IEIE Transactions on Smart Processing and Computing, vol. 3, no. 5, October 2014
http://dx.doi.org/10.5573/IEIESPC.2014.3.5.298

MAC Layer Based Certificate Authentication for Multiple Certification Authority in MANET

J Chandra Sekhar and R Sivarama Prasad

Research Scholar, Department of Computer Science and Engineering, Acharya Nagarjuna University / Nagarjuna Nagar, Guntur, Andhra Pradesh, India jcsekhar9@gmail.com, raminenisivaram@yahoo.co.in

***** Corresponding Author: J Chandra Sekhar

Received January 15, 2014; Revised March 17, 2014; Accepted July 28, 2014; Published October 31, 2014

** Regular Paper*

***Abstract*:** In this study, a novel Randomly Shifted Certification Authority Authentication protocol was used in ad hoc networks to provide authentication by considering the MAC layer characteristics. The nodes achieve authentication through the use of public key certificates issued by a CA, which assures the certificate's ownership. As a part of providing key management, the active CA node transfers the image of the stored public keys to other idle CA nodes. Finally the current active CA randomly selects the ID of the available idle CA and shifts the CA ownership by transferring it. Revoking is done if any counterfeit or duplicate non CA node ID is found. Authentication and integrity is provided by preventing MAC control packets, and Enhanced Hash Message Authentication Code (EHMAC) can be used. Here EHMAC with various outputs is introduced in all control packets. When a node transmits a packet to a node with EHMAC, verification is conducted and the node replies with the transmitter address and EHMAC in the acknowledgement.

***Keywords*:** Authenticated group key agreement protocol, Enhanced hash message authentication code, Randomly shifted certification authority authentication protocol

1. Introduction

1.1 MANET

A Mobile Ad hoc Network (MANET) is a set of wireless mobile nodes that forms a temporary network without any centralized administration. This system is a collection of dynamic, independent, wireless devices that groups a communications network devoid of any backing of a permanent infrastructure. The ultimate goal of designing a MANET network is to make available a self-protecting, "dynamic, self-forming, and self-healing network" for the dynamic and non-predictive topological network.

The idea of a MANET is also called infrastructure-less networking, because the mobile nodes in the network dynamically establish routing among themselves to form their own network on the fly. According to the positions and transmission range, every node in MANET acts as a router that tends to move arbitrarily and is connected dynamically to form a network.

MANETs have applicability in several areas, such as in military applications where cadets relay important data of the situational awareness on the battleground, in corporate houses where employees or associates share information inside the company premises or in meeting halls, attendees using wireless gadgets participating in an interactive conference, critical mission programmers for relief matters in any disaster events, such as large scale mishaps, e.g., war or terrorist attacks, and natural disasters. These networks have also been used in private areas and home networking, "location-based" services, sensor networks and many more services based on MANET [1, 2].

Issues

- bandwidth limitations
- vibrant and non-predictive topology
- limited processing and minimum storage of mobile nodes

1.2 Authentication for MANET

Security in mobile ad hoc networks is difficult to achieve because of the vulnerability of the links, inadequate physical protection, the dynamically changing topology, and the sporadic nature of the connectivity. The dynamic change in topology results in a change in the trust relationships among the nodes.

Authentication plays an essential role and forms the basis of security in MANETs. In addition, it is provided with the authentication protocol. An authentication protocol involves a sequence of message exchanges that verify the identities of the nodes in a distributed system wishing to communicate. Authentication can be realized using either public or private key cryptography. This is of particular importance because it provides the first line of defense against attacks and forms the basis for achieving the other security goals of integrity and confidentiality. Public key cryptography (PKC) is accepted widely as an effective mechanism for providing fundamental security services, such as authentication, confidentiality, integrity and non-repudiation. PKC involves a trusted third party that holds the public key certificates acting as a certification authority (CA) [3].

Issues in providing authentication

- dynamic topology of the network
- frequent link failures
- node mobility
- limited wireless medium [4]

1.3 Need for MAC layer-based authentication in MANET

A medium access control (MAC) layer plays an important role in coordinating channel access among the nodes so that information is transferred from one node to another. The terms of security in mobile ad hoc networks are of vital importance because of their wireless nature. For ad hoc networks, it is essential to consider these in the context of the overall system. Therefore MAC should be taken into consideration. The nodes in an ad hoc network need to strictly obey the rules of the MAC to transmit security-related messages while still maintaining the necessary quality of service (QoS) [3].

Issues in MAC layer authentication

i. Wireless channels are not as reliable as wired ones, suffering from path loss, fading, interference, and a limited usable bandwidth.
ii. Next according to its name, a MANET is composed of a number of nodes that can move around.
iii. Consequently, the network topology can experience continuous change and cause frequent route breakages and re-routing activity.
iv. MANETs by nature are self-organized, self-controlled and distributed [5].

