Journal of Theoretical and Applied Information Technology
15st September 2026. Vol.104. No.17

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

MODIFIED FLEXIBLE NODE AUTHENTICATION FOR MANETS: HASH CHALLENGE–RESPONSE FOR SECURE DYNAMIC SOURCE ROUTING (DSR)

AHMAD K. ALOMARI
Faculty of Science and Information Technology, Jadara University, Irbid, Jordan
Emails: a.alomari2@jadara.edu.jo

ABSTRACT

Mobile Ad Hoc Networks (MANETs) are a novel technology that has a dynamic topology, self-configuring, and self-motivated. The primary feature of an ad hoc network isn't dependent on any established infrastructure because it lacks a centralized arbiter or server. Wireless MANETs have several issues, including performance analysis, energy efficiency, security, and network stability. To date, a great deal of research has been conducted to create security strategies for MANETs. The current strategies that aim to build a defense against different types of attacks at different levels will be covered in this analysis. Researchers therefore create several routing protocols. Wireless networks cannot effectively employ the routing methods designed for conventional networks. A few novel routing methods have been developed for wireless ad hoc networks that are appropriate for the constantly evolving ad hoc wireless environment. In this study, we proposed a technique to improve the efficiency of routing protocols and boost node-to-node dependability in mobile ad hoc networks (MANETs). Our system focuses on node authentication, and we use an on-demand routing protocol, such as the Dynamic Source Routing protocol (DSR), to implement it. This technique relies on the hash function, secret value, and time stamp.
Keywords: *MANETs, Routing protocols, hash function, DSR, source node, destination node.*

1. INTRODUCTION

In recent years, we have been witnessing a tremendous growth of wireless communication technologies. The wireless network infrastructure exhibits significant progress, making the availability of wireless applications increase constantly. Wireless devices, such as laptops, tablets or smartphones, can be found everywhere, and they are all getting strongerin what it concerns their capacities. The importance of these gadgets in our daily lives is growing.

Wireless technologies are now popular for several reasons. Due to the substantial decline in the cost of wireless devices, service providers are now able to drastically lower the cost of wireless services, making them considerably more accessible to end customers [1]. In emerging markets, wireless network installation is significantly less expensive than conventional network installation. Voice and data services may now be offered via these networks because of significant advancements in wireless technology. Because of the ensuing appeal, anytime, anyplace services are very desirable to end consumers.

Wireless networks come in two varieties: The first kind is an infrastructure-based network, which is a network with reconstructed infrastructure consisting of wired and fixed network nodes and gateways. Typically, these preset infrastructures are used to supply network services. The second kind is infrastructure less (ad hoc) networks, where an arbitrary collection of independent nodes collaborates to create a network on the fly [2]. There is no prior agreement on the precise function that each node should perform.

One of the fields of study that is expanding the quickest right now is mobile ad hoc networks, or MANETs. High-degree node mobility and wireless communication are combined in this novel kind of self-organizing network. Thus, even in places without an established communication infrastructure, people and cars may be operated online. These networks lack established infrastructure, such as base stations and centralized administration centers, in contrast to traditional wired networks [3]. The type of typology this association of nodes forms is arbitrary. While nodes within radio range can interact directly with one another, nodes outside of that range must employ an intermediary node or nodes to connect in a mobile ad hoc network. In these two scenarios, a wireless network is automatically formed by all of the nodes participating in the communication

process. Consequently, one may refer to this kind of wireless network as a mobile ad hoc network.

This kind of flexibility makes them attractive for many fields of application, for example, in the military field, where the network topology may change rapidly. When deployed to combat, military forces (such as infantry, tanks, or aircraft) that are outfitted with wireless communication equipment are more effectively connected. In disaster recovery activities, where the fixed or current infrastructure may not be functioning, this kind of network is also used [4]. Because of their ad hoc self-organisation, they are especially appropriate for virtual conferences, where establishing conventional network infrastructures is an expensive and time-consuming process.

