**ABSTRACT**

Route identification and digital signature has been considered in Mobile Ad hoc NETwork (MANET) for efficient message broadcasting. The integrity and authenticity through acknowledgement packets, forged acknowledgement attack is not possible due to dynamic traffics. In addition, the route identification usually filters out newly observed polluted nodes through digital signature scheme. Thus, the information state is obtained through Gittins index, because the traffic changes continuously and demand for security arises. In this paper, we propose a Sender Route Authentication with Multi-bit Digital Signature (SRA-MDS) model to improve security level during message broadcasting in MANET. Initially, the route authentication in MANET is verified through evaluate the confidence value and probability measure of the neighboring node that efficiently performs the route authentication to reduce the network overhead. Authenticated routes are selected for message broadcasting using authentication and verification algorithm, aiming at reducing the forged acknowledgement attacks. Broadcast message is finally secured on dynamically changing topology using Multi-bit Digital Signature generation. A single instance digital signature with multiple bits is used to highly secure the broadcasted message in SRA-MDS model. Extensive performance analysis is performed to prove the effectiveness and strengths of the proposed message broadcasting model in MANET. Moreover, simulations were performed to measure several parameters, like the network overhead, secure message forwarding rate and acknowledgement attack rate. It shows that SRA-MDS model significantly reduces the network overhead, acknowledgement attack rate and improves secure message forwarding rate compared to the state-of-the-art works.

**KEYWORDS** Route Identification, Digital Signature, MANET, Forged Acknowledgment Attack, Sender Route Authentication, Message Broadcasting.

**INTRODUCTION**

Due to the dynamic nature and intermittent changes in the topology Mobile Adhoc Network susceptibility, the different attacks create significant problems. As a result, the security aspects have to be considered so that message broadcasting can be performed in an efficient manner. In mobile ad hoc networks, whenever a Sender wants to broadcast the messages to the destination node, the security is the major concern. However, the several research without use any specified authentication scheme for broadcasting messages. Accordingly, this scheme does not ensure the security of the network. Therefore, overall network throughput also reduced. The secure intrusion detection scheme was developed in earlier and the detailed explanation is obtained in following. An intrusion detection system called, Enhanced Adaptive Acknowledgement (EAACK) [1] was designed with the main objective of improving the packet delivery ratio by reducing the network overhead through Digital Signature with Appendix (DSA) and Digital signature with message recovery (RSA) schemes. However, forged acknowledgement attacks also increased with the increase in the packet delivery ratio.

Mobile ad-hoc networks (MANET) are significantly used in several applications in mobile computing and wireless communications. Security is a major concern for mobile ad hoc networks. User Authentication and Intrusion Detection in MANETS (UA-ID) [2] addressed both intrusion and provided authentication for the users through Markov decision process. But, security aspects were not covered. A user authentication (or IDS) scheme can be planned to ensures the security circumstances and resources in MANETs.

An Efficient key Management scheme was presented in [21] aiming at reducing the memory and computation overhead for large scale wireless sensor networks. This scheme ensures the security as normal public key which can considerably reduce the search time in large scale WSN. In addition, this scheme provides the better scalability of network and also used to support the node addition and deletion operation. However, through the key distribution, the public key technology provides high computationally cost for WSNs.

Based on the above mentioned issues, we propose a Sender Route Authentication with Multi-bit Digital Signature (SRA-MDS) model. Initially, to ensure authentication of the sender route, the confidence and probability values are measured which reduces the message overhead. After that, the authenticated routes are selected by applying authentication and verification algorithm that significantly reduces the forged acknowledgement attacks. Finally, Multi-bit Digital Signature generation is used to highly secure the broadcasted messages on dynamically changing topology improving the message forwarding rate in MANET.

The remaining part of this paper is organized as follows. Section 2 briefly surveys the recent literature and the related works contributed by many researchers in the field of secure route path in MANET. In Section 3, the proposed SRA-MDS model and the objective behind the work with the aid of neat architecture diagram is explained. Section 4 describes experiment setup. Section 5 describes the results of the simulation and a performance evaluation. Finally, we conclude this paper and future research scope in Section 6.