In our previous work [15], novel security architecture for MANET for trust and authentication was designed. Here, multiple paths are established based on AOMDV. Next, trust and reputation management is applied using the local and global reputation values. A standard authentication scheme for MANETs using Threshold Secret Sharing is proposed. This provides security inside a network, allowing only legitimate users to utilize the network. In this algorithm, multiple Certification Authority (CA) nodes are selected based on the evaluated reputation index, transmission power and mobility.

In the second part of this study, a certificate exchange and revocation mechanism for multiple Certification Authority (CA) nodes is proposed. Here, using a cluster based certificate revocation scheme, the nodes are classified into three different categories normal nodes, warned nodes and attacker nodes. Next, to provide authentication between the clusters heads, an ID based one round authenticated group key agreement protocol (AGKA) is used. For key authentication, a pair-wise key is calculated by the ephemeral and long-term private keys of each CH. The proposed schemes provide some measure of protection against malicious accusation, succeeding in causing the revocation of the certificates of trustworthy, well-behaving nodes.

From an analysis of the existing studies related to certificate exchange and revocation in MANET, it is clear that only few certificate-based mechanisms can consider the MAC protocols. On the other hand, they did not combine the certificate authentication with the MAC layer characteristics.

As an extension of this work, this study considered the constraints of MANET along with the MAC layer-related characteristics for the development of CA-based authentication and revocation protocols, and proposed a MAC layer-based certificate authentication for multiple certification authority in MANET.

2. Related Work

R. Murugan and A. Shanmugam [1] developed a combined solution for routing and MAC layer attacks. This makes use of three techniques simultaneously, which consists of a cumulative frequency-based detection technique for detecting MAC layers attacks, a data forwarding behavior-based detection technique for detecting packet drops and a message authentication code-based technique for packet modification. This solution presents a reputation value for detecting malicious nodes and isolates them from further network participation until its revocation. This approach has fewer overheads compared to the existing technique.

G.A. Safdar and M. McLoone [3] proposed a novel Randomly Shifted Certification Authority authentication protocol (RASCAAL) for ad hoc networks. RASCAAL employs a trusted third party for authentication purposes, which holds the public key certificates and acts as a certification authority (CA). This system has been developed to consider the radio technology communication-related characteristics of the underlying IEEE 802.11 MAC for ad hoc networks. This is achieved by integration with the CSMA/CA medium access rules to enable the nodes to exchange securely messages for different transactions.

This property enhances the overall security of the communicating nodes significantly. The protocol design was verified formally using Burrows-Abadi-Needham (BAN) logic.

K.Suresh Babu and K.Chandra Sekharaiah [6] proposed CBDAT, a Cross layer-Based Detection and Authentication Technique for MANET. This technique defines the observer node to monitor the neighbor transmissions and calculate the trust values. The observer node is elected considering the residual energy, node degree and stability information. The trust value is protected using message authentication code (MAC). While transmitting data in the selected path, the MAC grants more access time for those nodes with a high trust value. This technique proficiency precludes more security attacks and improves the system performance but packet drop occurs.

Gulshan Kumar and Mritunjay Rai [7] designed the Assured Neighbor based Counter Protocol, which gives confidentiality, authentication and data integrity using a parallel approach of routing packets on the MAC Layer in MANETs. The protocol is divided into two phases where the first phase assures the isolation and detection of malicious nodes based on the routing layer information. A certain threshold level is defined with a certain value. The trust counter for each node maintains the trust value based on whether the counter value increases or decreases depending on the threshold value that decides whether the node is malicious or not. In the second phase, they provide the security on the Link layer using the COUNTER mode to provide authentication, integrity and encryption. This protocol achieves a high packet delivery ratio corresponding to various attackers. On the other hand, the reliability of the particular node cannot be assured.

Alejandro Cornejo et al, [8] described a protocol for learning about the neighboring nodes in a network environment. The protocol is used to establish and tear down the communication links with neighboring nodes as they move from one region of the network to another. The protocol is implemented on top of the abstract MAC layer service presented, which provides reliable message delivery within the local neighborhood and also provides the sender with an acknowledgment when all neighboring nodes have received a message. On the worst case delay, there is an upper bound guaranteed by the abstract MAC layer service that a message can experience before it is received or acknowledged. They determine the time complexity of the neighbor discovery protocol in terms of the bounded delays provided by the underlying abstract MAC layer but message loss occurs.

