ISSN: 2277-9655
Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Dection of Routing Misbehaviour in MANET

Dr. R. Madhanmohan[*1], K.Manikandan[2]

[*1] Assistant Professor, [2] P.G Student, Department of Computer Science Engineering, Annamalai University, Annamalai Nagar, India

maniprems.k@gmail.com

Abstract

Ad hoc on demand Distance Vector (AODV) is one of the most suitable routing protocols for the MANETs and it is more vulnerable to black hole attack by the malicious nodes. A malicious node that incorrectly sends the RREP (route reply) that it has a latest route with minimum hop count to destination and then it drops all the receiving packets. Therefore, we proposed the multiple IDS (intrusion detection system) nodes are deployed in MANETs in order to detect and prevent selective black hole attacks. All IDS 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. The NS2 simulation results confirmed that the propose protocol IDS shown better performance than conventional protocol AODV

Keywords: Intrusion detection system (IDS), Black hole attack.

Introduction

A Mobile Ad hoc network (MANET) is an autonomous network that consists of mobile nodes that communicate with each other over wireless links. These types of networks are suitable for usage in situations where a fixed infrastructure is not available, not trusted, too expensive or unreliable. In the absence of a fixed infrastructure, nodes have to cooperate in order to provide the necessary network functionality. Routing is one of the primary functions each node has to perform anytime and anywhere in order to enable connections between nodes that are not directly within each other's sending range [1]. The development of efficient routing protocols is a nontrivial and challenging task because of the specific characteristics of a MANET environment. An example of MANET environment is shown in Figure.

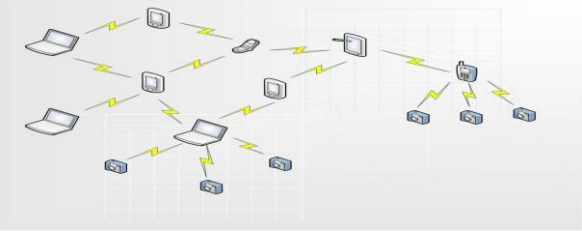

Figure 1.1AdHoc Networks

Each mobile node acts as a host when requesting/providing information from/to other nodes in the network, and acts as router when discovering and maintaining routes for other nodes in the network. MANET nodes perform the routing functions themselves. Due to the limited wireless transmission range, the routing generally consists of multiple hops[2]. Therefore, the nodes depend 2 on one another to forward packets to the destinations. The nature of the networks places two fundamental requirements on the routing protocols. First, it has to be distributed. Secondly, since the topology changes are frequent, it should compute multiple, loop-free routes while keeping the communication overheads to a minimum [3].

Ease of Use

Ad Hoc on demand distance vector

Ad hoc On-Demand Distance vector algorithm provides dynamic, self starting and multi hop routing between the nodes. AODV allows mobile nodes to obtain routes quickly for new destinations, and does not require nodes to maintain routes to destinations that are not in active communication [4]. AODV allows mobile nodes to respond to link breakages and changes in network topology in a timely manner. Types of messages:

Route Requests(RREQs)
Route Replies(RREPs)
Route Errors(REERs)

ISSN: 2277-9655
Impact Factor: 1.852

Whenever a route is required for a particular destination a route request (RREQ) packet is broadcasted. This broadcast message propagates through the network until it reaches an intermediate node that has recent route information about the destination or until it reaches the destination node. Whenever an intermediate node forwards the route request packet, it records in its own tables which node the route request came from. This route information is used to form the reply path for the route reply (RREP) packet as AODV uses only symmetric links. As RREP packet traverses back to the source, the nodes along the reverse path enter their routing information in their tables. Nodes monitor the link status of next hops in active routes. Whenever a link failure occurs, the source is notified with a route error (RERR) message and a route discovery may be requested again if needed. The RERR message indicates those destinations which are now unreachable due to the loss of the link.

Generating Route Requests

A node disseminates a RREQ when it determines that it needs a route to a destination and does not have one available. This can happen if the destination is previously unknown to the node or if a previously valid route to the destination expires or is marked as invalid. The Destination Sequence 8 Number field in the RREQ message is the last known destination sequence number for this destination and is copied from the Destination Sequence Number field in the routing table. If no sequence number is known, the unknown sequence number flag MUST be set. The Originator Sequence Number in the RREQ message is the node's own sequence number, which is incremented prior to insertion in a RREQ[1]. The RREQ ID field is incremented by one from the last RREQ ID used by the current node as show in Figure . Each node maintains only one RREQ ID. Maintaining the Integrity of the Specifications.