**RELATED WORKS**

Mobile Ad-hoc Network (MANET) security is a significant approach in several applications. But, the free space and wide range transmission of nodes make MANET accessible to malicious attackers. In this case, it is significant to design effective intrusion-detection mechanisms to preserves MANET from attacks. There are a few research works that properly analyze the security of these proposals.
A. Security Based Message Broadcasting

Privacy is one of the main aspects in multipath routing for safe and secure message broadcasting in MANET. The security aspects have to be considered for message broadcasting in an efficient manner. Joint Authentication and Topology Control (JATC) [3] provided mechanisms for security using discrete optimization problem improving the message delivery rate through cooperative communication model. However, JATC is created as a discrete stochastic optimization issues without any prior perfect channel status. In [4], Unobservable Secure On-demand Routing protocol was designed to address the issues related to security and improves the packet delivery ratio through ID-based cryptosystem. USOR is effective because it employs mixture of grouped signature and ID-based encryption for route discovery. Security analysis reveals that USOR preserves the user privacy against inside and outside attackers. However, these unobservable routing schemes were not performed DoS attacks effectively.

Another method, Geographic Routing Overhead for Location Service (GRO-LS) [5] was designed with the objective of improving the message broadcasting using ID and location information. However, scalability remained unsolved. To address the issues related to scalability, Efficient Geographic Multicast Protocol (EGMP) [6] was designed that concentrated on data transmission overhead by solving scalability through the construction of multicast tree. To improve the content of message being sent, Multicast Authentication using Batch Signature (MABC) [7] was designed and resulted in the improvement of packets being filtered. Hash Message Authentication Code (HMAC) [18] was used to address security against black hole attack.

B. An Efficient Intrusion Detection System

Routing protocols were designed in MANET to provide the self-organized properties of the network without protection against any inside or outside network attacks. In [13], Tropical Intrusion Detection (TID) was introduced to address the Packet Drop Attack (PDA) through Route Intrusion Detection (RID) that extensively reduced the routing overhead. However, security mechanism was compromised. In [15], Position-based Opportunistic routing was introduced to improve the data being delivered using Virtual Destination-based Void Handling (VDVH), enhancing the packet delivery ratio. However, neighbor position information was not updated, resulting in reducing the latency rate. For making effective forwarding decisions, Greedy Perimeter Stateless Routing Protocol (GPSRP) [16] was introduced to reduce the intrusion through Adaptive Position Update (APU). To improve data latency and Quality of Service (QoS) used unicast and broadcast protocol [17] ensuring packet delivery ratio under normalized routing load. Though robustness was ensured in high traffic environments, security remained unaddressed.

C. Key Distribution Based Message Broadcasting

Obtaining the routing information and linking the node through different nodes is an important element for network monitoring. Additive metrics [8] were used and sequential topology inference algorithm was used based on neighbor joining to improve the correctness ratio and node ratio. However, the indirect information was not applied for sharing secret keys. In [9] High-Rate Uncorrelated Bit Extraction (HBUBE) was used to improve the key sharing rate. But, attacks arising during bit extraction remained unaddressed. The role of black hole attacks was solved in [10]. However, measures were not taken for secured data transmission. Another method for secured data transmission using Sequential Aggregate Signatures (SAS) [12] was designed to secure the nodes against several attacks to improve the network lifetime. It also creates a session key for all pair of sender and destination nodes of a MANET for secure message transmission.

Mobility based key management [14] was introduced using multicast tree to address security issues through keying interval. Though security was ensured, the reliability of data being delivered remained unaddressed. However, in MANET multicasting, forward and backward secrecy leads to the increased packet drop rate due to mobility. Trusted Third Party (TTP) [19] mechanism was introduced to maintain message integrity through effective key management scheme. However, the process was time consuming due to the application of public key cryptography. Symmetric Encryption [20] was used to address authentication through digital signature scheme.

In [22], Trust management based mechanism was designed for end users in resource control networks using lightweight symmetric key management system. However, lightweight mechanism increases the complexity of system with time and number of neighboring nodes. The Key management (KM) and secure routing (SR) integrated framework was introduced [23] in Mobile Ad-hoc Networks (MANETs) to provide security features contains confidentiality, integrity, authentication, and non-repudiation. This method is used where public key of the nodes is certified by different nodes. However, it does not contain certification revocation mechanism to this multipath technique.