Gaurav Kulkarni and Brajesh Patel [9] developed a Cross layer timestamp-based network security technique. The technique reduces the encryption packet overflow, which is due to PKE or public key exchange and derives the public key directly from the neighbor's table, which is transmitted using the routing information exchange. The energy overhead due to encryption or performance compromise are quite low in the proposed system. In addition, as the protocol is embedded in the network layer, it is easily adaptable to any existing architecture without modifying the MAC or physical layer standard or protocol but the energy consumption is high.

T.R.Panke [11] proposed a clustering-based certificate revocation scheme for fast certificate revocation in MANET. A threshold based mechanism was used to restore the accusation function of the nodes in the WL and solve the issue of the number of normal nodes being reduced gradually. The effectiveness of this scheme was demonstrated by extensive simulation results. On the other hand, the simulation results did not analyze its robustness or its cost in terms of overhead and throughput.

Priti Rathi and Parikshit Mahalle [12] reported a threshold based certificate revocation scheme in MANETs. This scheme can revoke the certificate of malicious nodes when the first misbehavior of the nodes is detected. The improper certificate revocation, which occurs due to false accusations made by malicious node, is solved. In addition, the problem of window of opportunity is solved, in which the revoked certificates are assigned as a valid to new nodes. On the other hand, the computational cost in low-powered wireless nodes can be prohibitive. This scheme requires the unselfish cooperation of the communicating peers, which is not possible in certain network environments.

T.Buvaneswari and A. Antony Truth Ayaraj [13] proposed a novel accuser of security-based certificate revocation in MANET. In certificate accusation and recovery mechanisms, the number of nodes capable of accusing malicious nodes decreases with time. The threshold based approach is used to enhance the effectiveness and efficiency. This scheme can improve the reliability and accuracy while providing security.

A.Praveena and L.M.Nithya [14] addressed the problem of ensuring secure communications in MANETs and proposed a CCRVC scheme. This scheme combines the merits of both the voting-based mechanism and non-voting-based mechanism to eliminate the malicious certificate and the problem of false accusation. This can remove an accused node based on the single nodes accusation and minimize the cancellation time compared to voting-based mechanism. The cluster-based model is used to replace the falsely accused nodes by the cluster head to provide higher accuracy compared to the non-voting-based mechanism. A new motive method releases and replaces the legitimate nodes to refine the number of available normal nodes in the network. This scheme is more efficient in canceling the certificates of malicious attacker nodes, reducing the cancellation time and improving the validity of certificate revocation.

3. Proposed Solution

3.1 Overview

The Novel Randomly Shifted Certification Authority Authentication protocol was used for ad hoc networks to provide authentication by considering the MAC layer characteristics. The Nodes achieve authentication using public key certificates issued by a CA, which assures the certificate's ownership.

Here, the MAC protocol provides a CA node with

Table 1. Notations used in this paper.

Notation	Usage
CA_i	CA node
Nj	Non-CA node
$CAid_i$	CA node's ID
Nid_j	Non-CA node's ID
TS_i	Time stamp value
H	Hash value
$CApub_i$, $CApri_i$	CA node's public and private key
Npubi, Nprii	Non-CA node's public and private key
E-PRI	Encrypted with private key (CA/non-CA nodes)
BCAST_COUNT	Broadcast count value

prioritized access to the medium to transmit an active message in the management frame. To help provide key management, the active CA node transfers the image of the stored public keys to other idle CA nodes. Here, the transaction is carried out by a public key. Finally the current active CA randomly selects the ID of the available idle CA and shifts the CA ownership by transferring it. Revoking is done if any counterfeit or duplicate non CA node ID is found. Therefore, only the nodes possessing the relevant public key pairs can decrypt the messages.

Enhanced Hash Message Authentication Code (EHMAC) can be used to provide authentication and integrity in the form of preventing MAC control packets. Here, EHMAC with varying output is introduced in all control packets. When a node transmits a packet to a node with EHMAC, verification is done and it replies with the transmitter address and EHMAC in the acknowledgement. In such a way, the message is authenticated with the control of packets.

3.2 Randomly Shifted Certification Authority Authentication protocol (RSCAAP)

In the Randomly Shifted Certification Authority Authentication protocol (RSCAAP), the nodes achieve authentication using the public key certificates issued by a CA, which assures the certificate's ownership.

3.3 RSCAAP is explained in following steps

3.3.1 Initialization

As a part of the initialization, key management was provided for the protocol. The offline storage of all participating node public keys can be performed and the ACTIVE CA node can transfer the image of the stored public keys to other IDLE CA nodes upon request. To reduce the traffic in one CA, the number of public keys to be stored can be divided. Depending on the density of the non-CA nodes, keys up to a certain number can be stored per CA. On demand transfer of public keys can occur between both the ACTIVE_CA and other IDLE_CA nodes employing multi-hop operation in the network.

