MLAMAN: A NOVEL MULTI-LEVEL AUTHENTICATION MODEL AND PROTOCOL FOR PREVENTING WORMHOLE ATTACK IN MOBILE AD HOC NETWORK

Tu T. Vo[1], Ngoc T. Luong[1,2], Doan Hoang[3]

[1] *Faculty of Information Technology, Hue University of Sciences, Hue University, Viet Nam*
[2] *Faculty of Mathematics and Informatics Teacher Education, Dong Thap University, Viet Nam*
[3] *Faculty of Engineering and Information Technology, the University of Technology Sydney, Australia*
[1] *vttu@hueuni.edu.vn;* [2] *ltngoc@dthu.edu.vn;* [3] *Doan.Hoang@uts.edu.au*

Abstract. Wormhole attack is a serious security issue in Mobile Ad hoc Network (MANET) where malicious nodes may distort the network topology and obtain valuable information. Many solutions, based on round trip time, packet traversal time, or hop-count, have been proposed to detect wormholes. However, these solutions were only partially successful in dealing with node high-speed mobility, variable tunnel lengths, and fake information by malicious nodes. To address those issues, this paper proposes a novel multi-level authentication (MLA) model and protocol (MLAMAN) for detecting and preventing wormhole attacks reliably. MLAMAN allows all intermediate nodes to authenticate control packets on a hop-by-hop basis and at three levels: 1) the packet level where the integrity of the packets can be verified, 2) the node membership level where a public key holder-member can be certified, and 3) the neighborhood level where the neighborhood relationship between nodes can be determined. The novelty of the model is that it prevents malicious nodes from joining the network under false information and pretense. It detects wormhole nodes effectively under various scenarios including variable tunnel lengths and speeds of moving nodes. The effectiveness of our approach is confirmed by simulation results through various scenarios.

Keywords. AODV; MANET; MLA; MLAMAN; mobile ad hoc network; network security

1. Introduction

A Mobile Ad hoc Network (MANET [5]) is a collection of wireless mobile nodes without network infrastructures, routers or access points. The topology of the network can change unpredictably and frequently because of nodes joining or leaving. In a MANET, nodes communicate with neighbors to discover and maintain routes to their destinations. Data transfer from a source node to a destination node can be routed through intermediate nodes, which act both as hosts or routers. A network routing protocol in a MANET specifies how nodes in the network communicate with one another. It enables a node to discover and maintain the routes as needed between itself and other nodes. Many routing protocols have been developed for MANETs [3]; among them, Ad hoc On-demand Distance Vector (AODV) [21] and Dynamic Source Routing (DSR) [10] are the most important protocols. Because of the ad hoc nature, Denial of service (DoS) is a serious issue in MANET. DoS attacks aim to deny a user of a service or a resource he/she would normally expect to receive. Disrupting the routing services at the network layer is an example of DoS [22] where a malicious node tries to deplete resources of other nodes. Other types of DoS include Blackhole [24], Sinkhole [19], Grayhole [4], Flooding [25] , Whirlwind [20], and Wormhole [12].

The wormhole attacks in Ad hoc Networks are described in [9][12][14] cite where the authors categorize several types of packet tunneling wormhole attacks , including wormhole through the tunnel (called out-of-band channel - OB), wormhole using encapsulation, wormhole using packet relay, and wormhole with high power transmission. Such wormhole attacks may operate in two modes: Hidden Mode (HM) and Participation Mode (PM). In HM, malicious nodes are hidden from normal nodes, which on receiving a packet they simply forward the packet without processing it. By doing so, the malicious nodes are invisible as they never appear in the routing tables of their neighbors. In contrast, in PM, malicious nodes are visible during the route discover process because they process control packets just like other normal nodes. These malicious nodes appear in the routing tables of their neighbors and the hop-count (HC) values increase when control packets are routed. This type of attacks can easily be carried out with on-demand routing protocols, typically the AODV routing protocol to eavesdrop information.

Previous researches on wormhole attacks mainly focus on detection algorithms that rely on Geographical Location, Round Trip Time, Packet Traversal Time, Hop-Count information, or Digital signatures. These algorithms, however, have many weaknesses: With geographical location based approaches such as LBK [15] or SeRLoc [16], nodes continuously broadcast location data (GPS information) and all transmissions between node pairs are encrypted. On the other hand, the TIK [6] solution rely on synchronization among all nodes. These solutions thus incur high communication overhead. With time analysis based approaches such as DelPHI [1], MHA [9], and TTHCA [12][13], a malicious node may collaborate with the route discovery process but deliberately provides fake information in the control packets. With digital signature based approaches such as SAODV [18] which does not have a key management mechanism, malicious nodes can pass over the security by using fake keys. On the other hand, ARAN [23] supports key management, but it is not able to detect wormhole node under HM mode (according to [8]). This paper proposed MLAMAN, a new MANET wormhole detection model that comprises a multi-level authentication (MLA) mechanism, an MLA-secured routing protocol, and a node membership certification protocol. The MLA mechanism uses digital signatures with the RSA [2] public key encryption and SHA_1 [11] hashing function. With MLA, all intermediate nodes can authenticate control packets on a hop-by-hop basis and at three levels: 1) the packet level where the integrity of the packets can be verified, 2) the node membership level where a public key holder-member can be certified, and 3) the neighborhood level where the neighborhood relationship between nodes can be determined. The MLAMAN protocol is a modified version of the AODV to incorporate the MLA mechanism. The node membership certification protocol allows nodes to participate in the routing procedure. It is demonstrated that the proposed solution is effective in wormhole detection under various network scenarios, and prevents malicious node from taking part in the route discovery process with fake information.

The remainder of this article is structured as follows. Section 2 discusses related work. Section 3 describes the proposed MLAMAN model for wormhole detection with multi-level authentication (MLA) mechanism. The proposed MLAMAN protocol (MLA mechanisms for Mobile Ad hoc Network) by integrating the MLA into the route discovery procedure of AODV protocol. A public key management method and protocol to provide Membership

Certification (MC) for a node before it can participate in the route discovery process. Section 4 presents the performance evaluation results by simulation using NS2 [7]. Finally, section 5 concludes the paper and provides a discussion on future work.

2. Related works

This section summarizes related work that focuses on location-based, time-based, and digital signature-based approaches in detecting and preventing wormhole attacks in MANETs. *On geographical location based approach.* The authors in [15] described a graph theoretic model to characterize the wormhole attack and prevent wormholes. They used a Local Broadcast Key (LBK) method to install a secure Ad-hoc Network against wormhole attacks. Two types of nodes are involved: guard nodes and regular nodes. The Guard nodes continuously broadcast location data obtained from localization systems such as the Global Positioning System (GPS) or SeRLoc [16]. Regular nodes calculate their location relative to the guards' beacons and by doing so they can detect abnormal resend transmission by the wormhole attackers. All transmissions between node pairs are encrypted by the local broadcast key of the sending end and decrypted at the receiving end. This approach is suitable for networks with fixed and static topology wireless sensor networks. For dynamic topologies, the solution is not effective as its performance suffers badly due to large time delay variations and communication overhead caused by continuous broadcast of location data.

On time analysis based approach. The authors in [6] described the TIK protocol for detecting wormhole attacks. TIK uses Packet Leashes solution that appends timing information to a packet to limit its admissible transmission distance. Thus, a wormhole attack is detected when packets are delivered at a much shorter time than possible through expected valid routes. TIK depends on a strict synchronization among all nodes. As synchronization is difficult and resource-consuming, such detection method become less effectiveness in high-speed mobile networks. The authors in [1] described the Delay Per Hop Indication (DelPHI) solution for detecting wormhole attacks. The idea is to allow the source node to receive the route reply packets on many routes and calculates the round trip time (RTT) per route. It is assumed that a route with a small number of hops has a small RTT, so the route that has a higher RTT per hop count than a pre-calculated threshold is considered a wormhole route. However, in dynamic environments where the network loads are unpredictable and nodes move rapidly, the RTTs are highly variable, the proposed solution becomes less reliable. The authors in [9] proposed the multi-hop count analysis (MHA) solution based on hop counts. MHA does not require Round Trip Time (RTT) measurement. MHA modifies the AODV route discovery protocol to identify several unique routes between the source and the destination nodes. A route with a much lower HC value than other routes is then assumed to include a wormhole and is avoided. The authors in [12] presented a wormhole detection algorithm based on Traversal Time and Hop Count Analysis (TTHCA) for the AODV routing protocol. TTHCA obtains the packet transversal time (PTT) by subtracting the highly variable processing times of nodes along the route from the RTT and provides a more reliable wormhole detection performance with low error rates, and small computational costs. However, the TTHCA detection ability to malicious nodes is restricted because the PTT of packet is seriously affected by nodes moving at fast speeds. An improved TTHCA to identify time measurement tampering in traversal time and hop count analysis wormhole detection algorithm, is described in [13].