Due to this increased applicability, security matters in the mobile ad hoc networks must be better looked at, as the basic functions of conventional networks (packet forwarding, routing, and network management) are carried out by dedicated nodes. In ad hoc networks, these functions are performed collaboratively by all the available nodes. In these types of networks, the communication between the nodes is done through a multi-hop system. Wireless links are used for direct communication between the nodes that are within each other's radio range. For the nodes that are not within each other's radio range, one or multiple intermediate nodes are used to ensure successful communication [5]. Those intermediate nodes act as routers. In mobile ad hoc networks, as their name says, the nodes are free to join, leave or move inside the network. Due to this dynamic topology, there is a constant need for the routes to be updated.

As seen above, because ad hoc networks allow a great freedom of movement for the nodes that join them, this means that the network topology has a configuration that can change rapidly. This changing nature of the nodes is unpredictable, as it takes place at random. This type of topology, together with a lack of infrastructure and wireless connectivity that is prone to error, has a considerable effect on the network because it leads to recurrent link breakages. By adopting a completely dispersed and self-organizing character, MANET protocols must lessen the unreliability of fundamental network functions [6]. Distributing network service functionality among as many nodes as feasible prevents a single point of attack from a security standpoint. Taking into consideration that MANETs have unique characteristics, the mechanisms used to secure conventional networks are more likely to be unsuitable or cannot be adapted to fit the security needs of ad hoc networks. For this purpose, MANETs need to be equipped with specialized mechanisms and protocols.

It has been difficult to come up with a comprehensive general solution; most of the solutions proposed so far focus on some particular security vulnerabilities [4]. A view of the bigger picture is needed for MANETs to be provided with efficient general solutions, i.e. we have to first fully understand all the vulnerabilities and security risks of this type of network. As there are still many issues to be solved regarding the deployment of security for the routing protocols of MANETs, a lot of investigation still needs to be conducted for the development of appropriate solutions to these issues. At this point, the critical issue that poses the biggest challenge in this field is that of security, so the focus must be on the design of specialised solutions to keep these networks safe.

In this paper, we are attempting to improve a scheme used in different kinds of routing protocols which aim to resist different forms of attacks like eavesdropping, man-in-the-middle attack, routing attack and wormhole attack.

2. RELATED WORK

Many articles have been published to demonstrate how the security of routing protocols can be improved, and most of them were proposed by Singh, Singh, and Gupta, who presented a study on security and energy-efficient design strategies for Mobile Ad Hoc Networks (MANETs) [7]. The authors examined the difficulties posed by dynamic topology, limited energy at nodes, and security threats that undermine network performance. Their work describes different attack types in MANETs, including active attacks such as black hole attacks and passive attacks such as traffic monitoring. To enhance network reliability and security, the study uses the LEACH (Low Energy Adaptive Clustering Hierarchy) protocol, which lowers energy consumption through effective cluster formation and cluster-head selection. The authors also investigated clustering methods such as K-Means and Mean Shift clustering to organize nodes and optimize communication. The proposed solution applies setup and steady phases to handle data transmission while minimizing power consumption. In addition, the study underscores the significance of secure routing, authentication, availability, and data integrity in MANET environments. Simulation outcomes showed that the proposed approach extends network lifetime, increases the number of alive nodes, and improves data transmission performance even when malicious nodes are

present. The results suggest that integrating clustering mechanisms with energy-aware routing protocols can substantially strengthen MANET security and efficiency while preserving reliable communication in highly dynamic wireless networks.

3. Pillai, Kumar, and Ajina presented a comprehensive survey of security issues in Mobile Ad Hoc Networks (MANETs) [8]. The study emphasizes that MANETs are especially susceptible to security threats because of their decentralized architecture, dynamic topology, limited battery power, and open wireless medium. The authors reviewed major network weaknesses, including the lack of secure boundaries, the absence of centralized management, restricted power resources, and scalability limitations. The survey further grouped attacks into passive and active categories, addressing common threats such as black hole, wormhole, flooding, spoofing, replay, rushing, and denial-of-service attacks. The paper also identified key security requirements for MANETs, including availability, integrity, confidentiality, authenticity, non-repudiation, and anonymity. To tackle these issues, the authors reviewed multiple security mechanisms, including intrusion detection systems, cluster-based intrusion detection techniques, secure routing protocols, watchdog and pathrater approaches, and methods for preventing wormhole attacks. Moreover, the survey considered secure routing strategies based on authentication, trust management, neighbor verification, message randomization, and encryption techniques. The study concluded that although substantial progress has been achieved in securing MANETs, the dynamic and infrastructure-less character of these networks continues to generate security challenges that call for stronger and more adaptive protection mechanisms.