Dynamic key management can take place, where nodes can listen for an ACTIVE_CA_MESSAGE, and upload their public keys in a SEND_PUBLIC_KEY. RSCAAP does not require synchronization of the public key certificates maintained by the CA nodes. Hashing is employed in the RSCAAP protocol to provide message integrity. Keyed hashing can also be used to provide authentication of the nodes in addition to message integrity and the associated key can be stored in both the CA and non-CA nodes at the time of initialization [3].

Message 1: ACTIVE_CA_MESSAGE:

$$CA_i \rightarrow N_{(j---n)}, CA_{(i...n)} :$$
$$[CAid_i, CAid_{i-1}, CApub_i, TS_i, BCAST\_COUNT, H] \quad (1)$$

Message 2: SEND_PUBLIC_KEY:

$$N_j \rightarrow CA_i :$$
$$E[Nid_j, Npub_j, TS_i, H]\, CApub_i \quad (2)$$

In (1) and (2), Ts is the time stamp value and H is the hash of the message for integrity checking. The PUB specifies the public key (CA or non-CA node). In (1), $CAID_i$ is the ID of the current ACTIVE CA to which the ownership has been transferred from CA_{i-1}; hence, CAi forms the new cluster for the current transaction. IDLE_CA and non-CA nodes can identify the current ACTIVE_CA from the ACTIVE_CA_MESSAGE. BCAST_ COUNT is incremented each time the message is rebroadcast by other intermediate IDLE_CA nodes up to a maximum value (Normally equal to the number of CA nodes in the network) to limit the number of rebroadcasts; all intermediate IDLE_CA nodes must concatenate their IDs in the message before rebroadcasting.

3.3.2 Public Key Request/Reply and Secure Transaction

Any non-CA node that wishes to communicate with another node requests the public key of the destination node from the current ACTIVE_CA in a PUBLIC KEY at the end of initialization. The protocol assumes that at least one of the non-CA nodes is in the range of a current ACTIVE_CA node so that it can initiate secure communication with another non-CA node. The ACTIVE_CA will either have the required public key certificate itself or can request it from other IDLE_CA nodes, and will complete the transaction by the transmission of a PUBLIC_KEY_REPLY, as shown below [3].

Message 3: PUBLIC KEY REQUEST:

$$N_j \rightarrow CA_i :$$
$$E[Nid_j, Nid_{j+1}, TS_i, E(Nid_j, Nid_{j+1}, TS_i)Npri_j]CApub_i \quad (3)$$

Message 4: PUBLIC KEY REPLY:

$$CA_i \rightarrow N_j :$$
$$E[Npub_{j+1}, TS_i, CAid_i, H]Npub_j \quad (4)$$

In Eqs. (3) and (4), N_j is the node requesting the N_{j+1} public key and $NPRI_j$ is the node. N_j's private key, N_j, can successfully initiate a secure transaction with N_{j+1} using its public key. A message "X" can be sent in a SECURE_TRANSACTION_MESSAGE, as described in (5) by node Nj to node N_{j+1}, in which N_j also supplies its public key for two way communication.

Message 5: SECURE TRANSACTION MESSAGE:

$$N_j \rightarrow N_{j+1} : [Npub_j, TS_i, X] \text{ E-Npub}_{j+1} \quad (5)$$

3.3.3 CA Ownership Transfer

The current ACTIVE_CA randomly selects the ID of any other available IDLE_CA and shifts the CA ownership by a TRANSFER_CA_OWNERSHIP message in the end of a successful transaction. If there is inactivity in the channel due to no communication between the nodes, the current ACTIVE_CA waits for the time period of TRANSFER_CA_OWNERSHIP frame + 2 * max IEEE 802.11 MAC frame. When the ownership has transferred to ACTIVE_CA, it announces that there is inactivity in the channel with no communication between the nodes. This results in the formation of a temporary cluster with a randomly selected cluster head for duration equal to the current transaction. The broadcast nature of the message and the presence of both the old ACTIVE_CA_ID and newly elected ACTIVE_CA_ID help identify any malicious ACTIVE_CA.

Message 6: TRANSFER CA OWNERSHIP

$$CA_{i-1} \rightarrow CA_i : [CAid_{i-1}, CAid_i, TS_i, E(CAid_{i-1}, CAid_i, TS_i)CApub_i, BCAST\_COUNT, H] \quad (6)$$

In Eq. (6), the BCAST_COUNT value is used to limit the number of rebroadcasts, thus lowering the communicational related energy consumption of a node. This value is found only in the messages sent by the CA nodes (ACTIVE and IDLE_CA nodes). The CA ownership transfer message is rebroadcast by the intermediate IDLE_CA nodes with an increment in the BCAST_COUNT value. The BCAST_COUNT value is reset by the destination node or once it reaches a maximum value, which is equal to the number of available CA nodes in the network.