The above said methods provided solutions to improve the throughput minimizing the memory and computation overhead by reducing the localization error through different schemes. The literature also provided insight into various optimization problems for secured data transmission. Based on the aforementioned techniques and issues addressed through it, the problem therefore is focused on secured message broadcasting. The objective behind the design of secure message broadcasting is to ensure security using sender route authentication and multi-bit digital signature where the mobile nodes sent their packets through intermediate nodes on a cooperative basis. As the efficient route identification cannot be obtained through conventional digital signature, the necessity of Multi-bit Digital Signature generation with multiple bits to highly secure the broadcasted message is introduced.

The modification required from single-bit to multi-bit is also derived using the necessary and sufficient conditions for achieving optimal message forwarding rate. This is performed by introducing the MDS algorithm. The MDS algorithm evaluates the confidence and probability measure accordingly by designing an Authentication and Verification algorithm, aiming at ensuring secure message
forwarding rate. Extensive simulations are also conducted to show that the proposed model significantly reduces the routing overhead while selecting the best route and improve security during message broadcasting. The MDS algorithm also converges to the optimal values under various network configurations.

II. PROPOSED METHODOLOGY

A. Sender Route Authentication with Multi-Bit Digital Signature

In this section, we propose a secure and efficient Multi-bit Digital Signature model (MDS). Initially, the confidence correlation is evaluated to authenticate the sender route for the source and neighbor nodes. After that, route selection is performed using authentication and verification algorithm for reduces forged acknowledgement attacks. The main objective is that for each packet ‘P_i’ to be sent to the destination node ‘MDN_j’, a public, private key pair is generated for the packet ‘P_i’ for each source-destination pair. The generation is based on the MDS algorithm. Unlike the secured intrusion detection model for MANET, requires to evaluate the Digital Signature algorithm using single bit for each mobile node separately, the proposed SRA-MDS model requires single instance digital signature with multiple bits to highly secure the broadcast message. Fig. 1 given below shows the flow model for Sender Route Authentication with Multi-bit Digital Signature.

![Figure 1 Flow of Sender Route Authentication with Multi-bit Digital Signature](image)

Fig. 1 given above performs the secure message broadcasting through Sender route authentication with the main objective of minimizing network overhead. Authenticated routes are then selected by applying the authentication and verification algorithm that reduces the forged acknowledgement attacks through confidence value and probability measure. Finally to perform secure message broadcasting, MDS algorithm is applied for each mobile node with the assumption of cooperative node structure. The elaborate description of SRA-MDS model is explained in the forthcoming sections.

1) Adversary model

The design of attack model is defined based on the ability of adversaries. Here, we consider the following three cases:

1. Without compromising any Sensor Nodes or Neighbor Nodes (SN/NN). An adversary can only eavesdrop during message broadcasting in the air, so he can modify or inject the forged attacks with this public information through route path.

2. Compromising Sensor Nodes (SNs). After compromising a Sensor Nodes (SN), an adversary can obtain secrets such as confidence values/entropy values. Then, an adversary can obtain messages and packets passed through the captured sensor nodes or impersonate the comprised sensor node to forge acknowledgement attacks.

3. Compromising Neighbor Nodes (NNs). After compromising a Neighbor Nodes (NN), an adversary can obtain the secrets such as public/private keys and perform the following attacks. First, an adversary can decrypt the public key of sensing packets sent by its neighboring nodes. Second, an adversary can generate forged broadcasted message.

2) Security Assumptions

Lemma 1:

Whenever a source node establishes a route with destination nodes via neighboring nodes, the source node in SRA-MDS model ensures multiple routes leading to the destination node.

Lemma 2:

Whenever a source mobile node sent the route request (RREQ) to the destination through its neighbor nodes, a correlation between the source and the neighbor node is made using the confidence value. The neighbor node sent back the route reply message (RREP) by evaluating both the probability measure values in addition to the confidence value 1, -1 or 0, through which the probability measure is evaluated.

3) Security proof using SRA-MDS model

Sender Route Path Authentication is provided in MANET using SRPA-MDSMB where verification of message being broadcasted. Broadcast message is also secured on the dynamically changing topology using the Multi-bit Digital Signature generation. Similarly, Route Path Verification in MANET is made in an efficient manner. Finally, the forged acknowledgement attacks are reduced in a significant manner using the authentication and verification algorithm.