4. Nargunam, Bose, and Nayagam proposed BioTrust-QoS, a bio-inspired, QoS-aware, and secure routing protocol for IoT-based Mobile Ad Hoc Networks (MANETs) [9]. The work targets key challenges in MANETs, including dynamic topology, constrained energy resources, routing instability, quality-of-service requirements, and security threats. The proposed protocol unifies bio-inspired optimization, adaptive trust management, machine learning-based mobility prediction, and QoS-aware routing within a single framework. BioTrust-QoS applies Modified Proportional Topology Optimization (MPTO) to enable efficient cluster formation, and it uses Enhanced Seeker Search Optimization (ESSO) along with a Multi-Objective Trust-Centric Flower Pollination Algorithm (M-TCFPA) to select cluster heads. For enhanced security, it introduces a multidimensional trust model that judges nodes according to QoS performance, social behavior, and energy status. In addition, a Multi-Layer Deep Recurrent Neural Network (ML-DRNN) forecasts node mobility and proactively repairs routes before link failures arise. The protocol also integrates an Intelligent Dynamic Trust (IDT) model and intrusion detection mechanisms to recognize malicious nodes and counter attacks such as black hole, selfish, wormhole, and denial-of-service. Simulation outcomes showed marked gains in packet delivery ratio, throughput, attack detection rate, and end-to-end delay relative to conventional protocols including AODV, ESCT, and ETRS. Overall, the results suggest that integrating bio-inspired optimization, adaptive trust evaluation, machine learning, and QoS awareness can significantly improve both security and performance in IoT-based MANET environments.

5. Alomari proposed a mutual authentication mechanism for Mobile Ad Hoc Networks (MANETs) intended to strengthen trust among communicating nodes while preserving secure network operation [10]. The study examines the problem of authenticating nodes in a decentralized setting, where the lack of fixed infrastructure makes traditional security approaches difficult to deploy. The proposed method allows both communicating parties to verify each other's identity before initiating a communication session, thereby lowering the likelihood of impersonation and unauthorized network access. Moreover, the protocol includes an authentication key updating procedure to improve long-term security and reduce the effect of compromised credentials. The key renewal mechanism refreshes authentication information periodically without creating substantial communication overhead. The author assessed the proposed scheme in terms of security effectiveness, authentication reliability, and operational efficiency under dynamic network conditions. The results indicated that the protocol enhances resilience to common security threats while sustaining acceptable performance. Additionally, the mutual authentication procedure strengthens trust relationships among mobile nodes and enables secure communication in rapidly changing network topologies. The study concludes that combining mutual authentication with dynamic key updating offers a feasible and effective approach for improving security in MANET environments.

3. DIFFERENT ATTACKS OF MANETs

First of all, ad hoc networks must be defended against passive attacks, which can be done with the help of the following tools: digital signature, authentication, encryption and access control [11, 12,21]. Another challenge is represented by the protection against active attacks. Iintrusion and the number of selfish nodes also pose a problem that needs to be taken care of ssymmetric and asymmetric cryptography constitute the basis of encryption and authentication. In the following sections, we shall examine several assault types and their behavior in the sections that follow. The experiments and the reactions of the components to some of the attacks that have been demonstrated in real life were observed.

Eavesdropping (passive attack)
The attacker snoops on the network in order to collect data, getting access to private information regarding the topology, optimal routes and geographic locations in the network while the information is being routed. In this case, the attack is very hard to detect, and vital information such as the node's private and public key, password, etc., can be compromised. It is much easier to conduct this type of attack in a mobile ad hoc network than in a wired network [12].