3.3.4 Node/CA ID Revocation

The already associated nodes and nodes that may potentially join the network information in both the ACTIVE and IDLE_CA nodes provide an information base. Every CA node knows the other available CA nodes and the corresponding maximum BCAST_COUNT value. Therefore, any rogue CA node or malicious activity can be detected if the BCAST_ COUNT value has gone beyond the maximum value. The IDLE_CA nodes always concatenate their own IDs before performing any rebroadcasting for increased security and neighborhoods monitoring, which helps to identify any compromised or malicious CA nodes. If any fake or duplicate non-CA node ID is found, the ACTIVE_CA node can access the medium with priority to revoke that particular node ID in a NODE_ID_REVOKE message. Similarly, any old ACTIVE_CA who has just shifted the CA ownership or other IDLE_CA nodes can detect and announce a fake CA_ID using a CA_ID_REVOKE message.

Message 7: NODE_ID_REVOKE:

$$CA_i \rightarrow N_{(j....n)}, CA_{(i..n)} : E[Nid_j, CAid_i, TS_i, BCAST\_COUNT, H] CApri_i \quad (7)$$

Message 8: CA_ID_REVOKE:

$$CA_{i-1} \rightarrow N_{(j....n)}, CA_{(i..n)} : E[CAid_i, CAid_{i-1}, TS_i, BCAST\_COUNT, H] CApri_{i-1} \quad (8)$$

In Eqs. (7) and (8), Nid_j and $CAid_i$ are the malicious node and CA_IDs, respectively. Both messages are encrypted with the private keys of either the ACTIVE_CA or old ACTIVE_CA, which has just shifted the ownership. Therefore, only the nodes possessing the relevant public key pairs can decrypt the messages. RSCAAP does not provide a provision for the redemption of compromised CA nodes; rather, a CA node is declared malicious by revocation (CA_ID_REVOKE).

3.3.5 RSCAAP Message Sequence Steps

In Fig. 1, the message sequence is given as follows:

1. In the broadcast of ACTIVE_CA_MESSAGE, Both N_j & N_{j+1} contend for the medium to send the

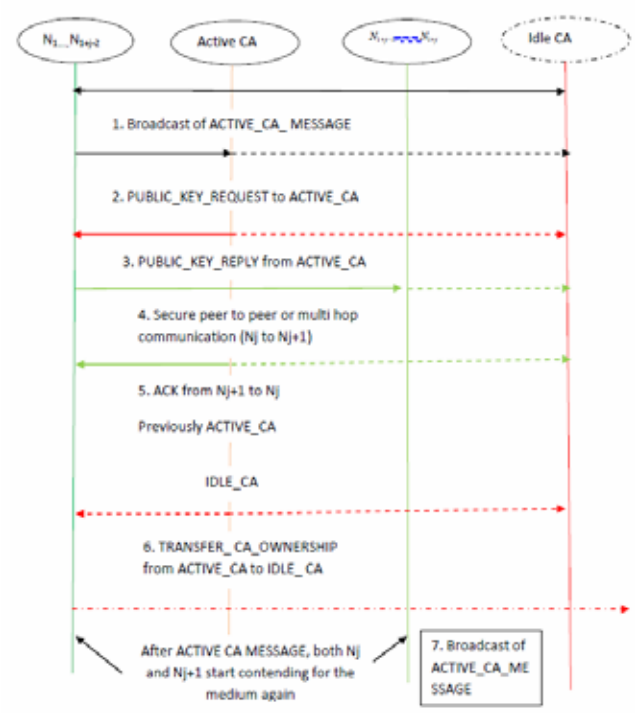

Fig. 1. Message Sequence Chart.

PUPLIC_KEY_REQUEST to the current ACTIVE_CA.
2. In PUBLIC_KEY_REQUEST to ACTIVE_CA, N_{j+1} = PUBLIC KEY REQUEST time + PIFS.
3. In PUBLIC_KE_ REPLY from ACTIVE_CA, N_{j+1} = PUBLIC KEY REQUEST time + DIFS.
4. In Secure peer to peer or multi hop communication (Nj to Nj+1), N_{j+1} = secure transmissions time + SIFS.
5. In ACK from N_{j+1} to N_j, previous ACTIVE_CA, N_{j+1} = inhibited from doing any further transmissions or backing off for ACK time + PIFS.
6. In TRANSFER_ CA_OWNERSHIP from ACTIVE_CA to IDLE_ CA, N_{j+1} = transfer packet time + PIFS.
7. In the broadcast of ACTIVE_CA_MESSAGE, IDLE_CA becomes ACTIVE_CA.