On digital signature based approach. Many proposed solutions deployed cryptographic techniques to protect routing packets and detect wormholes. The Secure AODV (SAODV) [18] is proposed to prevent malicious nodes from fabricating the HC number and the Sequence Number (SN) in route discovery packets. However, SAODV only supports end-to-end certification and not hop-by-hop, as a consequence, an intermediate node cannot certify packet from its preceding node. In addition, because SAODV does not have a key management mechanism for node, so malicious nodes can pass over security by using fake keys. The authors in [23] proposed the Authenticated Routing for Ad hoc Networks (ARAN) protocol for detecting and preventing attacks on insecure protocols. Different from SAODV, route discovery packet (RDP) in ARAN is signed and certified at all hop-by-hop nodes. ARAN supplements the public key management mechanism to provide authentication and non-repudiation services. However, it is not able to detect wormhole node under HM mode. Furthermore, ARAN assumes that there is no way to way to guarantee that one path is shorter than another in terms of hop count. Accordingly, ARAN does not guarantee a shortest path, but offers a quickest path which is chosen by the RDP that reaches the destination first. That means that ARAN is unable to identify the routing costs through intermediate relaying nodes.

3. MLAMAN - A Multi-Level Authentication Model for MANETs

This section describes our proposed Multi-Level Authentication model for mobile ad hoc networks, MLAMAN consists of three components: a multi-level authentication mechanism for detecting and preventing both PM and HM wormhole attacks, a modified AODV protocol (MLAMAN routing protocol) for route discovery and route maintenance, and an auxiliary node membership certification protocol. The following subsections describe the three elements of the MLA model.

3.1. The MLA mechanism

The MLA mechanism is designed to authenticate routing packets (RREQ or RREP) on a hop-by-hop basis and at three levels: *(1) Packet integrity level; (2) Node member certification level; (3) and Neighborhood verification level.* Table 1 defines symbols used in the paper.

Table 1. Description of symbols

Variable	**Descriptions**
MC$_{N_\delta}$	Membership certificate of node N_δ
T$_{MC}$	Time interval for N$_{center}$ checks PKDB to provide the MC
N$_\delta$	Node labeled N_δ
$k_{N_\delta}+$, $k_{N_\delta}-$	Public and private keys of node N_δ
En(v, k)	Encryption of value v using key k
De(v, k)	Decryption of value v using key k
H(v)	Hash value of v
IP$_{N_\delta}$	Address of node δ
PKDB	Public key database in node N$_{center}$

3.1.1. Packet integrity verification

The integrity verification process is designed to prevent a malicious node to tamper with the control packet when it is relayed from hop to hop. Under the PM mode, malicious nodes may deliberately alter the contents of the routing packets. The main idea is for a node (N_i) to verify the integrity of the RREQ packet (or RREP) it receives from a source node or an intermediate node N_j. The packet verification value is obtained as follows. First, the sending node N_j uses H to hash all protected fields of the RREQ (or RREP) packet and then encrypts the resulting hash value using its private key as shown in eqn 1. The encrypted value is saved into the VC field of the packet (RREQ or REP) before broadcasting it to its neighbor N_i.

$$P.VC = En(H(P.Fields\ \{VC\}), k_{N_j}-) \tag{1}$$

Where P is RREQ or RREP packets.

Algorithm 1 shows steps that N_i verifies the integrity of the packet RREQ (or RREP) on receiving from a source (or an intermediate) node N_j. Node N_i uses the public key $k_{N_j}+$ to decrypt the VC field value of packet (P.VC). Protected fields of the packet are hashed by N_i using the H function. If the hask value $val2$ matches $val1$ the integrity of the packet is verified, otherwise else the packet has been modified, and it can be concluded that the preceding node (node N_j) is a PM wormhole node.

Algorithm 1 Checking the Packet Integrity at node N_i

Input: RREQ or RREP packet; $k_{N_j}+$ is the public key of N_j

Output: True if RREQ (or RREP) packet is integrity; else return False

```
function BOOLEAN ISPACKETINTEGRITY(Packet $P$; Key $k_{N_j}+$)
    Begin
        $val_1 \leftarrow De(P.VC, k_{N_j}+)$;
        $val_2 \leftarrow H(P.Fields\backslash\{VC\})$;
        Return ($val_1 == val_2$);
    End
```

3.1.2. Node member authentication

As with other solutions that deployed cryptographic techniques, each node in the environment has a private key and a public key. The proposed solution also assumes that for a node to participate in the route discovery process it has to be certified and its certificate can be verified by any other node with the proposed procedure. This node member authentication excludes malicious nodes from the routing process and overcomes the weakness from SAODV. We use a reliable node named N$_{center}$ to manage and provide the Membership Certification (MC) to all nodes using the MCP and MC_{ACK} packets. Section 3.3. will discuss the procedure and the auxiliary protocol for this node membership certification.

Definition 1: Membership Certification is provided for all nodes automatically by the N$_{center}$ and it is added to the RREQ or RREP packet while node participates in the discovery route process. MC of node N_δ is calculated by first encrypting the hash value of the member's node address (IP_{N_δ}) and public key ($k_{N_\delta}+$) with the private key of the N$_{center}$ and then encrypting the encrypted result of the first step with the private key of the member node N_δ as shown in eqn 2.

$$MC_{N_\delta} = En(En(H(IP_{N_\delta}, k_{N_\delta}+), k_{N_{center}}-), k_{N_\delta}-) \tag{2}$$

Algorithm 2 shows steps to verify MC when node N_i receives a RREQ (or RREP) packet sent (or forwarded) by node N_δ. Node N_i decrypts the MC field of the packet (P.MC) using the public key of node N_δ and then decrypts the resultant with the public key of node N_{center}. If the value after decryption matches the hash value of N_δ node address then N_δ is a valid member node. Otherwise, the packet is dropped because the membership of sending node N_δ cannot be verified (either the node is unknown or has not been MCed by Ncenter). Note that the member nodes authentication process is performed only when the integrity of the packet RREQ (or RREP) has been verified.

Algorithm 2 Checking Members Node at N_i

```
Input: RREQ or RREP packet; $k_{N_\delta}+$ is public key of $N_\delta$
Output: True if $N_\delta$ is members; Else return False
function BOOLEAN ISMEMBERSNODE(Packet $P$; Key $k_{N_j}+$)
    Begin
        If Not IsPacketIntegrity(P, $k_{N_\delta}+$) Then return False;
        $val_1 \leftarrow De(De(P.MC, k_{N_\delta}+), k_{N_{center}}+)$;
        $val_2 \leftarrow H(IP_{N_\delta}, k_{N_\delta}+)$;
        Return $(val_1 == val_2)$;
    End
```

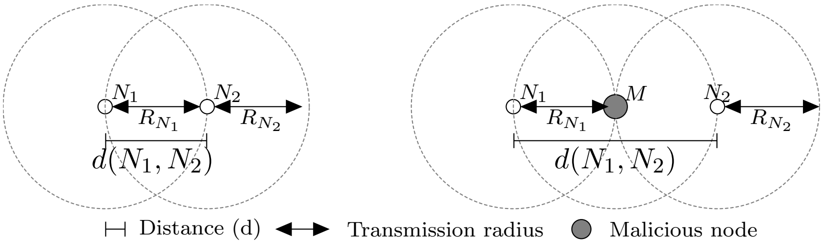
3.1.3. Neighborhood relationship verification

The proposed neighborhood relationship determination allows a member node to detect a route with wormhole node. When N_i receives RREQ (or RREP) packet from N_j, if both of N_i and N_j nodes are not physically neighbors, a HM wormhole node must have operated on the discovered route.