Denial of Service (DoS)
This attack aims to make a specific node not available for service. The entire service could be compromised if someone uses this type of attack. Denial of Service is the outcome of tampering with network integrity, redundancy and availability. In this type of attack, an adversary wants to use the node's resources or network bandwidth by overflowing the network with insignificant information [10].

Wormhole attack
In MANETs, it is among the most advanced and serious assaults. The attacker can tunnel the received message, which is transmitted over a short latency, by joining two components that are located at a predetermined distance from one another. A compromised node from a different part of the network receives the message through a path located outside the network, which makes the attack very difficult to detect, because the path through which the data is transmitted does not belong to the real network.

Black hole attack
In this case, all the traffic is rerouted and lured to a compromised node, which becomes a black hole. These malicious nodes trick all their neighboring nodes into attracting all the routing packets to them. Malicious nodes might initiate black hole attacks by promoting themselves to other nodes as having the best path to the desired destinations, which is how they are very similar to wormhole assaults.

Snooping attack
Duringthistypeofattackpackets ofthenodesareaccessedwithoutpermission.Because in MANETs, packets are communicated hop by hop, any malicious node can capture other packets [12].

Routing attack
Routing tables get deleted or modified by malicious nodes, causing packet overhead and increased processing time due to the destruction of the routing information table in ordinary nodes.

Man-in-the-middle attack
A rogue node positions itself between the source and the destination in this attack. After that, all packets are captured and either dropped or altered. MANETs are especially susceptible to this assault since they employ hop-by-hop transmission. Cryptography and authentication are the best defenses against this assault.

Fabrication Attack
By injecting fault information, the rogue node creates fault routing pathways and destroys the nodes' routing table [12]. Consequently, nodes squander network resources by sending their packets over flawed paths. An increase in lost packets and a decrease in packet delivery rate.

4. AUTHENTICATION PROTOCOL OF MANETS

The major types of ad-hoc routing protocols are: Proactive routing protocols: routing tables are updated through recurrent message sending. The most important protocols of this type are: OLSR (Optimised Link State Routing protocol) and DSDV (Destination-Sequenced Distance Vector).
Reactive (On-Demand) routing protocols: routes are generated only when necessary. Two of the most important protocols of this kind are: DSR (Dynamic Source Routing protocol) and AODV (Ad hoc On-Demand Distance Vector Routing protocol).

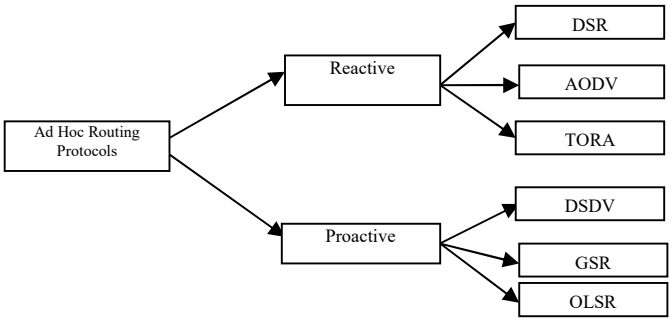

Figure 1: Types of ad hoc routing protocols

These protocols are differentiated by the manner in which the routing data is updated, identified, and what kind of data each routing table keeps. Various numbers of tables can be stored by every routing protocol. Multiple routing protocols for ad hoc networks were created to ensure security and authentication between the nodes. In this paper, we propose security schemes which can be applied to most of the routing protocols. To apply our schemes, we use the Dynamic Source Routing protocol (DSR) due to its popularity and frequent usage [13, 14].

