AUTHENTICATION SCHEME FOR PREVENTION OF BLACK HOLE ATTACKS IN MANETS

J R Indusree¹, Jidhesh R², P.M. Durai Raj Vincent³

¹,² IInd M.Tech (IT), VIT University
³ Associate Professor, SITE, VIT University

Received on 25-10-2016 Accepted on 02-11-2016

Abstract

A Mobile Ad-hoc Network (MANET) is a kind of wireless ad-hoc network that keeps configuring continuously. The nodes of the MANET are dynamic in nature as they are mobile. Conventional ad-hoc routing protocols are aimed at finding optimum route from source to destination. Security in MANETs is challenging because of the infra-structure less feature and dynamic nature of nodes in MANET. There are many security attacks in MANETs the prominent ones being black hole attacks, gray hole attacks, worm hole attacks sink hole attacks etc.. This paper details a survey done on the existing mechanisms for preventing and tackling black hole attacks in MANETs and also puts forward a digital signature based authentication scheme to detect adversaries which send fake RREP packets to source.

Keywords: MANET, Security, Malicious node, Intrusion, Black Hole, Digital Signature, RSA, Compression, Huffman coding

Introduction

Mobile Ad-hoc Network (MANET)[1] consists of nodes which are mobile. The network has the property of self-configuration as there are no central controllers or infrastructure to help configure and maintain the network. The nodes communicate with each other through radio waves. The various challenges faced by wireless networks are as follows:

- There are limitations on the computational capacity of the nodes in MANET. Complex security algorithms cannot be deployed at the nodes
- The bandwidth in wireless medium is limited which leads to less data rates compared to the wired medium.
- The nodes in a MANET are of different characteristics and hence compatibility should be ensured while establishing network
• Cryptography techniques require key management which is difficult in MANETs due to the dynamic nature of nodes
• Transmission errors are more in wireless environment leading to increased packet loss rates
• The power limitations restrict processing and mobility of nodes

As the wireless networks have already gained prominence, it is important to ensure security in networking. Security is challenging in MANETs as there is no central access point or control and also due to dynamic nature of nodes. The conventional routing protocols used in MANETs (Proactive as well as reactive) does not address security issues faced in MANETs.

The various security attacks on MANETs are as follows:

- **Denial-of-Service (DoS) attack:** The attacker depletes resources of the network purposefully so as to prevent genuine nodes from getting services.
- **Worm-hole attack:** This attack involves two or more adversaries where the route between the adversaries is faked and the packets are tunneled out of the correct route.
- **Flooding-attack:** It is a type of DoS attack where the adversary floods the network with fake packets with an aim to deplete the network resources.
- **Impersonation attacks:** These attacks include malicious nodes faking identity and participating in communication/routing for the purpose of accessing data or to mislead in the routing.
- **Packet modification attacks:** The attacker node will access the contents of the packet and modify the same before forwarding.
- **Black-hole[2] / Gray-hole attacks:** The malicious node will send the wrong RREP packets to source and when the source sends the packets these packets are dropped. Black hole attack involves malicious nodes dropping all the packets received. Whereas gray-hole attack is the one where selectively packets are forwarded or dropped.

There are many methods proposed to protect the network against various attacks most of them using encryption mechanisms or digital signatures to authenticate the sender or any intermediate node. Few other mechanisms are enhancements to the existing ad-hoc routing protocols (proactive or reactive). Among the various attacks, black hole/gray hole attacks are difficult to resolve as the nodes involved behave like normal nodes and involve in route discovery in the
same way as a normal node does.

Black hole attack can be single node based black hole attack or collaborative black hole attack. Single node attack (Figure 1) involves only one malicious node which misleads source by sending RREP message and the data packets are not forwarded instead dropped. Collaborative attacks (Figure 2) include at least two malicious nodes which try to capture the traffic towards them and then drop packets.

This paper summaries few of the existing mechanisms to prevent black hole in MANETs. The rest of the paper is organized as follows:

The section 2 explains related work carried out in the area of concern viz. existing mechanisms to prevent black hole attacks in MANETs. Section 3 briefs the proposed system. Section 4 contains comparison of proposed system with few of the existing techniques followed by section 5 which is the conclusion of this work.

Related Work

Sruthi R and Vijayakumar R [3] present a trust based scheme which regulates access for nodes to network based on the node’s behavior, thus isolating misbehaving nodes from getting access in routing. This mechanism consists of three modules the working of each are explained are as follows:

*Monitor module:* All nodes monitor their neighbor node’s actions and collect information about the neighbor nodes and generate an evaluation report.

*Trust Module:* This module is responsible for calculating trust value of each node and checking whether the value falls below the minimum threshold of 0.4. The node with value 0 is the most untrustworthy and the one which value 1 is the most trustworthy.