Definition 2: Two nodes (N_i and N_j) are geographic and physical neighbors of each other if they are within their transmission radius. Explicitly, N_i and N_j are neighbors only if $d(N_i, N_j) \leqslant min(R_{N_i}, R_{N_j})$, where R_{N_δ} is maximum transmission radius of N_δ and $d(N_i, N_j)$ is Euclidean distance between N_i and N_j as given by eqn 3, and (x_{N_δ}, y_{N_δ}) is the location coordinate of node N_δ.

$$d(N_i, N_j) = \sqrt{(x_{N_i} - x_{N_j})^2 + (y_{N_i} - y_{N_j})^2} \tag{3}$$

Example 1: In the network topology shown in Figure 1a), both of nodes N_1 and N_2 are neighbors in the physical sense because the distance between N_1 and N_2 is less than (or equal to) the minimum transmission radius of the two nodes. In MANETs, the location of a node changes due to its mobility nature. We adopt the use of GPS to obtain node location as described in [14][15].



a) Normal

b) Wormhole node using HM mode

Figure 1. Physical neighbor nodes

Example 2: In wormhole HM mode attack, malicious nodes are hidden from normal nodes. As shown in Figure 1b), a wormhole node M, on receiving the RREQ (or RREP) from N_1, it will forward the packet to N_2 without changing the packet. Hence, N_2 cannot detect the malicious node M with only packet integrity verification and member node authentication.

Algorithm 3 Checking Actual Neighbors

```
Input: RREQ or RREP packet
Output: True if source node is actual neighbors; Else return False
function BOOLEAN ISACTUALNEIGHBOR(Packet $P$; Key $k_{N_j}+$)
    Begin
        If Not IsPacketIntegrity(P, $k_{N_j}+$) Then return False;
        GPS g = getGPS(); //$N_i$ location
        $d \leftarrow Distance(P.GPS, g)$;
        Return ($d \leqslant Min(P.R, R_{N_i})$);
    End
```

The procedure for determining if a node is a true physical neighbor of another node is shown in Algorithm 3. In order to calculate the distance between the two nodes, N_j saves the location information and maximum radio range into GPS and R fields of the packet before sending (or forwarding) the packet. At node N_i, after receiving the packet from node N_j, it checks if the distance between itself and N_j is less than (or equal) the minimum of the radio range (R) of the two nodes then N_i and N_j are verified true neighbors, otherwise, there is a wormhole node on discovered route invisibly relaying the packet.

3.2. MLAMAN protocol – A secure AODV route discovery with Multi-Level Authentication

As part of the MLAMAN model, we propose MLAMAN protocol, a secure and enhanced AODV with built-in MLA mechanism for detecting and preventing wormhole attacks. Similar to AODV, MLAMAN protocol includes two phases: a broadcasting route request phase and an unicasting route reply phase. The control route packet structures of the new protocol (SecRREQ and SecRREP) extend the control packet structures of AODV (RREQ and RREP) to include five new fields (5NF): *GPS, R, MC, KEY* and *VC* as shown in Figures 2.

Original RREQ packet
Location (GPS)
Maximum radio range (R)
Member Certification (MC)
Public key (KEY)
Checking Value (VC)

(a) SecRREQ

Original RREP packet
Location (GPS)
Maximum radio range (R)
Member Certification (MC)
Public key (KEY)
Checking Value (VC)

(b) SecRREP

Figure 2. The control route packet structures of MLAMAN protocol

3.2.1. Broadcasting route request packet phase

a) Generating SecRREQ packet: If the source node (N_S) does not have a route to the destination node, it initiates a new route discovery process by broadcasting the SecRREQ packet to its neighbor nodes as in (4).

$$N_S broadcasts : SecRREQ \leftarrow \{RREQ^* \oplus 5NF\} \tag{4}$$

Where $RREQ^*$ is the original RREQ packet of the AODV routing protocol and 5NF is the five new fields of the SecRREQ. These new fields contain the following information:

- SecRREQ.GPS = N_S node GPS information;
- SecRREQ.R = 250 m;
- SecRREQ.MC = N_S node MC;
- SecRREQ.KEY = Source node public key $k_{N_S}+$;
- SecRREQ.VC = Encryption of H(SecRREQ.fields \ {VC}) using $k_{N_S}-$;

b) Processing and forwarding SecRREQ packet: When a node receiving a SecRREQ packet, the node (say N_i) drops this packet if it has not been certified, otherwise, it tests the integrity of the packet, verifies the node membership of the sending node, and determines if the sending node is a true neighbor according to the MLA mechanism.

- If the integrity SecRREQ packet is not verified, N_i drops the packet as the discovered route has been tampered by a malicious node under PM mode.
- If the SecRREQ packet is not sent by a certified member node, N_i drops the SecRREQ packet;
- If the SecRREQ packet is not sent by a true neighbor node, N_i drops the SecRREQ packet as the discovered route has been interfered by a malicious node under HM mode.

If all the conditions are satisfied, and the current node is the destination, it generates and sends back the SecRREP packet; otherwise, it updates a reverse route toward the source node and the 5NF of the SecRREQ packet with the latest information before broadcasting the updated SecRREQ packet to its neighbors. Figure 3 describes the MLAMAN route request packet algorithm using MLA mechanism.

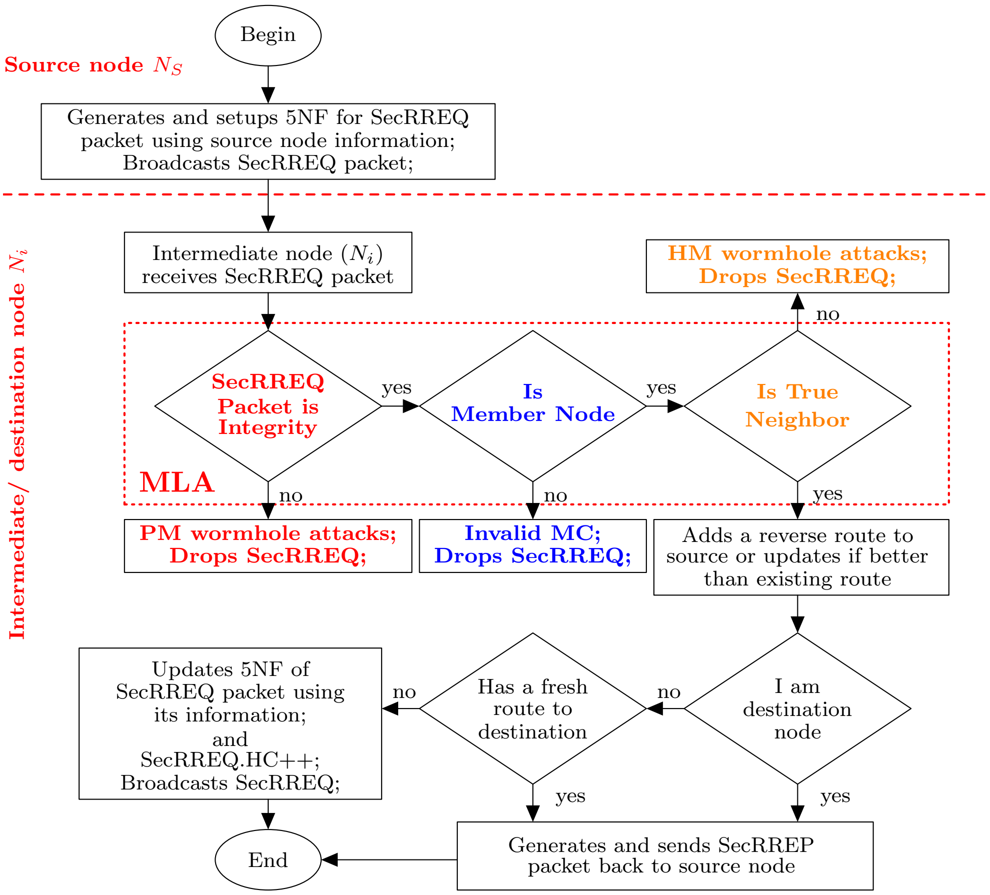

Begin
Source node N_S
Generates and setups 5NF for SecRREQ packet using source node information; Broadcasts SecRREQ packet;
Intermediate/ destination node N_i
Intermediate node (N_i) receives SecRREQ packet
HM wormhole attacks; Drops SecRREQ;
no
SecRREQ Packet is Integrity
yes
Is Member Node
yes
Is True Neighbor
MLA
no
no
yes
PM wormhole attacks; Drops SecRREQ;
Invalid MC; Drops SecRREQ;
Adds a reverse route to source or updates if better than existing route
Updates 5NF of SecRREQ packet using its information; and SecRREQ.HC++; Broadcasts SecRREQ;
no
Has a fresh route to destination
no
I am destination node
yes
yes
End
Generates and sends SecRREP packet back to source node