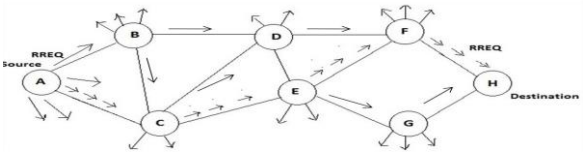

Figure 2.1 Broadcast of RREQ packets

Problem Methodology and Definition

Problem Definition

The Ad Hoc On-Demand Distance Vector (AODV) protocol is an on-demand protocol specialized for mobile ad hoc network. Because of nodes mobility and limited transmission range, the routes created by original AODV become invalid frequently leading to larger control overhead. Conventional routing protocols designed for Internet, which require periodical routing information changed, cannot perform well in MANET for dynamic topology, limited bandwidth and restricted nodes power. In most reactive protocols, the source node obtains the route to its target by flooding route request (RREQ) packet through the network.

In mobile ad hoc networks (MANETs) is the path selection scheme. Many Ad-hoc network routing protocols choose the number of hops (shortest path) as the metric for data transfer [5].

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. Thus, these are prone to degrade the network performance. 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-Black hole 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 broad-cast a block message, informing all nodes on the network, asking them to cooperatively isolate the Malicious node. This study employs NS2 to validate the effect of the proposed IDS deployment, as IDS nodes can rapidly block a malicious node, without false positives, if a proper threshold is set. 22.

Wireless ad-hoc networks are usually susceptible to different security threats and black hole is one of these, in this type of attack, a malicious node which absorbs all data packets makes use of the vulnerabilities of the on demand route discovery protocols, such as AODV. In the route discovery process of AODV protocol, Intermediate nodes are responsible to send a fresh path to the destination, sending discovery packets to the neighbor nodes. Malicious nodes abuse this process and they immediately respond to the source node with false information as though they have a fresh enough path to destination. Therefore source node sends its data packets via this malicious node assuming it is a true path. Black hole behavior may also be due to a damaged node dropping packets unintentionally. In any case, the end result of the presence of a black hole in the network is lost packets. How we can secure our network and its operation during network initializing,

ISSN: 2277-9655
Impact Factor: 1.852

packet forwarding and route maintenance process and how we can detect the malicious and selfish node. The above discussion needs the secure mechanism for secure routing in MANET and make sure that it can adapt the situation regarding to detection of malicious and selfish node mobility, while node leaving the network and joining the network.

Methodology

AODV provides a rapid, dynamic network connection, featuring low processing loads and low memory consumption. AODV uses a sequence number to distinguish whether the routing message is fresh. Routing messages in a network can be divided into path discovery and path maintenance messages. The former includes Route Request (RREQ) and Route Reply (RREP), while the latter includes Route Error (RERR) and Hello messages. Since the RREQ and RREP are directly and largely involved in the proposed IDS of this paper, In addition, each node maintains a routing table, the contents of which are updated while receiving a routing message. When a source needs to send data to a destination, but its routing table path to the destination is out of date, or there is no path, then, the source would broadcast a RREQ to all nodes in the network. Each intermediate node receiving a RREQ would first judge whether it is the source, or if such an 23.

RREQ is repeated; if yes, this RREQ would be dropped, if no, the RREQ would be processed and re-broadcasted. In processing the RREQ, an intermediate node first checks if a corresponding reverse route exists in its routing table, if not, the node would create an entry for a reverse route. The purpose of a reverse route is to allow the intermediate node to send a RREP back to the source. If there is a reverse route, the intermediate node checks the content of this entry, and if the destination sequence number in this entry is smaller than the source sequence number in the RREQ (a larger number means newer information), or if the two but the hop count recorded by the routing table is larger (smaller hop count means shorter path), then, the information in the entry would be replaced by the information in the RREQ.