*Reputation Module:* The reputation module assigns reputation to each node. Reputation value is also continuously monitored; value increases when the node does good actions and the value decreases when evidences come about the node that it has done some misbehavior. The threshold value for reputation is also 0.4. The node with trust value and reputation value less than the minimum threshold are marked malicious.
This method finds large number of malicious nodes in the network and essentially increases Packet delivery Ratio.

Anand A Aware and Kiran Bhandari [4] proposed a hash function based mechanism to prevent black hole attack in MANETs. In this scheme, the source node will send RREQ as part of route discovery. Intermediate nodes which have a route to destination or the destination node itself or some malicious node may reply back with RREP packet to the source. The source node will ignore the first arrived RREP guessing that the shortest route reply would be from malicious node. Also on sending data packet source applies a hash function; destination calculates this again after getting the data packet and if both values contradict the packet is dropped as an indication of malicious node which would have forged the packet. Data_Packet error is communicated back to source. This method efficiently prevents black hole attack but involves overhead of calculating hash value at both source and destination.

Nital Mistry et al. [5] propose an enhancement to AODV protocol using an additional function Pre_RecieveReply() for single malicious node detection. Three additional components are added to existing AODV viz. Cmg_RREP_Tab, MOS_WAIT_TIME and Mali_node. Time taken from the sending of RREQ to reception of RREP is called RREP_WAIT_TIME. MOS_WAIT_TIME is the half of RREP_WAIT_TIME. Cmg_RREP_Tab consists of the RREP packets. Whenever malicious nodes are detected, they get added to Mali_node list.

Prior to sending packets, function is executed as follows:

The Cmg_RREP_Tab is analyzed to find the RREP packets with higher destination sequence number compared with that of the source sequence number. The sender of such RREP packets is treated as malicious nodes and is added to Mali_node.

This technique improves the Packet Delivery Ratio, but the end to end delay and overhead is increased.

Su M-Y proposes [6] a modification to existing AODV which includes three new tables viz. RQ table, SN table and Block table. Intrusion Detection System (IDS) nodes are responsible for maintaining RQ table where the nodes store RREQ packets within their transmission range. SN table is used by IDS node to identify malicious nodes by analyzing the suspicious values. The suspicious value in this table increases for a neighbor node which sends RREP packet but never forwards RREQ packet. Once a malicious node is detected, it is added in the Block table.

This method employs cooperative isolation of malicious nodes and efficiently decreases the packet loss rate. One limitation with this technique is that it fails in case of collaborative attacks.
Vishnu K et al. [7] introduces mechanism to prevent black hole attacks which are collaborative in nature. Few trusted nodes in the network are selected as BBN nodes which form a back bone network. For newly arrived nodes BBNs are responsible for allocating RIP with which they can participate in routing. For packet transfer source node broadcast RREQ to the destination node as well as to the new nodes. If only destination node replays with RREP, there is no black hole. Otherwise, it indicates that there might be malicious node in the network. In this case neighbor nodes of the RIP change to promiscuous mode where the source node alerts these neighbor nodes to monitor actions of RIP. Again for detection of malicious node dummy packets are send by the source node. The neighbor nodes monitor the packet flow and if the loss rate increases rapidly this means that the corresponding RIP is a malicious node.

This system may fail if the malicious nodes are more in number than normal nodes.

Po-Chun Tsou et al. [8] proposes a scheme against collaborative attacks which is based on DSR routing and is hybrid in nature. Routing starts when the source node sends out bait RREQ prior to route discovery. This packet is bait in the sense that the destination of the packet is randomly selected and does not exist. The bait packets survive for a short period of time so as to avoid congestion. Malicious nodes are easily detected by the fact that no nodes can send back an RREP since the target address of RREQ is not genuine. So the nodes which replay back with RREP are marked as malicious. The exact position of the adversary can also be known since it is recorded in the RREP packets additional field. After this phase normal DSR initiates route discovery.

BDSR method effectively improves PDR and also reduces communication overhead.

Ankita V. Rachh et al. proposed [9] enhanced AODV protocol where few nodes called leader nodes are formed which are responsible for the detection of malicious nodes. When the source node sends out RREQ packets, a timer is set. If the source receives RREP before the timer expires, then a test packet (which is fake) is sent to the destination to verify if the route does not have any malicious node. If the test packet reaches the destination and source gets a reply for this, then it indicates that the route is safe. If acknowledgement is not obtained and the packet loss rate exceeds a minimum threshold, then leader nodes inform all the neighbors about the, malicious nodes. RREQ packets are sent again and route discovery is re initiated.

This method provides an increased throughput and packet delivery ratio.

Ravinder Kaur and Jyoti Karla [10] present an authentication scheme based on normal digital signatures. In this scheme,
every legitimate node is supposed to have a digital signature. The source node broadcasts RREQ packet for route discovery. If the RREQ reaches the destination, destination node will send back the RREP packet by selecting the optimal route. Each node which receive the RREP or which creates RREP is supposed to append its ID and corresponding digital signature. The source node will verify each node’s signature with whatever is available in its database and ensures if the nodes are legitimate.