Figure 3. MLAMAN route request algorithm

3.2.2. Unicasting route reply phase

a) Generating SecRREP packet: Figure 4 describes route reply packet algorithm using the MLA mechanism. A node generates a SecRREP packet if it is either the destination (N_D) or an intermediate (N_i) which has a "fresh" route to the destination as in (5).

$$N_D(orN_i)unicasts : SecRREP \leftarrow \{RREP^* \oplus 5NF\} \tag{5}$$

Where $RREP^*$ is the original RREP packet of the AODV routing protocol and 5NF is five new fields of the SecRREP. These new fields contain the following information:

- SecRREP.GPS = N_D (or N_i) node GPS information;
- SecRREP.R = 250 m;
- SecRREP.MC = N_D (or N_i) node MC;
- SecRREP.KEY = Public key $k_{N_D}+$(or $k_{N_i}+$);
- SecRREP.VC = Encryption of H(SecRREP.fields $\setminus$ {VC}) using $k_{N_D}-$ (or $k_{N_i}-$);

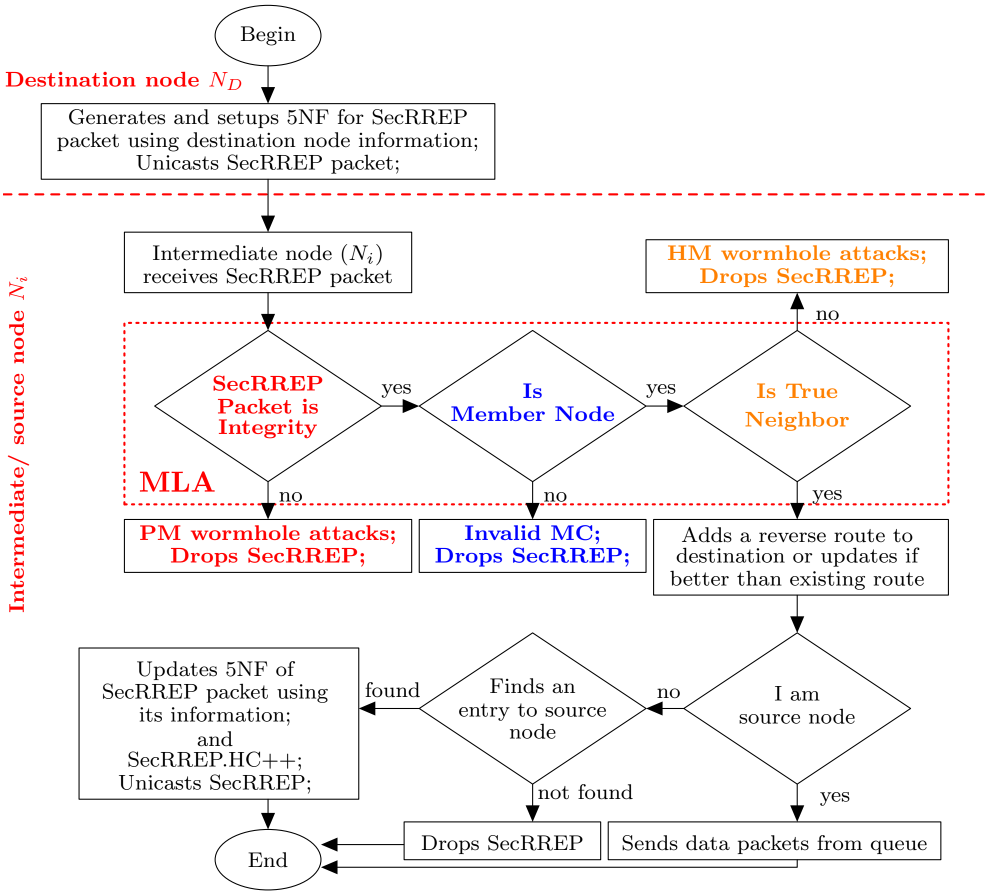

Begin
Destination node N_D
Generates and setups 5NF for SecRREP packet using destination node information; Unicasts SecRREP packet;
Intermediate/ source node N_i
Intermediate node (N_i) receives SecRREP packet
HM wormhole attacks; Drops SecRREP;
no
SecRREP Packet is Integrity
yes
Is Member Node
yes
Is True Neighbor
MLA
no
no
yes
PM wormhole attacks; Drops SecRREP;
Invalid MC; Drops SecRREP;
Adds a reverse route to destination or updates if better than existing route
Updates 5NF of SecRREP packet using its information; and SecRREP.HC++; Unicasts SecRREP;
found
Finds an entry to source node
no
I am source node
not found
yes
End
Drops SecRREP
Sends data packets from queue

Figure 4. MLAMAN route reply algorithm

b) Processing and forwarding SecRREP packet: When a node receives a SecRREP packet, the node drops the packet if it has not been certified, otherwise, it tests the integrity of the packet, verifies the node membership of the sending node, and determines if the sending node is a true neighbor according to the MLA mechanism.

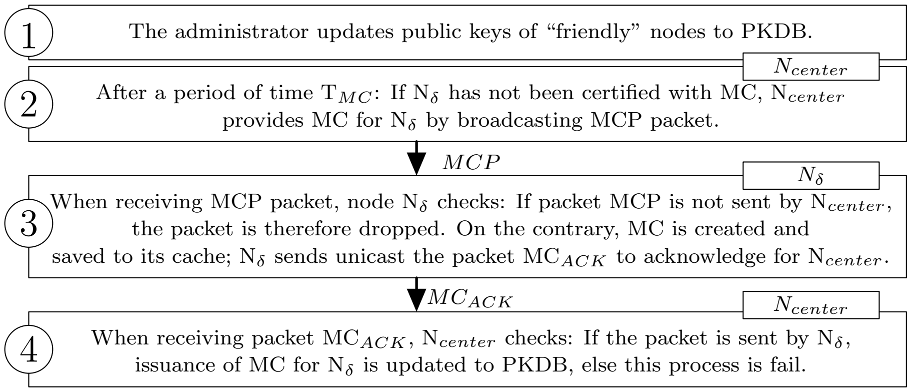
- If the integrity SecRREP packet is not verified, N_j drops the packet as the discovered route has been tampered by a malicious node under PM mode.

- If the SecRREP packet is not sent by a certified member node, N_j drops the SecRREQ packet;
- If the SecRREP packet is not sent by a true neighbor node, N_j drops the SecRREQ packet as the discovered route has been interfered by a malicious node under HM mode.

If all the conditions are satisfied, and the current node is the source node, it will send data packets to the destination node through the discovered route; otherwise, it updates a reverse route to the destination node and the 5NF of the SecRREP packet with the lastest information before sending the packet to the next hop the source node.