3.4 Enhanced Hash Message Authentication Code (EHMAC)

When a node wants to transmit the packets to nodes, all the packets are encrypted with EHMAC and EHMAC [2] was used in all control packets. When the packet is sent, its verification is performed and it replies with the transmitter address and EHMAC in the acknowledgement. In such a way, the message is authenticated with the control of packets. The goal in message authentication is for one party to efficiently transmit a message to another party in such a way that the receiving party can determine if the message received has been tampered with.

When the node sends and receives the control packet (RTS, CTS or ACK) before doing anything, it must authenticate with CA and check the integrity of the information in this packet. If the procedure is performed successfully, the CA sends the control packets to the sender or receives the control packets from the sender. The node must check the control packets received by the CA and the CA should also check the packets. Many cryptography approaches can be discussed to ensure the authentication and integrity checking. On the other hand, most of them are eliminated due to the limited resources constraint.

Symmetric key cryptography is faster and less costly from a computation and complexity point of view, so a symmetric key cryptography is preferable to the public key cryptography on the MAC layer. Message authenticated code (MAC), particularly the hashed MAC (HMAC), is selected because it is one of the lowest security costs that is well adapted to solve this problem. The HMAC uses known cryptographic hash functions, such as MD5 and SHA1, to ensure the integrity of the message. HMAC is defined as follows:

$$\text{HMAC}(D,K) = H(K \oplus a) \| H(K \oplus b)\}\}D) \quad (9)$$

In Eq. (9), D is the data to send and H is the hash function. a is the inner padding and b is the outer padding. When there is a small number of a bit to send in the block, the inner padding adds the elements. If the data is more than the packets, the outer padding will make another block. On the other hand, HMAC is efficient for long messages, but for short messages, the nested constructions result in significant inefficiency. For example, to MAC, a message shorter than a block, the HMAC requires at least two calls to the hash function rather than one. This inefficiency may be particularly high for some applications, such as message authentication of signaling messages, where the individual messages may all fit within one or two blocks. In this study, EHMAC was used to overcome that drawback. EHMAC is not only significantly more efficient than NMAC for short messages but is also somewhat more efficient for longer messages. Assume K is the shared key, and the data is a compressed data packet or any control message. EHMAC is defined as follows:

$$\begin{cases} \text{if } (|D| \le 445 \text{ bits}) \text{ then } H(K \oplus a \| D \| 1) \\ \textit{ElSE} \\ \text{then } H(K \oplus a \| H(K \oplus b \| M_{pref} \| M_{suff} \| 0) \end{cases} \quad (10)$$

In Eq. (10), H is the hash function, and the data is 64 bytes in length. M_{suff} and M_{pref} are dependent on the hash function. In the case of SHA, the M_{suff} and M_{pref} values are

$$\begin{aligned} M_{pref} &= M_1 - M_{|M| - 286} \\ M_{suff} &= M_{|M| - 286} - M_{|M|} \end{aligned} \quad (11)$$

EHMAC provides more efficient message authentication than HMAC while also providing proofs of security.

4. Simulation results

4.1 Simulation Model and Parameters

Network Simulator Version-2 (NS-2) [10] was used to simulate the proposed algorithm. In the simulation, the channel capacity of mobile hosts was set to the same value: 11 Mbps. The distributed coordination function (DCF) of IEEE 802.11 for wireless LANs was used as the MAC layer protocol. This function has the functionality to notify the network layer about link breakage. In the simulation, mobile nodes move in a 1000 meter x 1000 meter region for 50 seconds simulation time. The simulated traffic is a Constant Bit Rate (CBR).

In the simulation, attacks are simulated where the attacker nodes send spurious certificates to the nodes that have requested those certificates. These attacks can be isolated attacks, where every attacker certifies a different public key. On the other hand, the attackers may also launch a cooperative attack, where a group of attackers collude and send certifications for the same public key that is spurious. Both types of attacks, isolated and collusion were simulated. Each node successfully executed the initialization step by exchanging the requisite number of certificates with the honest nodes in the network. The numbers of attackers were varied as 1,2,3,4, and 5.

Table 2 lists the simulation settings and parameters.

Table 2. Simulation Settings.

Number of Nodes	50
Area Size	1000 X 1000
Mac	802.11
Radio Range	250m
Simulation Time	50 sec
Traffic Source	CBR
Packet Size	512
Speed	5 M/s
Routing Protocol	CERM
No. Of Attackers	1,2,3,4 and 5.

4.2 Performance Metrics

The performance was evaluated according to the following metrics:

Average Packet Delivery Ratio: This is the ratio of the number of packets received successfully and the total number of packets transmitted.