Then, if this intermediate node has a route to the destination, and the route is not expired, then, the intermediate node would return the RREP to the source by the reverse route. However, if the intermediate node does not have a (forward) route to the destination, it will broadcast the RREQ to continue searching a route to the destination node. where s and d represent the source node and the destination node, respectively, the gray lines represent the tracks of the RREQ, and the black lines represent reverse routes, as reserved in the routing tables of the intermediate nodes. Each node only needs to know the following node, and does not need to know all nodes of the entire route. Taking the node g for example, the following node back to s is node f. Node h would receive two RREQs, transmitted from e and g. In this case, it is assumed that the RREQ from e arrives first; therefore, the RREQ from g, which arrives later, would be immediately dropped. When the destination node, or some intermediate node, which knows a route to the destination, receives an RREQ, , it would reply an RREP to the source by a uncast method, rather than the broadcast method, If the intermediate node receiving the RREP does not have a forward entry in its routing table, it would create a forward entry and store the data of the RREP into the new entry. If there is a forward entry, the destination sequence number in this entry would be compared with that in the RREP. If the latter is larger, then the intermediate node would update thi entry according to the RREP, and then send the RREP back to the source via the reverse route, 24.

This was created upon the receipt of the RREQ. The entries with a white background are forward entries. Once the source receives a RREP, it can transmit the data packets to the destination along the forward route. In AODV, each mobile node would periodically send Hello messages, thus, each node knows which nodes are its neighboring nodes within one-hop. If one node has not received a Hello message from a neighboring node within a certain time, the node would send an RERR message to the nodes recorded in the corresponding precursor list of the routing table, which records a list of the nodes on a route with a disappeared node. The nodes receiving an RERR would remove the compromised route from their routing tables. AODV routing protocol, despite its excellent packet arrival rate, cannot fight the threat of black hole attacks,

The main objective is to identify and isolate black hole nodes. An IDS node observe every node‟s number of broadcasted RREQs, and the number of forwarding RREQ in AODV, in order to judge if any malicious nodes are within its transmission range. Once a black hole is identified, the IDS node will send a block message through the MANET to isolate the malicious node 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 the 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 SN

ISSN: 2277-9655
Impact Factor: 1.852

(suspicious table).When the suspicious value of a node exceeds a threshold, a Block message is broadcasted by the detected IDS to all nodes on the network in order to cooperatively isolate the suspicious node. 25

All IDS nodes in this study execute a mechanism, called an ABM(Anti-Black hole 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, and the time of identification. 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.

Simulation & Results

In this section, we discuss the simulations that we conducted at the as consider insights gained on detection of routing misbehavior MANET. Having shown how we tested the Black Hole implementation, we will present the simulations of Black Hole Attack to demonstrate its effects. Then we will evaluate the effects of Black Hole Attack in an Ad-Hoc Networks.