3.3. MLAMAN auxiliary protocol and procedure for providing node membership certificate

In a MLAMAN ad hoc network, any node can verify the certification of another node and only certified nodes can participate in the route discovery process. Figure 5 shows the procedure for providing the MC to member nodes. The MLAMAN administrator possesses a database of public keys (the PKDB) of all possible nodes that can join the ad hoc environment. Any node in the PKDB can be designated as the N$_{center}$ node. Some nodes in the PKDB may have already had their membership certified by the N$_{center}$ and some are yet to be certified. Periodically after T_{MC} time interval, N$_{center}$ checks the PKDB to see if all members have been provided with a membership certificate (MC). If node (N$_\delta$) is not yet provided with an MC, N$_{center}$ broadcasts a membership certificate packet (MCP) to for the destination N$_\delta$. On receiving the MCP, node N$_\delta$ sends an MC$_{ACK}$ packet back to the N$_{center}$ to confirm that it receives the MC. The procedure requires a PKDB and an auxiliary protocol for granting certificates to members of PKDB.



The administrator updates public keys of "friendly" nodes to PKDB.

After a period of time T$_{MC}$: If N$_\delta$ has not been certified with MC, N$_{center}$ provides MC for N$_\delta$ by broadcasting MCP packet.

When receiving MCP packet, node N$_\delta$ checks: If packet MCP is not sent by N$_{center}$, the packet is therefore dropped. On the contrary, MC is created and saved to its cache; N$_\delta$ sends unicast the packet MC$_{ACK}$ to acknowledge for N$_{center}$.

When receiving packet MC$_{ACK}$, N$_{center}$ checks: If the packet is sent by N$_\delta$, issuance of MC for N$_\delta$ is updated to PKDB, else this process is fail.

Figure 5. The process provides MC for member nodes

3.3.1. The Public Key Database

The administrator sets up a reliable node named N$_{center}$ to provide MC for members. In N$_{center}$, a public key database (PKDB) of all nodes is created with the structure shown in Table 2. Each record in the PKDB consists of: node address (Nodes), node public key (Key+), and node MC status. Where, two Nodes and Key+ attributes are updated directly by administrators to ensure that only legitimate nodes are provided with MC.

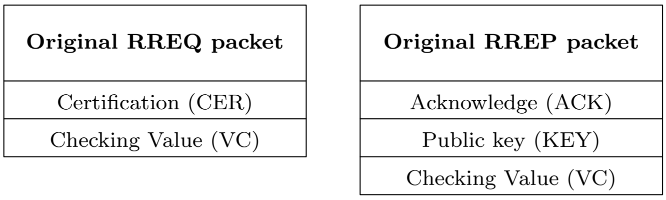
Table 2. Public key database structures

Nodes	**Key+**	**Completed**
IP_{N_1}	$k_{N_1}+$	yes
IP_{N_2}	$k_{N_2}+$	yes
IP_{N_3}	$k_{N_3}+$	no
...	...	...
IP_{N_n}	$k_{N_n}+$	yes

3.3.2. MLAMAN membership certification protocol

a) Broadcasting MCP packet and saving MC

N$_{center}$ provides MC for a member node N$_{\delta}$ by broadcasting a MCP packet. This protocol is again an enhanced protocol of AODV for broadcasting the RREQ packet. The structure of the MCP packet is similar to that of the RREQ packet and includes two new fields (2NF): *CER* and *VC*, as described in Figure 6(a).



(a) MCP

(b) MC$_{ACK}$

Figure 6. The control packet structures of membership certification protocol

Generating MCP packet: Periodically after T$_{MC}$ time interval, N$_{center}$ checks to see if all node members are provided with an MC by broadcasting the MCP packet to all its neighbors as in (6).

$$N_{center} broadcasts : MCP \leftarrow \{RREQ^{*} \oplus 2NF\} \tag{6}$$

Where $RREQ^{*}$ is the original RREQ packet of the AODV routing protocol and 2NF is two new fields of the MCP packet. The new fields contain the following information: the CER field as calculated by (7) and the packet integrity VC field.

$$MCP.CER = En(En(H(IP_{N_\delta}, k_{N_\delta}+), k_{N_{center}}-), k_{N_\delta}+) \tag{7}$$

Processing and forwarding MCP packet: When a node receives a MCP packet, it tests the integrity of the packet. If all the conditions are satisfied, and receiving node is the destination, it just simply saves the MC into cache and sends an MC$_{ACK}$ packet back to the N$_{center}$; otherwise, it updates a reverse route toward the source node and broadcasts the MCP packet to its neighbors. Algorithm 4 shows the procedure for testing and saving the Member Certification at a N$_\delta$ node. When N$_\delta$ receives the MCP packet, it tests the integrity of the packet and whether the MCP is sent by the N$_{center}$ node. If all the conditions are satisfied, N$_\delta$ saves the MC in its cache and unicasts the MC$_{ACK}$ packet to confirm its certified status to the N_{center}; otherwise, the packet is dropped.

Algorithm 4 Testing and saving Member Certification

Input: MCP packet; Output: True if MCP is valid; Else return False

```
function BOOLEAN TESTANDSAVEMC(Packet P)
    Begin
        If Not IsPacketIntegrity(P, $k_{N_{center}}+$) Then Dispose(P) and Return False;
        $val1 \leftarrow De(P.CER, k_{N_\delta}-)$; //Now val1 equal $En(H(IP_{N_\delta}, k_{N_\delta}+), k_{N_{center}}-)$;
        $val2 \leftarrow De(val1, k_{N_{center}}+)$;
        If $val2 \neq H(IP_{N_\delta}, k_{N_\delta}+)$ Then Dispose(P) and Return False;
        Else
            $MC \leftarrow En(val1, k_{N_\delta}-)$; //Now MC value as formula 2
            SaveToCache(MC);
            Generating and Replying the MC$_{ACK}$ packet back to $N_{center}$;
            Return True;
    End
```

b) Replying the MC$_{ACK}$ packet

A certified member node N$_\delta$ is required to send a MC$_{ACK}$ packet back to confirm its status to the Ncenter. The procedure is similar to the procedure for unicasting the RREP packet of the AODV. The structure of MC$_{ACK}$ packet is similar as RREP packet and includes three new fields (3NF): ACK, KEY and VC. The ACK field is calculated by (9), the KEY value is the public key of N$_\delta$ and VC field is the packet integrity.

Generating MC$_{ACK}$ packet: After saving the MC successfully, the node N$_\delta$ unicasts the confirmation packet MC$_{ACK}$ to back to the N_{center} as in (8).

$$N_\delta unicasts : MC_{ACK} \leftarrow \{RREP^* \oplus 3NF\} \tag{8}$$

Where $RREP^*$ is the original RREP packet of AODV routing protocol and extended with the three new fields as described in Figure 6(b).

$$MC_{ACK}.ACK \leftarrow En(En(H(IP_{N_{center}}), k_{N_\delta -}), k_{N_{center}}+) \tag{9}$$

Processing and forwarding MC$_{ACK}$ packet: When a node receives a MC$_{ACK}$ packet, it tests the packet integrity. If all the conditions are satisfied and the receiving node is the source, the node just simply updates the successfully provided MC to the N$_{center}$; otherwise, the packet is dropped. Algorithm 5 shows the steps for testing and saving the acknowledgement at the N$_{center}$ node. When the N$_{center}$ receives an MC$_{ACK}$ packet, it tests the integrity of the packet and whether the MC$_{ACK}$ is sent by the N$_\delta$ node. If all the conditions are satisfied, the N$_{center}$ updates the confirm status of the node in the PKDB; otherwise, the packet is dropped.

Algorithm 5 Testing MC$_{ACK}$ packet and updating PKDB

Input: MC$_{ACK}$ packet; Output: True if MC is saved successful; Else return False

```
function BOOLEAN TESTMC_ACK(Packet P)
    Begin
        //P.KEY is $k_{N_\delta}+$
        If Not IsPacketIntegrity(P, P.KEY) Then Dispose(P) and Return False;
        $val1 \leftarrow De(P.ACK, k_{N_{center}}-)$; //Now $val1$ equal $En(H(IP_{center}), k_{N_\delta}-)$;
        $val2 \leftarrow De(val1, P.KEY)$;
        If $val2 \neq H(IP_{N_{center}})$ Then Dispose(P) and Return False;
        If (IP$_{N_\delta}$ exists in PKDB) Then
            PKDB.Rows[IP$_{N_\delta}$].Completed ← Yes;
            Return True;
        Else
            Dispose(P) and Return False;
    End
```

4. MLAMAN Simulation Results and Performance Analysis

Using NS2 version 2.35, we simulate MLAMAN and evaluate its performance. The simulation area was a 2000 m X 2000 m square region, large enough to accommodate an ad hoc network with multiple hops. The simulation time was set at 1000 seconds, long enough for the simulated network to settle down beyond its initial and transitional state.100 normal and 2 malicious nodes were generated for the simulation and 802.11 was used for wireless transmission. A source node sent out constant bit rate (CBR) traffic with packet sizes of 512bytes at a rate of 2 packets per second. FIFO was used for packet queueing. Table 3 tabulates relevant simulation parameters.