Our paper has been done on the verification between the nodes. Mobile ad hoc networks that use authorized nodes are becoming more and more available to general use and also a research topic with increased importance over the last few years. Mobile nodes, which may function as both senders and forwarders for messages, make up the structure of a MANET. Our focus will be on a unique aspect of these protocols, which is the ability to identify routes, which helps to overcome the network's dynamic topology limitation [13, 15-16]. Mobile ad hoc networks provide two security challenges. Communication between the nodes is made possible by the security of the routing protocols, which is the first issue. The protection of the data that is moving across the network along routes set by the routing protocols is the second issue. In an ad-hoc network, there are two kinds of attacks: passive attacks and active assaults.

Our proposed idea utilizes hash functions, although digital signatures can be used as well. To acquire strong security, the scheme of SAODV (Security AODV: represents an AODV extension) includes algorithms that use digital signatures and hash chains to accomplish the security on different levels. The digital signature is attached to every node to provide integrity and authentication for the messages concerning the routing: RREQ, RREP and RRER. All the neighbor nodes that receive the packet verify the digital signature. The hash chains are used to secure the hop-count mechanism [17-19].

In this scheme, we use the random number generator, besides the one-way hash function. We use this method to improve the communication between the nodes and to perform node authentication. The steps of this scheme are explained in Figure 2. In our scheme, we still use a digital signature and time to live (TTL). Where TTL lists the number of times this message can be resent and the digital signature is attached to every node to provide integrity and authentication for the messages sent between two nodes.

Parameters used: ID_s: identity of the source node; ID_d: identity of the destination node; N_s: Random number generated by source node; N_d: Random number generated by destination node; PK_s: Public key of the source node; PK_d: Public key of the destination node; $H(x)$: secure one-way hash function; k: Secret value.

Secret Value k Distribution with Confidentiality and Authentication: We can use the public key to exchange the secret value to provide protection against both active and passive attacks.
Diffie-Hellman Key Exchange: The Diffie-Hellman algorithm's efficiency depends on the hardness of computing discrete logarithms.

Our approach is based on a practical one-way hash function. We also deliver a theoretically stronger foundation on Pseudo-Random Function (PRF).
As stated before, in this scheme we use the random number generator, besides the one-way hash function. To improve the communication between the nodes, we use this method to perform node authentication, and we explain it as follows:

- The source node S wants to communicate with the destination node D, as illustrated in Figure 2. Node S first produces a nonce N_s and encrypts that value with the public key of destination node $E_{PK_D}(N_s)$. The source node sends it with the request message to the destination node D.
- When the destination node receives the message from the source node, directly or by intermediate nodes, if it is out of the range of the source node, the destination node decrypts the value $E_{PK_D}(N_{si})$ using its private key to get

N_s. After that, D the node generates N_d and computes $f_1 = H(ID_d \oplus N_s \oplus N_d)$ and sends it with the time stamp (T_d) and $E_{PK_S}(N_d)$, where PK_s is the public key of the source node, to the source node.

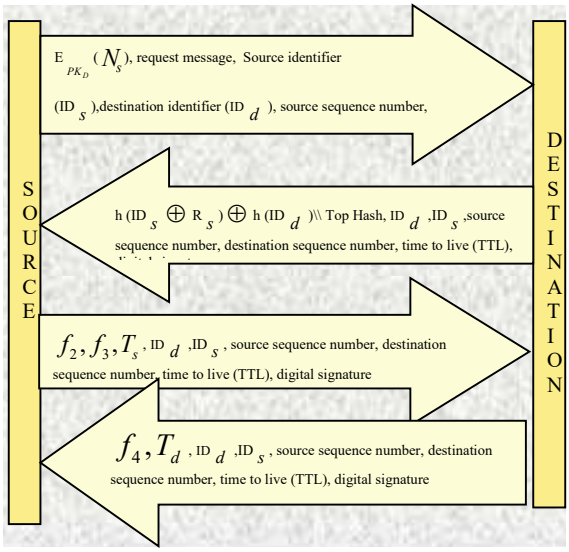

Figure 2: Authentication Improvement In Routing Protocols Of Manets

- When the source node receives $f_1 E_{PK_S}(N_d)$ values from the destination, it verifies the time of the message by comparing the current time of the source node with the destination node's time. If the message is accepted, the source node will get N_d by decrypting $E_{PK_S}(N_d)$ using the private key. After that, the source node looks for the identities of the destination node ID_i, such as $1 \le i \le n$ the number of nodes in the MANETs, by computing $f_i = (ID_i \oplus N_s \oplus N_d)$ and making the following comparison $f_i \stackrel{?}{=} f_1$. If the destination node passes the authentication of the source node, it is considered legitimate; otherwise, it is ignored. After that, the source node computes and sends this message to the destination node with the new time of the source (T_s).