Simulation Setup

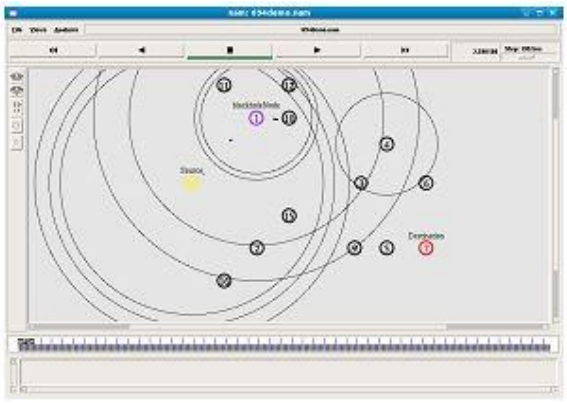

Figure 4.1 Normal Route Discovery

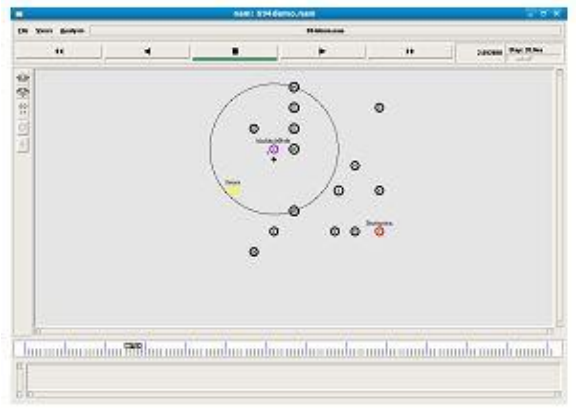

Figure 4.2 Block hole Attack AODV

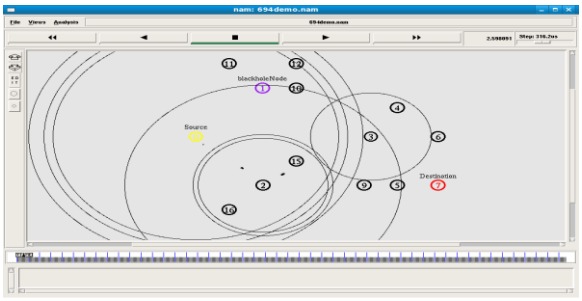

Figure 4.3 IDS AODV

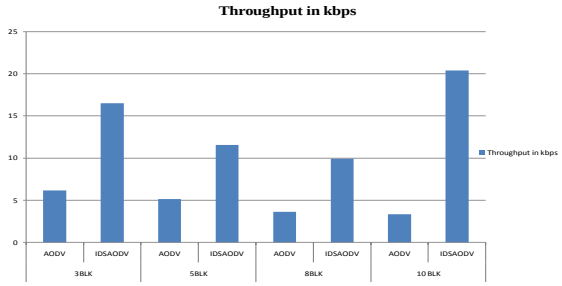

Figure 4.4 Throughput in kbps

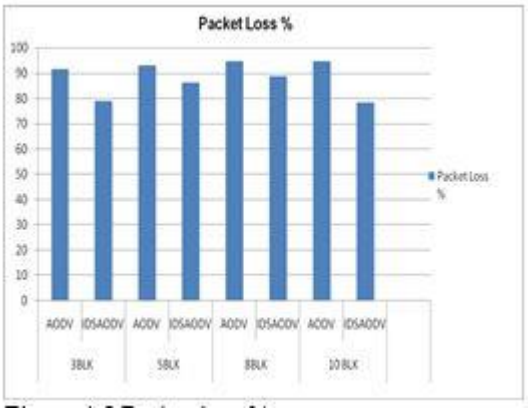

Figure 4.5 Packet loss %

ISSN: 2277-9655
Impact Factor: 1.852

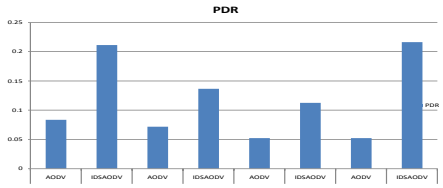

Figure 4.6 Packet Delivery Ratio

Conclution and Future work

Conclution

This project attempts to mitigate malicious nodes, by deploying IDS in MANETs (mobile Ad hoc networks). All IDS 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 the 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 SN (suspicious table).When the suspicious value of a node exceeds a threshold, a Block message is broadcasted by the detected IDS to all nodes on the network in order to cooperatively isolate the suspicious node.

Future work

In future we will try to mitigate malicious nodes, by deploying IDS in MANETS (mobile Ad hoc networks), not only for mitigating Black hole attack but also for other different types of attacks in MANET. The attacks are Gray hole attack, Worm hole attack, Link Spoofing, Link Withholding and Location disclosure. Gray hole attack in which a node changes its behavior, e.g. dropping a packet for one node and forwarding for other or dropping packet for a period of time and after it will not drop the packet. Such types of nodes are difficult to identify. Future plan is to identify the different types of attacks and implement it on simulator.

References

[1] *Hung-Min Sun, Chiung-Hsun Chen, Yu-Fang Ku (2012). "A novel acknowledgment-based approach against collude attacks in MANET. Expert Systems with Applications", 39 (2012), 7968–7975*

[2] *Ming-Yang Su (2011), "Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems". Computer Communications 34 (2011) 107–117*

[3] *Medadian, M.; Mebadi, A.; Shahri, E., "Combat with Black Hole attack in AODV routing protocol", Communications (MICC), 2009 IEEE 9th Malaysia International Conference on, vol., no., pp.530-535, 15-17, Dec.2009.*

[4] *Latha Tamilselvan, Dr. V. Sankaranarayanan, „„Prevention of Black hole Attack in MANET", in: Proc. of the International Conference on Wireless Broadband and Ultra Wideband Communication, 2007.*

[5] *Latha Tamilselvan, Dr.V. Sankaranarayanan, "Prevention of co-operative black hole attack in MANET", Journal of Networks 3 (5) (2008) 13–20*