B. Sender Route Authentication

The first step for efficient message broadcasting in MANET is to ensure authentication of the sender
route, due to high vulnerability nature of the network and frequent topology changes. The proposed model, SRA-MDS ensures Sender Route Authentication in MANET. The SRA-MDS model uses confidence value and probability measure aiming at reducing the network overhead.

**Lemma 1:**

Let us assume that whenever a source node wants to establish a route with the destination nodes through other neighboring nodes, the source node in SRA-MDS model uses confidence value of neighboring nodes that provides multiple routes to the destination.

Now the source node identifies packet-forwarding confidence measures of neighboring nodes regarding the routes. Finally the source node selects the confident route for message broadcasting. Accordingly, the source node updates the confidence measure value on the basis of its consideration of route quality. As a result, the network overhead in identifying the route is reduced by evaluates confidence correlation value. The forthcoming section elaborates in detail the design of route authentication scheme.

1) **Sender Route Authentication**

The Sender Route Authentication is performed where the message being broadcasted is secured as the message cannot be displayed while transmitting through the network. In order to authenticate the sender route, the sender node trusts the neighbor node to perform an action. In this SRA-MDS model, the first entity is called the sender nodes; the second entity is called the neighbor node. So, a representation to denote the confidence correlation is given as below,

\[ CC : SN_i \rightarrow NN_j \] (1)

From (1), where ‘CC’ represent the confidence correlation for route authentication for the source and neighbor nodes, ‘SN_i’ and ‘NN_j’ respectively. Fig. 2 shows the representation of sender route authentication. Fig. 2 shows three sender nodes which represent ‘SN_3’, ‘SN_5’, and ‘SN_2’, where the neighbor nodes for ‘SN_3’ are ‘NN_4 and NN_5’ respectively and neighbor nodes for ‘SN_5’ are ‘NN_1 and NN_6’, respectively.

![Figure 2 Diagrammatic representation of route authentication](image)

In order to identify and establish route for neighbor nodes, the confidence value for each sender node is measured. Initially, sender node transmits a RREQ message to its neighboring node. Subsequently, the neighboring nodes sends back RREP message to the sender with its confidence value and probability measure. Based on the confidence value, the best neighbor nodes for each sender nodes are identified. If there is more than one neighboring node for particular sender node, the process is repeated with their corresponding confidence value. Finally, the neighbor node that has the most confidence value is selected as the authenticated route node.

The confidence value of the confidence relationship and probability measure that the source node performs for efficient route authentication with neighbor node point of view is provided as below,

\[ C : SN_i \rightarrow NN_j \] (2)

\[ Prob : C(SN_i \rightarrow NN_j) \] (3)

Where ‘C’ denotes the confidence value (i.e., 1, -1 or 0) and ‘Prob’ denotes the probability measure between the source and the neighbor nodes respectively. In order to perform sender route authentication, an entropy value is obtained based on the probability measure ‘Prob’. Therefore, the entropy based sender route authentication is measured as below:

\[ CC : SRA, SN_i \rightarrow NN_j = 1 - (Prob) , \text{ where } 0 \leq Prob \leq 1 \] (4)

\[ CC : SRA, SN_i \rightarrow NN_j = 1 + (Prob) - 1, \text{ where } -1 \leq Prob \leq 0 \] (5)

From (4) and (5), when ‘Prob’ = 1, then the source node has increased confidence measure on the neighbor node and the sender route authentication value is 1. Then the sender route is authenticated and performs message broadcasting to its neighboring node. When, ‘Prob’ = -1, then the source node does not have confidence measure on the neighbor node and the no operation is performed. Finally, when, ‘Prob’ = 0, then the source nodes does not have any idea about the neighbor node and therefore the sender route authentication value is 0. Therefore, there is no route is authenticated and message broadcasting to its neighboring node also failed.