- When the destination gets the last value from the source node, it checks $T_d > T_s$. If it is valid, the node D starts the authentication process by computing f_2 again. After that, it checks if $N_d^* = f_2 \oplus H(k_i \oplus N_s) \stackrel{?}{=} N_d$. For the last authentication process, the destination node computes $f_3^* = H(ID_i \backslash\backslash N_d \backslash\backslash N_s \backslash\backslash k)$ and sees if $f_3^* \stackrel{?}{=} f_3$. Finally, the destination node produces $f_4 = H(ID_d \oplus N_d \oplus N_s \oplus k)$ and sends it with the new time T_d to the source node.
- When the source receives the last value from the destination node, it starts the last verification process by checking $T_s > T_d$ and computing $f_4^* = H(ID_d \oplus N_d \oplus N_s \oplus k)$ to see if it matches the received value $f^*_4 \stackrel{?}{=} f_4$.

The source and destination authenticate each other. Naturally, the hash value is authenticated together with the destination ID that is contained as a component of the hash value.

1) Case Study (Example by Using DSR)

We choose the Dynamic Source routing protocol to apply our proposed scheme with nonce and secret value k. In this protocol, communication is started with the first RREQ message sent by a node. This means that the first stage of the routing process is deployed: the route discovery process. The RREQ travels with the source's digital signature DS attached. The neighbors which receive the RREQ examine the signature of the source and, thereupon, take a decision. To support message integrity, we still use the one-way hash function. Destination sequence number is also utilized in order to avoid the formation of loops and to verify if the route is also the newest one.

We presume that the source node S is attempting to find a route to the destination node D. There is a route $S\ D$ that goes through intermediate nodes $X\ G$. We still use here L: life time of the package (maximum number of hops), DSS: Digital signature of node S, h_S: Hash value added by the source node to the packet.

The operations of our protocol will work as explained below: A RREQ is generated by the source node S, with the time stamp of the source node, to initiate route discovery. RREQ includes several parameters, enumerated as follows: source

address, destination address, Seq, LREQ, authentication request (auth req), DSS digital signature of source, hash value h_S and a routing table that includes all the intermediate nodes which find themselves on the path from S source to D destination. A message can be broadcast a limited number of times. This number is known as the lifetime of a packet. Every broadcast automatically decreases the lifetime number by one. If the time number reaches zero, the packet will be dismissed. Source produces the h_S output using a one-way hash function.

$$h_S = H(S, D, \text{Seq, LREQ})$$

When a neighbour of S, for example X, receives the RREQ message with T_s, the first thing it does is to check the DS of S. If S passes the examination and it is considered authentic, the intermediate node X proceeds in verifying the Seq and matches it with the one that it has stored in its cache. X dismisses the packet if the Seq stored is higher than the Seq received. If Seq is equal to or higher, the node X adds its identifier to the route list and digital signature $DS\ X$ to the message and replaces the h_S by h_X and then rebroadcasts

$$h_X = H(h_S, X, \text{LREQ -1}), \text{E}_{PK_D}(N_s).$$

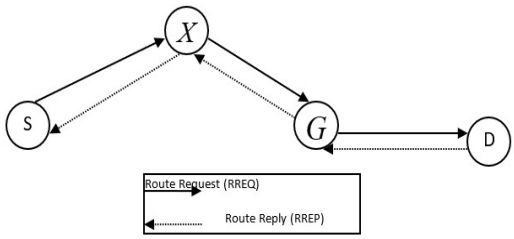

Figure 3: Broadcasting routing request and routing replay

This procedure is similar for the next neighbor node G. It checks both signatures of S, X and after that, it verifies the sequence. When the checklist is completed, it adds its identifier to the route list and a digital signature DSG to the message, it replaces the h_X by h_G, and finally rebroadcasts.