Table 3. Simulation parameters

Parameters	**Setting**
Simulation area	2000 x 2000 (m^2)
Simulation times	1000 (s)
Number nodes	102 (2 malicious nodes)
Maximum radio range (R)	250 (m)
Traffic type	CBR
Transport protocol	UDP
Data rate	2 packets per seconds
Packet size	512 bytes
Queue type	FIFO (DropTail)
Routing protocols	AODV and MLAMAN
Hash function (H)	SHA_1
Prime (p, q)	29, 31
T$_{MC}$	10 (seconds)

4.1. Wormhole Detection Performance

We evaluate the wormhole detection performance of the proposed MLAMAN based on tunnel length and mobility speed metrics. Wormhole detection ratio (WDR) is defined as eqn 10.

$$WDR = (1 - \frac{FalsePositive + NegativesInstances}{TotalSevRREQ + SecRREP}) * 100\% \tag{10}$$

There are 32 scenarios are simulated, each involves 100 normal mobile nodes and 2 malicious nodes. Nodes move in a Random Way Point [26] pattern with a specified maximum speed (MS). Maximum speeds are set at 0, 10, 20 and 30 m/s. 40 pairs of communicating nodes are set up with the source nodes in blue and destination nodes in red. Sources send data at 5 seconds apart from one another, with the first at time zero. Two malicious nodes are positioned near the center of the network with TL (tunnel length) hops between them. TL is set at 1, 2, 3, and 4 hops for various simulations. The hop distance is set at 250m for the network topology shown in Figure 7.

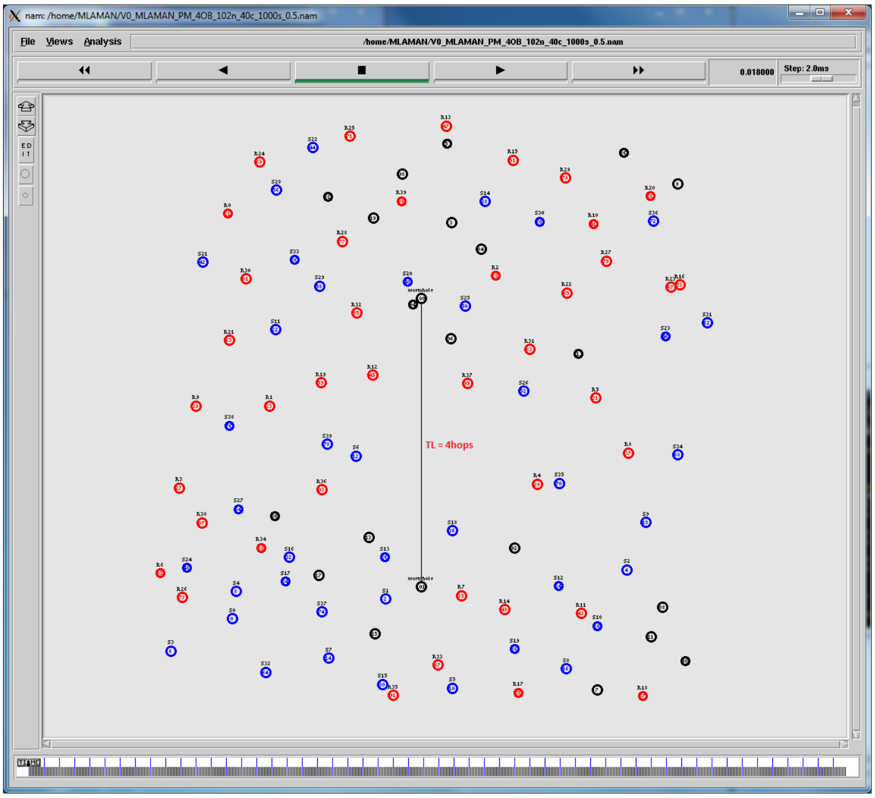

nam: /home/MLAMAN/V0_MLAMAN_PM_4OB_102n_40c_1000s_0.5.nam
File
Views
Analysis
/home/MLAMAN/V0_MLAMAN_PM_4OB_102n_40c_1000s_0.5.nam
0.018000
Step: 2.0ms
wormhole
TL = 4hops
wormhole

Figure 7. Network topology simulation, 40UDPs connections and Wormhole nodes using 4hops tunnel length

Simulation results in Figure 8 show that MLAMAN has a 100% the successful detection rate in detecting invalid control route packets for static, stationary network topology where nodes do not move, and over 99.9% detection rate for all mobile scenarios. Under the PM mode during the route discover process, wormhole nodes process control packets just like other normal nodes, MLAMAN detects invalid control route packets (SecRREQs or SecRREPs forwarded by wormhole nodes) by verifying the integrity of these packets using the packet integrity authentication algorithm. Under the HM mode, malicious nodes, on receiving the control packets, simply forwards them to others without processing packet, hence, packet integrity verification and node membership authentication are no longer useful. In this case, MLAMAN detects wormhole node by performing the actual neighbor authentication algorithm at the receiving node to determine if the received SecRREQ (or SecRREP) packet is forwarded by a wormhole node. The weakness of MLA is the actual neighbors authentication using node location to detect malicious node, thus, it can be mistaken in mobility network topology at high speeds.

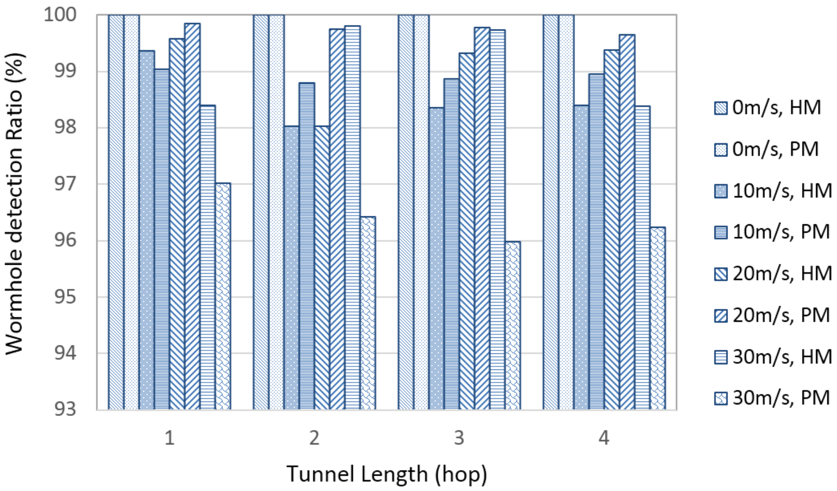


Figure 8. Wormhole detection performance for MLAMAN based on Tunnel Length and Mobility Speed metrics, 40UDPs connections

In this section, we simulate MANETs under different traffic conditions and tunnel lengths and evaluate MLAMAN's performance. Same as before, 32 scenarios are simulated, each has 100 normal mobile nodes and 2 malicious nodes and all of nodes move randomly with a maximum speed of 20 m/s. Traffic conditions range from light to heavy and are represented by the number of UDP network connections (NCs) between source-destination node pairs from 10 for light traffic to 40 for heavy traffic. Other parameters remain the same as described in Table 3. Simulation results in Figure 9 show that MLA has PM wormhole node detection effectuation is better than HM wormhole node. The successful detection ratio over 98.03% of wormhole nodes using both of HM and PM modes for all simulation scenarios. With TTHCA, the detection performance is excellent for long tunnels, but it degrades to less than 90% [12] when the tunnel length is less than 5 due to the difficulty in measuring short the packet transversal times. This fact also implies that TTHCA may not perform well when nodes are moving at various speeds. The detection results in simulation results in Figure 8 and Figure 9 confirm that MLA outperformed TTHCA and other methods [9][12] for short tunnel length and high mobility speed simulation scenarios.

