destination node will return an ACK message after receiving data packets, and the source node may add 1 to the fidelity level of the neighboring node, upon receipt of an ACK response. If no ACK response is received, 1 is subtracted from the fidelity level, which indicates a possible black hole node on this route, and data packets are dropped before reaching the destination node.

Kurosawa et al. [5] proposed a dynamic learning method to detect a black hole node. It is required to observe if the characteristic change of a node exceeds the threshold within a period of time. If yes, this node is judged as a black hole node, otherwise, the data of the latest observation is added into dataset for dynamic updating purposes. The characteristics observed in [5] include, the number of sent RREQs, the number of received RREPs, and the mean destination sequence number of the observed RREQs and RREPs. However, [5] it does not involve a detection mode, such as revising the AODV protocol or deploying IDS nodes, thus, it does not isolate black hole nodes.

Luo et al. [6] added an authentication mechanism into the AODV routing protocol, by combining hash functions, message authentication codes (MAC), and a pseudo random function (PRF) to prevent black hole attacks. Djahel et al. [7] proposed a routing algorithm based on OLSR (Optimized Link State Routing) [2] to prevent the attack of cooperative black holes, by adding two control packets, namely 3 hop_ACK and HELLO_rep.

III. PROPOSED ALGORITHM

A. *Design Considerations:*

In this approach, several IDS (intrusion detection system) nodes are deployed in MANETs in order to detect and prevent selective black hole attacks. The IDS nodes must be set in sniff mode in order to perform the so-called ABM (Anti-Blackhole Mechanism) function. All IDS nodes in this study execute a mechanism, called an ABM (Anti-Blackhole Mechanism), which is mainly used to estimate the suspicious value of a node according to the amount of abnormal difference between RREQs and RREPs transmitted from the node. When a suspicious value exceeds the predefined threshold, a block message is broadcast by a nearby IDS, giving notice to all nodes on the network to cooperatively isolate the malicious node. The Block message contains the issuing IDS, the identified black hole node. Upon receipt of a Block message issued by IDS, normal nodes will place the malicious node on their blacklists, thus, the AODV routing protocol for normal nodes must be slightly revised.

- Assumptions
- Two neighboring IDS nodes are located within each other's transmission range in order to forward Block messages to each other.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 7, July 2014

- An authentication mechanism exists in MANETs, wherein, a node ID cannot be forged, and a block message, sent by an IDS node, cannot be modified or counterfeited.
- Every IDS is set in promiscuous mode in order to sniff all routing packets within its transmission range.
- There are three types of nodes in the network topology of this approach, which separately perform three algorithms, as follows.
- Malicious node: selectively executes the BAODV (Black hole AODV) routing algorithm for black hole attacks.
- Normal node: executes a slightly revised AODV, called MAODV (Modified AODV), to conduct normal routing, and also blocks the malicious nodes in collaboration with IDS nodes.
- IDS node: executes ABM (Anti-Blackhole Mechanism) to detect black hole nodes, and issues a Block message, if necessary.
- The procedure for IDS nodes namely, ABM (Anti-Black hole Mechanism), is described in two parts.
- When an IDS sniffs an RREQ: The RQ table is inquired at both ends of the route, as well as the Source sequence number, i.e., (Src node, Dest node, Src_seq), in the RREQ. In case of an absence of this entry, an entry is added; the two ends of the route, Src_seq, hop count, and the ID of the RREQ broadcasting node are copied into the new entry. In cases of the presence of this entry, the ID of the broadcasting node is added into the ‘‘Broadcasting nodes” field, and then, judgment to determine whether the hop count in RREQ is greater than Maximal hop count of this entry. If yes, this field value is replaced with the RREQ’s hop count.
- When an IDS sniffs an RREP: Checks if RREP forwarding node is the destination node, if yes, no processing is required; if not, then (Src node, Dest node) in RREP are indexed to inquire of the RQ table in the following three cases.
- Case1: If there is no corresponding entry in the RQ table, it indicates the RREP forwarding node is not within the transmission range of the IDS that previously broadcasted the corresponding RREQ. The algorithm stops without subsequent processing.
- Case2: If there is corresponding entry in the RQ table, and the ‘‘Broadcasting nodes” field contains the ID of a RREP forwarding node; it indicates that this is a reasonable reply to RREQ.
- Case3: If there is a corresponding entry in the RQ table, and the “Broadcasting nodes” field does not contain the ID of the RREP forwarding node it indicates this is not a reasonable RREP reply. Thus, it must inquire about the SN table by this RREP forwarding node, by searching the ”Node ID” With two possible case results as below.
- Case3.1 This entry exists in the SN table – checks if the status is active. If active (already blocked), it stops with no further handling. Otherwise, the suspicious value of the entry in the SN table is added with 1, and then checks if this value reaches the threshold. If yes, the status is set as active and a Block message is broadcasted.
- Case3.2 This entry does not exist in the SN table – a new entry is added in SN table, and the ID of the RREP forwarding node is entered, the suspicious value is set as 1, and the status is set as inactive.