$$h_G = H(h_X, \text{E, LREQ-2}), \text{E}_{PK_D}(N_s).$$

Finally, the RREQ arrives at the destination node D with the source's time stamp T_S, which ensures the value $T_d < T_s$. After that, it checks all the signatures included in the RREQ message and matches the Seq with the previously stored Seq in its cache. If the examination concluded that S and the intermediate nodes are valid and the packet is up-to-date, D it calculates: $h_D = H(G, \text{LREQ-2, H}(X, \text{LREQ-1}, H(S, D, \text{Seq, LREQ})$ and confronts the value of h_D with h_G. If both values coincide, the integrity of the packet is authenticated. Otherwise, the message is discarded. If all the parameters pass the examination, the destination node generates a nonce N_d, and then it computes $f_1 = H(ID_d \oplus N_s \oplus N_d)$.

Finally, the destination node D generates a RREP, which it sends back S on the same route that RREQ arrived, only in reverse. Route Reply (RREP) message also includes some parameters, enumerated as follows: Seq, source address, destination address, route list, h_D, (T_d) and $\text{E}_{PK_S}(N_d)$ and a list with all the signatures of the intermediate nodes from source to destination. Every intermediate node follows the same procedures as when it receives a RREQ: checks the signature of D and verifies Seq to establish how fresh the route is. When RREP arrives S, this checks the signatures of all the nodes in the route list and Seq. Source S computes:

$$H = H(G, \text{LREQ-2}, H(X, \text{LREQ-1}, H(S, D, \text{Seq, LREQ})))$$

and compares with h_D to verify the integrity of the route list. If the values are equal, S it accepts RREP. Otherwise, the packet is dismissed. S Calculates the values of LREQ-1 and LREQ-2 based on the route list. After that, the source node creates a response to the destination node by generating

$$f_2 = H(k \oplus N_s) \oplus N_d$$

$$f_3 = H(ID_d \backslash\backslash N_d \backslash\backslash N_s \backslash\backslash k)$$

Sending it by the same path to the destination node. In the end, the destination verifies this value and, if it matches, the authentication process has succeeded. After all the procedures and the examinations are completed, a route is

established from the source node S to the destination node D.

5. SECURITY ANALYSIS

In this section, we explain how we achieved the mutual authentication between the nodes in MANETs, and then we explain how the scheme acts with different kinds of attacks.

Achieve Mutual Authentication
The process of mutual authentication is obtained after the secret shared value *k* is verified, i.e. it is the same at both ends of the communication. Also, the destination node has to certify that the last message received is from the source node. At this point, it is assumed that secure communication between the source node and the destination node has taken place. Our scheme guarantees the authentication of the source node through the secret shared value *k*. This prevents any compromised node from disturbing the communication process, as it will be detected when it tries to communicate with the destination node. The destination node will start the authentication process whenever it receives a challenge from the source node. It is also important for the authentication process to take place in a single session. To ensure this, timestamps are also employed in our scheme.

Anonymity, Untraceability and Eavesdropping
Anonymity and untraceability can be obtained through the use of a nonce (random numbers). The nonce must be added to each authentication request made by either the source node or the destination node. The source is notified that the destination is authenticated through a final hashed message sent by the destination. This step is to keep the destination node anonymous and untraceable. Once again, the messages must take place in the same authentication session. To make sure of this, the use of timestamps is again needed.

Our authentication scheme provides full protection against future forward and backwards traceability. The adversary has no control over nonce values N_s, N_d and the combination of N_s, T_s, T_d a hash function and also does not know the secret value k. All values between the source and destination nodes will be unique in each session and replaced after each successful session, which provides a high level of privacy.

Eavesdropping
Because the communication between the source node and the destination node is encrypted with a public key and the shared secret value is hashed with a nonce, an eavesdropping attack is unlikely to succeed because a malicious node cannot take part in the exchange between the source and the destination.