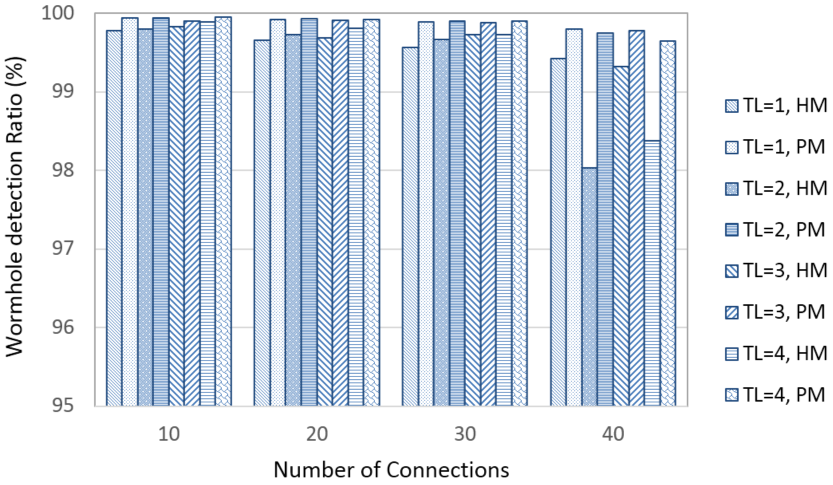


Figure 9. Wormhole detection performance for MLAMAN based on Number UDP connection and Tunnel Length metric, 20m/s mobility speeds maximum

4.2. Packet overhead and Packet delivery ratio

In this section we analyze the packet overhead (PO) for providing the node membership certification and the packet delivery ratio (PDR) in a normal network topology as shown in eqn 11 and 12.

$$PO = \text{Total of } MCP + MC_{ACK} \tag{11}$$

$$PDR = (\frac{\text{Number of packets delivered successfully}}{\text{Total of packtes are sent from source}}) * 100\% \tag{12}$$

Four specific scenarios are simulated, has all of them assume 20 pairs of communicating nodes with the first source node sending data at time zero and the rest sending data at 5-second intervals.

The first scenario simulates AODV protocol for 100-node MANET. The second scenario simulates MLAMAN for 100-node MANET and used with 100 member nodes in the PKDB database;

The third scenario simulates MLAMAN for100-node MANET with 80 member nodes from 0 to 79 identified in PKDB;

The fourth scenario simulates MLAMAN for 100-node MANET with 80 member nodes from 0 to 79 identified in PKDB and 20 new member nodes are installed into PKDB at 200th seconds.

Figure 10 shows that MLAMAN requires 80 seconds and an overhead of 19,645 of packets (CMP and MCACK) to provide MC for all 100 member nodes listed in the PKBD database. The overheads are 70 seconds and 18,056 packets for 80 member nodes. For the fourth scenario, total packet overhead of MLAMAN is 20,412 packets and 230 seconds for completing the member certification process.

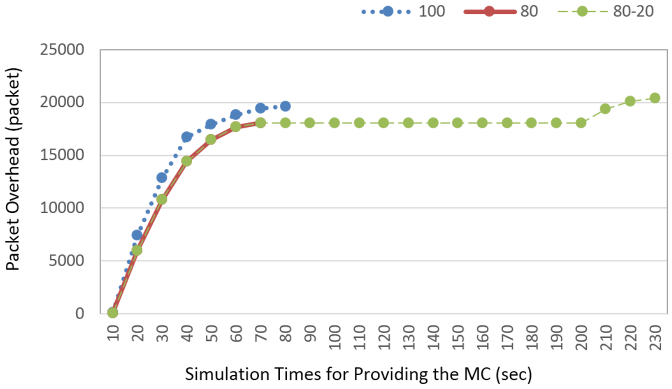


Figure 10. Packet overhead of MLAMAN protocol to provide MC for member nodes

Figure 11 shows that the packet delivery ratio of AODV is better than MLAMAN with all member nodes listed in the PKBD. With MLAMAN, most of the nodes cannot participate in the route discover process at the early stage of the operation as they have not yet been certified and hence packets cannot be delivered to their destination. As time progresses, more and more nodes are certified resulting in higher number of successful packet delivery. The MC process completes after 80 seconds providing all listed member nodes are operational. At the end of the simulation, the PDR for MLAMAN is 59.13% compared to 72.94% for the AODV for this scenario. With the scenario where 80 member nodes are installed in PKBD, PDR of MLAMAN is reduced to 23.89% due to the fact that around 50% of the destination nodes was not in PKDB. Final scenario, PDR for MLAMAN is improved to 52.1% eventually as 20 new member nodes are added into PKDB at time 200s.

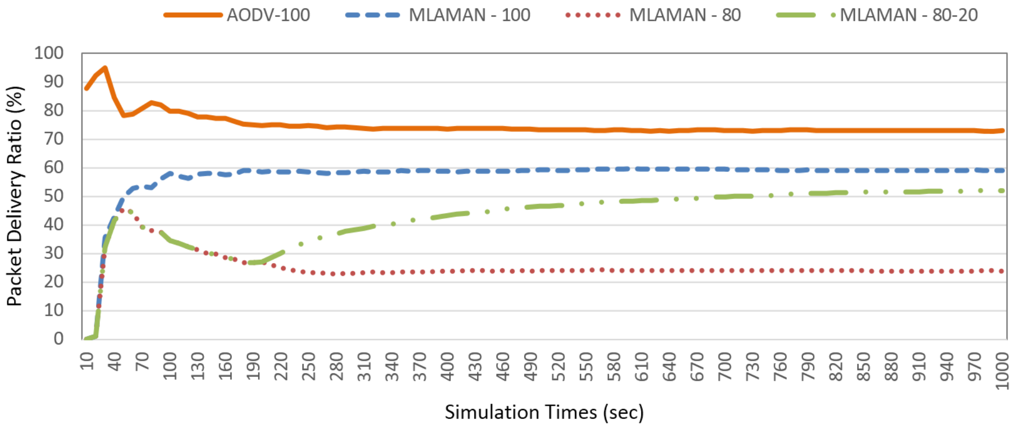


Figure 11. Comparison of packet delivery ratio of AODV and MLAMAN protocols in normal network topology

4.3. Route Discovery Time

To evaluate the route discovery time of MLAMAN compared to the original AODV protocol. MLAMAN requires every mobile nodes, on a hop-by-hop basis, to test the integrity of the control packets SecRREQ and SecRREP, verify the membership of the sending nodes as well as their neighborhood status for wormhole detection, it is expected that the route discovery time of MLAMAN be higher than that of AODV. The simulation results in Figure 12 are based on the average route discovery delay for scenario using 100 normal mobile nodes. It is clear that when the network traffic increases the route discovery time increases.

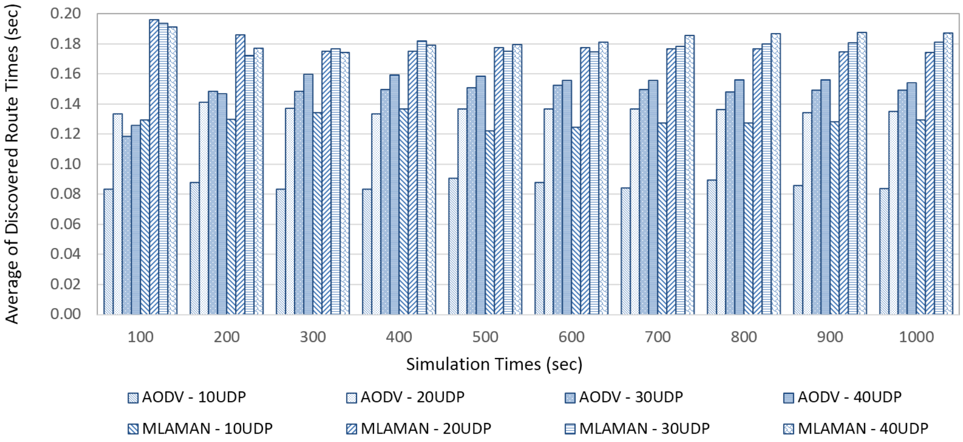


Figure 12. Route discovery delay of AODV and MLAMAN protocols in normal network topology

5. Conclusions and Future Works

We proposed MLAMAN, a novel model that deployed multi-level authentication and routing protocol to prevent wormhole attacks in MANETs. MLAMAN verifies the integrity and the authenticity of a routing control packet on a hop-by-hop basis. It also utilizes positioning information of the sending and receiving nodes to judge their neighborhood relationship. Simulation results demonstrated that the MLAMAN was very robust against wormhole attacks. For a static network topology, it was 100% successful in detecting wormhole attacks. For a dynamic and mobile topology where a minimum tunnel length of 1 hop and with a maximum node moving speed of 30 m/s it achieves a successful wormhole detection rate of over 95.98% in both Hidden and Participation Modes. To support MLAMAN, a management protocol was introduced to provide node membership certification to prevent malicious nodes from joining the network with the fake keys.