When the suspicious value of a node is found to have reached the threshold, the detected IDS will broadcast a Block message to notify other normal nodes in its transmission range, in order to update their Block tables. Simultaneously, nearby IDSs can hear this Block message, according to Assumption 1. When an IDS node hears a Block message, the following steps are taken. Check if ‘‘Node ID” field of SN table has the malicious node ID stored in the Block message. If there is such a node and the status is inactive (a fresh black hole node), change the status to active, and re-broadcast this Block message to notify the normal nodes and nearby IDSs within the transmission range.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 7, July 2014

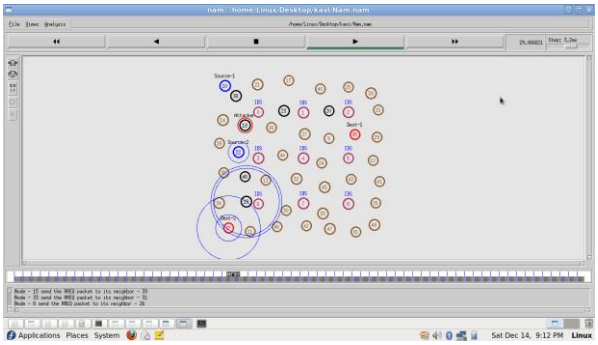

Fig.1. IDS to monitor the routing packet

When there is such node, and the status is active (a known black hole node), it is dropped without handling, and when there is no such node, create a new entry, store the identified node in the SN table, and set the Suspicious value as the threshold value and the Status as active, and then, re-broadcast this Block Message.

B. *Description of the Proposed Algorithm:*

Network Simulator (NS2) is a discrete event driven simulator developed at UC Berkeley. It is part of the VINT project. The goal of NS2 is to support networking research and education. It is suitable for designing new protocols, comparing different protocols and traffic evaluations. NS2 is developed as a collaborative environment. It is distributed freely and open source. A large amount of institutes and people in development and research use, maintain and develop NS2.

This increases the confidence in it. Versions are available for FreeBSD, Linux, Solaris, Windows and Mac OS X.Ns2 is used to validate the detection and isolation efficiency of the proposed IDS against black hole nodes. In an area of 250m _ 1000 m, 50 normal nodes executing the MAODV (Modified AODV) routing protocol were randomly distributed, and a couple of malicious nodes, selectively performing black hole attack, i.e., executing alternatively MAODV or BAODV (Black hole AODV), are randomly located, along with several fixed IDS nodes, which execute ABM (Anti-Blackhole Mechanism).

Twenty pairs were randomly chosen for data communication, each sending 5 kb UDP-CBR (Constant Bit Rate) per second. All normal nodes were moved in a Random-way point model, with random speeds ranging between 0 and 20 m/s. In addition, four types of pause times of the normal nodes, 0 s, 5 s, 10 s, and 15 s were separately considered. Pause time refers to the time that a moveable node can remain in one place, and then continue moving. For example, in the case of pause time 0, it means all nodes continuously moved.

IV. SIMULATION RESULTS

In this paper, the malicious nodes are detected and separated by deploying IDS in MANETs. All IDS nodes perform an ABM (Anti-Black hole Mechanism), which estimates the suspicious value of a node, according to the amount of abnormal difference between RREQs and RREPs transmitted from the node. With the prerequisite that intermediate nodes are forbidden to reply to RREQs, if an intermediate node, which is not the destination and never broadcasts a RREQ for a specific route, forwards a RREP for the route, then its suspicious value will be increased by 1 in the nearby IDS's suspicious node table. When the suspicious value of a node exceeds a threshold, a Block message is broadcasted by the IDS to isolate the suspicious node.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 7, July 2014