Resilience against Node Capture: This part calculates how a node capture affects the remaining network resilience. This is calculated by estimating the fraction of communications compromised between the non-compromised nodes by a capture of x-nodes.

Average Packet Drop: This is the average number of packets dropped by the misbehaving nodes.

End-to-End Delay: This is the amount of time taken by the packets to reach the destination.

The proposed MAC Layer Based Certificate Authentication for the multiple Certification Authority in MANET (MBCA) was compared with the ID-based multiple secrets key management scheme (IMKM) [8].

4.3 Results

Fig. 2 presents the average end-to-end delay of both schemes, when the attackers are increased from 1 to 5. The delay increased linearly with increasing number of attackers. On the other hand, the delay of MBCA was 74% lower than the existing IMKM technique.

Figs. 4 and 3 present the data packets decreased due to the attackers, and the packet delivery ratio, respectively. As the number of attackers increase, more data packets are dropped. On the other hand, MBCA has 55% fewer packet drops compared to the IMKM scheme. Because the packet drop is increasing linearly, the packet delivery ratio is decreasing, as shown in Fig. 3. MBCA shows a 6% increase in the packet delivery ratio compared to IMKM.

Fig. 5 presents the results of resilience against node capture. The resilience of MBCA is 33% lower than IMKM because MBCA has fewer compromised nodes.

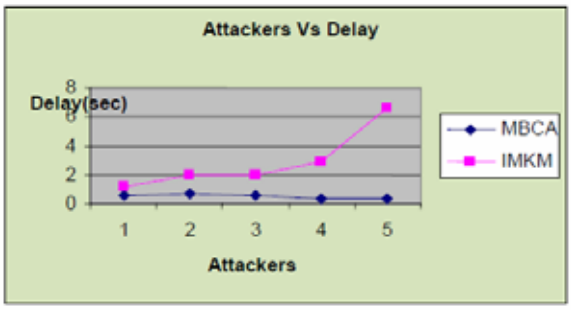

Fig. 2. Attackers Vs Delay.

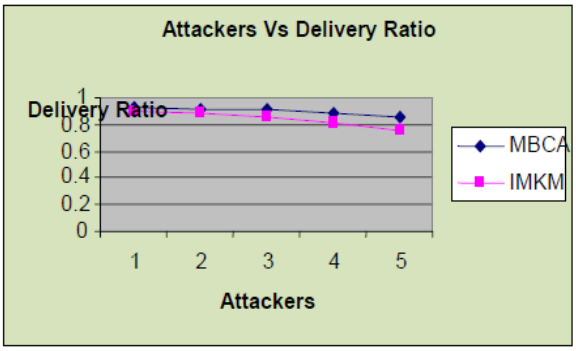

Fig. 3. Attackers vs. Delivery Ratio.

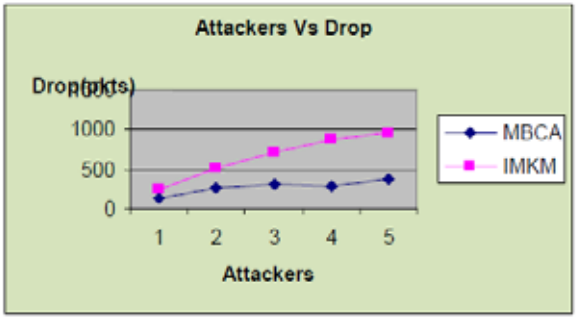

Fig. 4. Attackers vs. Drop.

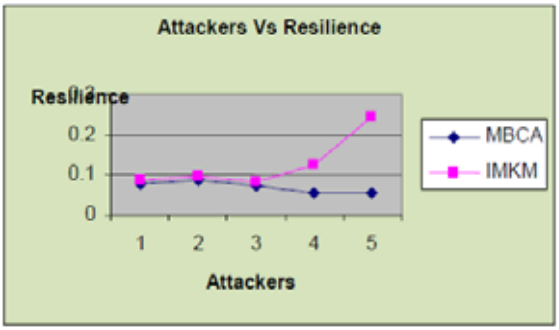

Fig. 5. Attackers vs. Resilience.

5. Conclusion

A novel Randomly Shifted Certification Authority Authentication protocol was used in this study as an extension work. The nodes achieved authentication using public key certificates issued by a CA, which assures the certificate's ownership. Here, the MAC protocol provides a CA node with prioritized access to the medium to transmit an active message in the management frame. As a part of providing key management, the active CA node

transfers the image of the stored public keys to other idle CA nodes. The transaction is achieved by a public key. Revoking is done if any fake or duplicate non CA node ID is found. Therefore, only the nodes possessing the relevant public key pairs can decrypt the messages. Enhanced Hash Message Authentication Code (EHMAC) [2] can be used to provide authentication and integrity in the form of preventing MAC control packets. Here EHMAC with varying output was introduced in all control packets. When a node transmits a packet to a node with EHMAC, verification is performed and it replies with the transmitter address and EHMAC in the acknowledgement. In such a way, the message is authenticated with the control of packets. As a future study, the proposed work will be extended to various MAC layers by considering the dynamic characteristics of the MAC layer.