Our next step is to setup MLAMAN with large key to improve the security performance using TLS library [17] and evaluate the security capability of MLAMAN through comprehensive simulations, taking into account practical scenarios including network sizes and node's speeds.

REFERENCES

[1] H. Chiu and K. Wong Lui, “DelPHI: Wormhole detection mechanism for Ad hoc Wireless Networks,” in *International Symposium on Wireless Pervasive Computing Proceedings*, 2006, pp. 6 – 11.

[2] W. Diffie, W. Diffie, and M. E. Hellman, “IEEE Transactions on Information Theory,” vol. 22, no. 6, 1976, pp. 644 – 654.

[3] A. Eiman and M. Biswanath, “A survey on routing algorithms for Wireless Ad-Hoc and Mesh Networks,” *Computer Networks*, vol. 56, no. 2, pp. 940 – 965, 2012.

[4] S. Gurung and S. Chauhan, “A novel approach for mitigating gray hole attack in MANET,” *Wireless Networks*, pp. 1 – 15, 2016.

[5] J. Hoebeke, I. Moerman, B. Dhoedt, and P. Demeester, “An overview of Mobile Ad hoc Networks: applications and challenges,” *Journal of the Communications Network*, vol. 3, no. 3, pp. 60 – 66, 2004.

[6] Y. C. Hu, A. Perrig, and D. B. Johnson, “Packet leashes: A defense against wormhole attacks in Wireless Networks,” in *IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE Cat. No.03CH37428)*, vol. 3, 2003, pp. 1976 – 1986.

[7] T. Issariyakul and E. Hossain, *Introduction to Network Simulator NS2.* Springer, 2009.

[8] V. M. Jan, W. Ian, and K. S. Winston, “Security threats and solutions in MANETs: A case study using AODV and SAODV,” *Journal of Network and Computer Applications*, vol. 35, no. 4, pp. 1249 – 1259, 2012.

[9] S. M. Jen, C. S. Laih, and W. C. Kuo, “A Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANET,” *Sensors*, vol. 9, no. 6, pp. 5022 – 5039, 2009.

[10] D. B. Johnson and D. A. Maltz, *Dynamic Source Routing in Ad Hoc Wireless Networks.* Boston, MA: Springer US, 1996, pp. 153–181.

[11] P. Jones. US secure hash algorithm 1 (SHA1). [Online]. Available: https://tools.ietf.org/html/rfc3174

[12] J. Karlsson, L. S. Dooley, and G. Pulkkis, “A New MANET Wormhole Detection Algorithm Based on Traversal Time and Hop Count Analysis,” *Sensors*, vol. 11, no. 12, pp. 11 122 – 11 140, 2011.

[13] ——, “Identifying Time Measurement Tampering in the Traversal Time and Hop Count Analysis (TTHCA) Wormhole Detection Algorithm,” *Sensors*, vol. 13, no. 5, pp. 6651–6668, 2013.

[14] S. Khurana and N. Gupta, “End-to-end protocol to secure ad hoc networks against wormhole attacks,” *Security and Communication Networks*, vol. 4, no. 9, pp. 994 – 1002, 2011.

[15] L. Lazos, R. Poovendran, C. Meadows, P. Syverson, and L. W. Chang, “Preventing wormhole attacks on Wireless Ad hoc Networks: A graph theoretic approach,” in *IEEE Wireless Communications and Networking Conference, 2005*, vol. 2, 2005, pp. 1193 – 1199.

[16] L. Lazos and R. Poovendran, “SeRLoc: Secure Range-independent Localization for Wireless Sensor Networks,” in *Proceedings of the 3rd ACM Workshop on Wireless Security*, 2004, pp. 21 – 30.

[17] T. library. RSA source code. [Online]. Available: https://tls.mbed.org/rsa-source-code

[18] G. Z. Manel, “Secure Ad Hoc On-demand Distance Vector Routing,” *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 6, no. 3, pp. 106 – 107, 2002.

[19] E. C. Ngai, J. Liu, and M. R. Lyu”, “An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks,” *Computer Communications*, vol. 30, no. 11, pp. 2353 – 2364, 2007.

[20] L. T. Ngoc and V. T. Tu, “Whirlwind: A new method to attack Routing Protocol in Mobile Ad hoc Network,” *International Journal of Network Security*, vol. 19, no. 5, pp. 832 – 838, 2017.

[21] C. E. Perkins and E. M. Royer, “Ad-hoc On-Demand Distance Vector Routing,” in *Proceedings of the Second IEEE Workshop on Mobile Computer Systems and Applications*, 1999, pp. 90 – 100.

[22] R. D. Pietro, S. Guarino, N. Verde, and J. Domingo-Ferrer, “Security in Wireless Ad-hoc Networks - A survey,” *Computer Communications*, vol. 51, pp. 1 – 20, 2014.

[23] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, “A secure routing protocol for Ad hoc Networks,” in *10th IEEE International Conference on Network Protocols, 2002. Proceedings*, 2002, pp. 78 – 87.

[24] R. Thillaikarasi and S. M. S. Bhanu, “An Efficient DSR Protocol to Detect Blackhole Attacks in WMN Using Cross Layer Approach,” *Wireless Personal Communications*, 2017.

[25] V. T. Tu and L. T. Ngoc, “SMA$_2$AODV: Routing Protocol Reduces the Harm of Flooding Attacks in Mobile Ad Hoc Network,” *Journal of Communications*, vol. 12, no. 7, pp. 371 – 378, 2017.

[26] J. Yoon, M. Liu, and B. Noble, “Random waypoint considered harmful,” in *IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE Cat. No.03CH37428)*, vol. 2, 2003, pp. 1312 – 1321.

Authors information

Tu T. Vo is an associate professor in the Faculty of Information Technology, Hue University of Sciences, Hue University. He received B.E. degree in Physics from Hue University in 1987 and PhD degree in computer science from Institute of Information Technology, Vietnam Academy of Science and Technology in 2005. His fields of interesting are network routing, analysis and evaluation of network performance, security wireless Ad hoc Network.

Ngoc T. Luong is working in the Faculty of Mathematics and Informatics Teacher Education, Dong Thap University. He received B.E. degree in Computer Science from Dong Thap University in 2007 and M.A. degree in Computer Science from Hue University of Sciences in 2014. He is a PhD student in Hue University of Sciences now. His fields of interesting are analysis and evaluation of network performance, security wireless Mobile Ad hoc Network.

Doan Hoang is a Professor in the School of Computing and Communications, University of Technology Sydney (UTS). Doan’s research focuses on cyber security and quality of service of software-defined infrastructures (Software-Define Networks (SDN)), Cloud, and Internet of Things (IoT). In particular, his current research projects include: Resource optimization in SDN environment, Software-defined architecture for provisioning IoT applications on demand, Network Functions Virtualization (NFV), SDN and virtualization for Cyber Security, Security metrics and maturity models for Cloud, and Trust assessment model for Personal Space IOTs. He is also into establishing infrastructure for real-time accessing, distribution, and protection of big assistive healthcare data.