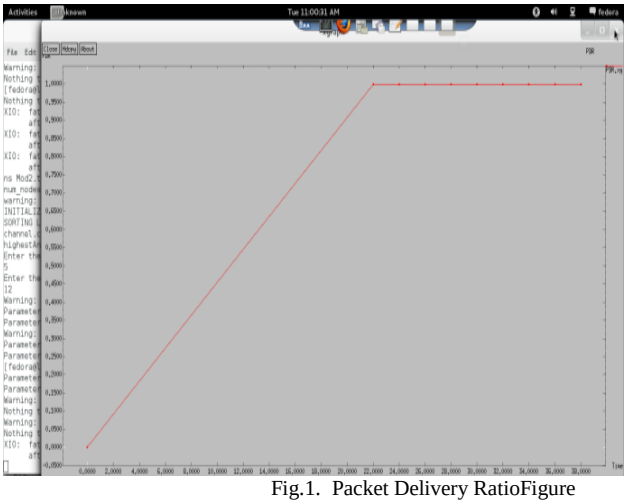

Fig.1. Packet Delivery RatioFigure

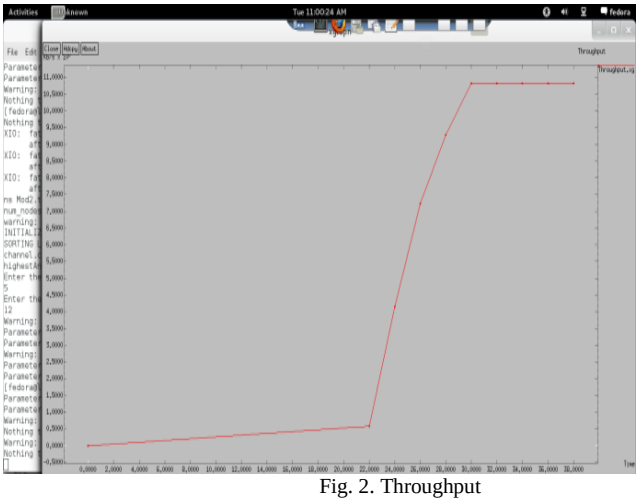

Fig. 2. Throughput

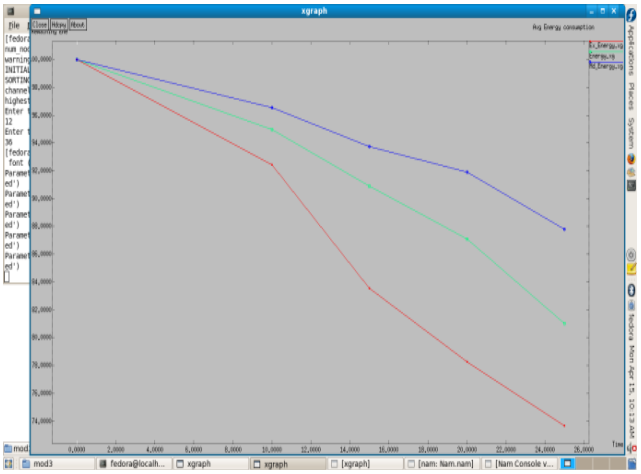

Fig. 3. Energy Consumption

V. CONCLUSION AND FUTURE WORK

In this paper, the malicious nodes are detected and separated by deploying IDS in MANETs. All IDS nodes perform an ABM (Anti-Black hole Mechanism), which estimates the suspicious value of a node, according to the amount of abnormal difference between RREQs and RREPs transmitted from the node. With the prerequisite that intermediate nodes are forbidden to reply to RREQs, if an intermediate node, which is not the destination and never broadcasts a RREQ for a specific route, forwards a RREP for the route, then its suspicious value will be increased by 1 in the nearby IDS's suspicious node table. When the suspicious value of a node exceeds a threshold, a Block message is broadcasted by the IDS to isolate the suspicious node.

REFERENCES

1.T. Clausen, P. Jacquet, Optimized Link State Routing Protocol (OLSR), IETF RFC 3626, October 2003.
2.C.E. Perkins, E. Beliding-Royer, S. Das, Ad hoc on-demand distance vector (AODV) routing, IETF Internet Draft, MANET working group, Jan. 2004.
3.D.B. Johnson, D.A. Maltz, Y.-C. Hu, ''The Dynamic Source Routing Protocol for Mobile Ad-hoc Network (DSR),'' IETF Internet Draft, July 2004.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 7, July 2014

4. Latha Tamilselvan, Dr.V. Sankaranarayanan, Prevention of co-operative black hole attack in MANET, Journal of Networks 3 (5) (2008) 13–20.
5. Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, Yoshiaki Nemoto, Detecting blackhole attack on AODV-based Mobile Ad Hoc Networks by dynamic learning method, International Journal of Network Security 5 (3) (2007) 338–346.
6. Junhai Luo, Mingyu Fan, Danxia Ye, ''Black Hole Attack Prevenstion Based on Authentication Mechanism", in: Proc. of the IEEE Singapore International Conference on Communication Systems (ICCS), pp. 173–177, 2008.
7. Soufine Djahel, Farid Nait-Abdesselam, Ashfaq Khokhar, ''An Acknowledgment-Based Scheme to Defend Against Cooperative Black Hole Attacks in Optimized Link State Routing Protocol", in: Proc. of the IEEE International Conference on Communications (ICC), pp. 2780–2785, 2008.