References

[1] R. Murugan and A. Shanmugam, "A Combined Solution for Routing and Medium Access Control Layer Attacks in Mobile Ad Hoc Networks", Journal of Computer Science 6.12 (2010). Article (CrossRef Link)

[2] Abderrezak RACHEDI and Abderrahim BENSLIMANE, "Impacts and Solutions of Control Packets Vulnerabilities with IEEE 802.11 MAC", Wireless communications and mobile computing 9.4 (2009). Article (CrossRef Link)

[3] G.A. Safdar and M. McLoone, "Randomly Shifted Certification Authority Authentication Protocol for MANETs", Mobile and Wireless Communications Summit, 2007, 16th IST, IEEE, 2007. Article (CrossRef Link)

[4] Sadasivam, Karthik and T. Andrew Yang. "Evaluation of Certificate-Based Authentication in Mobile Ad Hoc Networks". M.H. Hamza, P. Prapinmonkolkarn, T. Angkaew. *(Eds): Proc. of the IASTED Int. Multi-Conf. on Networks and Communication Systems (NCS 2005).*Krabi, Thailand. April'18-20, 2005. Article (CrossRef Link)

[5] Hongqiang Zhai, Jianfeng Wang, Xiang Chen and Yuguang Fang, "Medium access control in mobile ad hoc networks: challenges and solutions", Wireless Communications and Mobile Computing 6.2 (2006). Article (CrossRef Link)

[6] K.Suresh Babu and K.Chandra Sekharaiah, "CBDAT: Cross Layer Based Detection and Authentication Technique for MANET", IJCSNS International Journal of Computer Science and Network Security, 22 VOL.13 No.7, July 2013. Article (CrossRef Link)

[7] Gulshan Kumar and Mritunjay Rai, "Assured Neighbor Based Counter Protocol on Mac-Layer Providing Security in Mobile Ad Hoc Networks", Academy & Industry Research Collaboration Center, Jul 2011. Article (CrossRef Link)

[8] Alejandro Cornejo, Nancy Lynch, Saira Viqar and Jennifer L. Welch, "Neighbor Discovery in Mobile Ad Hoc Networks Using an Abstract MAC Layer", Communication, Control, and Computing, 2009. Allerton 2009 47th Annual Allerton Conference on IEEE 2009. Article (CrossRef Link)

[9] Gaurav Kulkarni and Brajesh Patel, "Time Stamp Based Cross Layer MANET Security Protocol", Global Journal of Computer Science and Technology Network, Web & Security Volume 13 Issue 10 Version 1.0 Year 2013. Article (CrossRef Link)

[10] Network Simulator, Article (CrossRef Link)

[11] T.R.Panke, "Clustering Based Certificate Revocation Scheme for Malicious Nodes in MANET", International Journal of Scientific and Research Publications, Volume 3, Issue 5, May 2013. Article (CrossRef Link)

[12] Priti Rathi and Parikshit Mahalle, "Proposed Threshold Based Certificate Revocation in Mobile Ad Hoc Networks", Intelligent Computing, Networking and Informatics ,Advances In Intelligent Systems and Computing , Volume 243,2014,pp377-388. Article (CrossRef Link)

[13] T.Buvaneswari and A. Antony Truth Ayaraj, "Novel Accuser of Security Based Certificate Revocation in MANET", International Global Research Analysis (GRA), Vol. 2, Issue. 11, pp. 94-98, Nov 2013. Article (CrossRef Link)

[14] A. Praveena and L.M. Nithya, "Cluster Enhanced Secure Authentication Scheme For Data Integrity In MANET", International Journal of Computer Science and Mobile Computing, Vol.3 Issue.4, April- 2014, pg. 693-700. Article (CrossRef Link)

J. Chandra Sekhar, M.Sc. (Computer Science), M.Tech.(CSE) is working as an Associate Professor in the Department of CSE, Chalapathi Institute of Technology, Guntur, A.P. He is a Ph.D. Research Scholar in the Department of CSE, Acharya Nagarjuna University, Guntur, A.P. He is having 10 years of experience in Teaching.

Dr. Ramineni Sivaram Prasad, Ph.D. is working as an Associate Professor & Research Director In Department of CSE, Acharya Nagarjuna University, Guntur, A.P. He has published more than 80 Research papers in both National and International journals, attended 104 seminars, has given several extension lectures, and published 5 books to his credit.