Let us consider two mobile nodes ‘MN_1’ and ‘MN_2’ respectively where ‘MN_1’ establishes the relationship with ‘MN_2’ and let the observation be denoted as ‘O’(i), then, the number of correct source route authentication is given as below

\[ \sum_{i=1}^{n} O(i) \] (6)

The probability of success rate is given as below

\[ Prob (O(N + 1)) = \frac{Prob (O(N + 1))}{Prob (n)} \] (7)

Where, ‘Prob’ denotes the probability of successful message broadcast with ‘N’ denoting the total number of messages broadcasted by source nodes with ‘n’ denoting the number of messages successfully broadcasted by the neighbor nodes.

C. **Route Selection**

Once the sender route is authenticated, an efficient route selection is made for message broadcasting using authentication and verification algorithm, aiming at reducing the forged acknowledgement attacks. From (7), if ‘Prob (O(N + 1)) = 0’, then Sender Route Authentication (i.e. SRA) is set to 1, following which the route is authenticated (i.e. RA) and message broadcasting is performed which is mathematically formulated as given below.

If ‘Prob (O(N + 1)) = 0’, then ‘SRA = 1’, ‘RA = True’ and ‘Broadcast message’ (8)

If ‘Prob (O(N + 1)) = 1’, then ‘SRA = 0’, ‘RA = False’ and ‘No Message Broadcast’ (9)

The design of authentication and verification algorithm for efficient route selection based on route authentication algorithm is given below.
Initialize Mobile Nodes \( MN_i = MN_1, MN_2, \ldots, MN_n \), Neighboring Nodes \( NN_i = NN_1, NN_2, \ldots, NN_n \), Confidence \( C' \), Probability Measure \( P' \).

1) **Key generation**

During the key generation in Multi-bit Digital Signature model, let us consider that the mobile node \( MN_i \) initially sends a packet \( P_i \) to the destination mobile node \( DMN_i \) that is mathematically formulated as given below.

\[
MN_i \rightarrow (P_i, DMN_i) \tag{10}
\]

If all the intermediate mobile nodes along the route path between node \( MN_i \) and destination mobile node \( DMN_i \) are cooperative and destination node \( DMN_i \) successfully receives a packet \( P_i \). Then, the mobile node \( MN_i \) sends back \( ACK_i \) to \( DMN_i \) which is given as below.

\[
DMN_i \rightarrow (ACK_i, P_i, MN_i) \tag{11}
\]

Within a predefined time period, if node \( MN_i \) receives packet \( P_i \), then the packet transmission from node \( MN_i \) to node \( DMN_i \) is successful and accordingly a key is generated. The key differs for each source, destination pair mobile nodes where the source mobile node \( MN_i \) selects a random hash value \( V_Ali \) and a pseudonym \( P_{Ni} \) for each mobile node. The public key and the private key sent to the destination mobile node \( DMN_i \) and Multi-bit Digital Signature (ST) is given as below,

\[
\text{Public Key} = (V_Ali, P_i) \tag{12}
\]

\[
\text{Private Key} = (V_Ali, ST_i) \tag{13}
\]

If the node does not receive a packet within a specified time period, then it is considered as forged acknowledgement attacks. Therefore, the mobile node \( MN_i \) identifies secure message forwarding through Multi-bit Digital Signature generation as discussed in next subsection.

2) **Multi-bit Digital Signature generation**

The proposed SRA-MDS model, using Multi-bit Digital Signature generation allows three mobile nodes to identify forged acknowledgement attacks. Let us consider that the first node is the sender mobile node \( MN_i \); the second node is the mobile destination node \( DMN_i \) and the final node \( TN_i \). Initially, the acknowledgement packet is sent to the first (i.e., sender mobile node) node. Then, the resulting Multi-bit Digital Signature, \( (ST_{i1}, ST_{i2}, \ldots, ST_{ik}) \) is sent by the final node and the acknowledgement packet \( P_i \) is sent to the mobile node \( MN_i \) is given as below.

\[
\text{MDS} \rightarrow (ST_{i1}, ST_{i2}, \ldots, ST_{ik}, P_i) \tag{14}
\]

Once the MDS is generated, the final process is to verify them through MDS verification that is discussed below.

E. **Multi-bit Digital Signature Verification**

The final process to be performed to verify the signature by applying Multi-bit Digital Signature Verification therefore it increases the secure message forwarding rate. The SRA-MDS model performs verification using following equation as given below,

\[
\text{if } (ST_{ik}) = (\text{Private Key}), \text{ then accept signature}
\]
Finally the broadcast message (i.e., packet) is secured on dynamically changing topology by applying the above three steps with the help of MDS algorithm as given below.