Vani A Hiremani and Manisha Madhukar Jadhao[11] introduced a mechanism which uses the Extended Data Routing Information (EDRI) table to prevent black hole attacks. The table is modified to have few more details like packet size at source and packet size at destination which is compared to find abnormalities. There is a separate function for the detection of black hole. If a malicious node is detected; the destination sends a negative acknowledgment to the source inorder to indicate that malicious node has been detected.

Proposed System

The existing techniques for preventing black hole attacks are mainly focused on malicious node detection by the involvement of source node or other intermediate and neighbor nodes during RREQ and RREP transfer. These techniques add to the workload of the nodes involved in the network. Unlike these methods, there are trust based mechanisms [12] and authentication mechanisms [13] where the node which sends back RREP is verified by digital signature algorithms such as RSA or DSA. Even though the usage of digital signature algorithms enhance security these techniques cause increased overhead of maintaining the large keys which are to be shared between nodes. This paper proposes an advanced technique based on asymmetric key cryptography which reduces the overhead incurred due to keys in digital signature algorithms and also enhances authenticity of nodes sending the RREP packet.

a. Features:

Authentication using RSA based digital signature[14]:

Digital signature scheme is used for verification and authentication of an entity. The RSA algorithm [15] is proven to be the efficient algorithm for authentication.

Compression of packet [16][17]: The most recently accepted key size of RSA algorithm is 4096 bits sharing which is causing lot of overhead during MANET routing. The proposed work reduces the entire packet size by compressing it using the lossless data compression technique: Huffman coding [18].
b. Architecture

The trust based server keeps a table of already known malicious nodes and also table containing digital signature values of every node which can be an identity (Figure 3).

The digital signature algorithm has two parts; one is hashing algorithm (SHA-3 is the advanced hashing algorithm [18]) using which hash value of the message is generated which is then signed with private key of RSA algorithm. The digitally signed packet is then compressed using Huffman coding technique. Huffman coding though less efficient compared to arithmetic coding in terms of compression ratio, it is faster than arithmetic coding [19] and hence is suitable for routing scenarios. These values are sent along with RREP packet which when the source receives, it decompresses the data and communicates to trust server which in turn using the public key stored in its database, extracts the signature and verifies with the digital signature.

c. Procedure:

Step 1: Source node S broadcasts RREQ packet for route discovery to destination D

Step 2: RREP would be sent by either an intermediate node which has a valid route to D or by the destination D itself. The packets sent whether control packet or data packet needs to be digitally signed with private key and then compressed using Huffman algorithm.

Step 3: Every node through the RREP packet is originated or passed will add their digital signature with its encrypted public key.

Step 4: The source node on receiving the RREP packet will first perform decompression and then verifies with the malicious node table in the trust server to cross check if the RREP packet is from an adversary.

Step 5: If the above check is passed, then the encrypted key is decrypted using shared public key and digital signature is verified in trust server database.

Conclusion

Various conventional mechanisms for preventing black hole attack in MANETs were studied on the basis of which a new authentication based mechanism is proposed. The technique would enhance the security of digital signature and also effectively reduces the overhead of sharing the digital signature public key by encrypting it and reducing key size. The central trust server provides unbiased service for all the nodes and hence proves efficient in detecting and isolating
malicious nodes that cause black hole attack. Table 1 shows comparison of various existing techniques with the proposed system.

References

1. Nawneet Raj, Priyanka Bharti and Sanjeev Thakur; “Vulnerabilities, Challenges and Threats in securing Mobile Ad-hoc Network” ; Fifth International Conference on Communication Systems and Network Technologies; 2015; pp 771-775

2. R. Ranjan; N. K. Singh; A. Singh ; ” Security issues of black hole attacks in MANET”; International Conference on Computing, Communication & Automation (ICCCA), 2015 ; pp 452-457


11. Vani A. Hiremani and Manisha Madhukar Jadhao; “Eliminating Co-operative Blackhole and Grayhole Attacks Using Modified EDRI Table in MANET”; International Conference on Green Computing, Communication and Conservation of Energy (ICGCE); 2013; pp944 - 948


13. S. Neelavathy Pari; S. Jayapal; S. Duraisamy; “A trust system in manet with secure key authentication mechanism”; Recent Trends In Information Technology (ICRTIT), 2012; pp 261 –265


15. Xin Zhou and Xiaofei Tang; “Research and Implementation of RSA Algorithm for Encryption and Decryption”; The 6th International Forum on Strategic Technology; 2011; pp 1118-1121


20. Ashish Kumar and Vishal Arora; “Analyzing the Performance and Security by using SHA3 in WEP”; IEEE International Conference on Engineering and Technology (ICETECH), 20th March 2015; pp 1-4