Algorithm 2 MDS algorithm

The three parts involved in MDS is shown in above algorithm. The first part involves the key generation along with the cooperativeness between the in-between mobile nodes and destination mobile node. Followed by this, a Multi-bit Digital Signature is generated through the third node along with the packet. Finally, the MDS verification is performed through an if-then condition that performs conditional search between secret and private key and accordingly, if both the secret and private keys are same, the signature is accepted or else the signature is rejected.

SIMULATION SETTINGS

The performance evaluation of the proposed secure message broadcasting framework using SRA-MDS model is provided with certain simulation results. The simulation results were performed on NS2 and compared with the existing Enhanced Adaptive Acknowledgement (EAACK) [1], User Authentication and Intrusion Detection in MANETS (UA-ID) [2] and Key Management for large scale network (KM-LSN) [21].

The nodes were initially placed within a fixed size of 1000 m * 1000 m in a square area and the motion of the nodes described using Random Way point model for simulation. The Dynamic Source Routing (DSR) protocols used in SRA-MDS model based on randomly moving objects. The simulation was performed using 70 mobile nodes and 50 ms for each iteration. Constant Bit Rate (CBR) data flow was used where each node generates 10 packets/seconds with a packet size of 512 bytes. The simulation speed is 50 m/s, where Omni directional antenna is used for simulation and performs single process at a time for transmitting or receiving packet. Three mobile nodes, three packets and three destination mobile nodes were used. Table 1 shows the simulation parameters for different scenarios.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simulator</td>
<td>NS-2.31</td>
</tr>
<tr>
<td>Network Coverage area</td>
<td>1000m * 1000 m</td>
</tr>
<tr>
<td>Mobility model</td>
<td>Random Way point model</td>
</tr>
<tr>
<td>Messages sent (bytes)</td>
<td>64 – 2048 (bytes)</td>
</tr>
<tr>
<td>Node movement (i.e., speed)</td>
<td>50 m/s</td>
</tr>
<tr>
<td>Number of nodes</td>
<td>10, 20, 30, 40, 50, 60, 70</td>
</tr>
<tr>
<td>Connected Path link</td>
<td>Multi direction</td>
</tr>
<tr>
<td>Packet rate</td>
<td>10 packets/seconds</td>
</tr>
<tr>
<td>Mobile Nodes</td>
<td>3 nodes</td>
</tr>
<tr>
<td>Packets</td>
<td>3 packets</td>
</tr>
<tr>
<td>Mobile Destination Nodes</td>
<td>3 destination nodes</td>
</tr>
</tbody>
</table>

Network Experiment is conducted on the factors such as network overhead rate, secure message forwarding rate and acknowledgement attack rate (i.e., reduces forged acknowledgement attacks).

SIMULATION RESULTS

In this section, the result analysis of secure message broadcasting framework using SRA-MDS model in mobile ad hoc network is compared with existing EAACK [1], UA-ID [2] and KM-LSN [21]. Simulation results are measured and the values are compared shown in below.

F. Impact on Network Overhead

Network Overhead (NO) using SRA-MDS model is the difference between the messages sent to the successfully messages received. Network Overhead rate is measured in terms of bytes. Lower the network overhead rate, more efficient the method is said to be.

\[ NO = (Message_s − Message_r) \]

(15)

From (15), ‘Message_s’ denotes the Message sent (in terms of bytes) whereas ‘Message_r’ denotes the bytes received.

![Figure 3 Measurement of Network overhead with respect to message sent in bytes](image)

A better insight into the simulation results for network overhead is illustrates in Fig. 3. In figure, the message sent varies between 64 bytes to 2048 bytes. On the other hand, the messages received at the destination vary according to the proposed and existing EAACK, UA-ID and KM-LSN methods. When the message sent was 512 bytes, the message received was 480 bytes using the proposed SRA-MDS and 470, 462 and 457 bytes using the existing EAACK, UA-ID and KM-LSN respectively. Therefore, the network overhead rate is for the four methods are 33 bytes, 44 bytes, 52 bytes and 55 bytes respectively. Sender Route Authentication with Multi-bit Digital Signature (SRA-MDS) model is compared against the existing EAACK, UA-ID and KM-ECC. From the figure, it is illustrative that the
The network overhead is minimized using proposed Sender Route Authentication with Multi-bit Digital Signature (SRA-MDS) model when compared to the two other existing works. This is because with the application of the Sender route authentication evaluates the confidence and probability measure efficiently authenticates the route and significantly reduces the network overhead rate by 37.52% compared to EAACK [1]. Furthermore, using a confidence correlation, the source node identifies packet-forwarding to neighboring nodes with minimum network overhead rate by 70.29% compared to UA-ID [2] and 81.11% compared to KM-LSN [21] respectively.

**G. Impact of Forged acknowledgement attacks rate**

Forged acknowledgement attacks refer to the rate of attack made through forged acknowledgement. It is measured in terms of percentage (%). Lower the forged acknowledgement attacks, more efficient the method is said to be.

![Figure 4 Measurement of Forged acknowledgement attacks rate](image)

The comparison of forged acknowledgement attacks is presented in Fig. 4 with respect to the varying number of messages and message sizes in the range of 64 – 2048 bytes. With increase in the number and size of messages, the forged acknowledgement attacks are also increased. As shown in the figure with the increase in the message size, the forged acknowledgement attacks are increased in all the methods. But comparatively it is reduced using proposed SRA-MDS model. This is because of, route selection is performed for message broadcasting using authentication and verification algorithm. This algorithm performs message broadcasting through the values of sender route authentication and probability measure reducing the forged acknowledgement attacks by 8.37% compared to EAACK[1], 2.62% reduced compared to KM-LSN [21] and reduced to 3.76% compared to UA-ID [2] respectively.

**H. Impact of Secure message forwarding rate**

Message forwarding rate is defined as the ratio of number of messages received to the messages being sent and it is measured in terms of percentage (%). The formulation for message forwarding rate is given as below,

\[
MFR = \frac{\text{No.of messages received}}{\text{No.of messages sent}} \times 100
\]

Fig. 5 depicts the message forwarding rate attained using number of messages sent at the range of 10 to 35 with varying sizes at different simulation periods using NS2. From the figure, the value of message forwarding rate achieved using the proposed SRA-MDS model is higher when compared to two other existing techniques namely, EAACK [1], UA-ID [2] and KM-LSN [21]. In addition, while increasing the number of messages being sent, the message forwarding rate is increased using all the methods.

![Figure 5 Measure of message forwarding rate with respect to number of message sent](image)

But comparatively, it is higher in SRA-MDS model because the SRA-MDS model applies the MDS algorithm for single instance digital signature with multiple bits that highly secure the broadcasted message improving the message forwarding rate by 7.68% compared to EAACK [1]. In addition, with the effective selection of in-between mobile nodes, with the key differing for each source-destination pair, the message forwarding rate improves by 16.68% compared to UA-ID [2] and 22.10% compared to KM-LSN [21] respectively.

**CONCLUSIONS**

This paper proposed an effective and secured message broadcasting model to provide accurate results using multi-bit digital signature in MANET. The objective of secured message broadcasting model is to reduce the network overhead by evaluating the confidence and probability measure through sender route authentication in MANET which significantly contribute to the relevance. To do this, a confidence correlation measure to determine the route authentication for the source and neighbor nodes to determine the authenticated route. Based on this measure, a new authentication and verification algorithm is applied which reflects the weights of confidence value and probability measures and to perform message broadcasting. In addition, security was also provided for the route being selected by applying the Multi-bit Digital Signature (MDS) algorithm based on the digital signature generation and digital signature verification. Through the simulation, our MDS algorithm provided more accurate secured message broadcasting in MANET. In addition, the proposed authentication and verification algorithm effectively reduced the forged acknowledgement attacks and improved the performance rate of message being broadcasted when compared to the state-of-the-art works. To increase the merits of our research work, it is our plan to investigate the following issues in future research:

1) Possibilities of adopting k deterministically from the private key to further improve the security model caused by Multi-bit Digital Signature (MDS) algorithm;
2) examine the possibilities of adopting a cryptographic hash function to minimize the network overhead;

**REFERENCES**