Impersonation Attack Resistance
During the communication, all the values are hashed and XORed. This prevents a node impersonation attack. Our scheme also proposes the use of updated nonce, i.e. random numbers, for each communication between the source and destination nodes, making the resistance stronger. The result of our scheme shows that the nodes communicate with each other in MANETs through a secure channel.

Man-in-the-Middle Attack
After the mutual authentication process takes place, the messages cannot be modified by an attacker because future communication is performed and controlled by two authenticated parties. In each new communication, the secret value k is updated, as well as the random nonce numbers. After its authentication, the destination is protected until the completion of the session. The security level is also increased by the use of hash functions on the messages.

Denial of Service Attack (DoS)
DoS attacks are very tricky to detect, and oftentimes, some manage to pass undetected. The objective of the protocol is to take action against the vulnerability presented by a DoS attack, avoiding the desynchronization of the system. Because our scheme is enhanced with timestamps, an active attack on a node is impossible. This is due to the fact that the previous timestamp is always stored by the node, which will not allow any other authentication to take place until it receives a timestamp higher than the previous one. Due to this monotonically increasing timestamp, an impersonation and replay attack is not possible. In case of an attempt to use a higher fake timestamp, this protocol is also at an advantage: the node does not update its timestamp unless a successful authentication is performed. This prevents the protocol from DoS attacks.

Journal of Theoretical and Applied Information Technology
15st September 2026. Vol.104. No.17

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

6. SIMULATION SETUP AND PERFORMANCE EVALUATION

This section tests authentication enhancements for on-demand data routing by comparing the standard protocol with its secure versions under both standard and simulated routing attack conditions. The study aims to measure two specific operational impacts: (a) the operational costs resulting from adding new security fields, and (b) the improved security performance that enables the detection of active threat attacks.

Simulation Setup

The mobile ad hoc network for its nodes allows for communication across multiple wireless hops. The same mobility and data traffic conditions were used to test all protocols in each scenario, and the average results were calculated using different random seed values. The secure variables follow the mutual authentication mechanism (random number, timestamp, secret value, hash/cryptography) and authenticated path discovery described previously in this paper (Figures 2-3).

Table 1: Baseline Definitions Used In The Evaluation

ID	Protocol	Security fields	Expected effect
B 0	Standard DSR (vanilla)	None	Lowest delay/overhead; weakest under attacks
B 1	DSR + routing integrity	Hash + signature on routing control packets (RREQ/RREP/RERR)	Blocks many forged control packets; moderate overhead
P	Proposed full scheme	Nonce + timestamp + secret value + encryption + hash/signatures	Strongest against injection/replay/MITM; highest overhead

Attack Injection Model

We conduct effective attacks that mimic real-world threats to test security claims during route discovery and packet redirection. The experiment involves malicious nodes that we introduce with specific control ratios to test their ability to execute black hole traffic attacks that drop all incoming traffic, wormhole control tunnel attacks between two complicit nodes, middleman attacks that alter routing information and payload data, routing spoofing/poisoning attacks that generate fake routing control messages, and denial-of-service attacks that consume network bandwidth and processing power through persistent routing requests and authentication attempts.

Table 2: Attack Injection Parameters (Typical Configuration)

Attack	Injected action	Knobs (varied in experiments)
Black hole	Advertise attractive route; drop data packets	Malicious node ratio = {0,10,20,30,40}%; drop rate = {50-100}%
Wormhole	Tunnel RREQ/RREP via colluding pair	Tunnel delay; distance between colluding nodes; malicious node ratio
MITM	Modify routing fields/payload in transit	Modified packet ratio; malicious node ratio
Fabrication	Forge routing control messages (fake RREP/RERR)	Forged message rate (pkts/s); malicious node ratio
DoS flooding	Flood route requests/authentication attempts	Flood rate (pkts/s); malicious node ratio; acceptance time window

Metrics and Result Presentation

The study presents results including packet delivery ratio (PDR) measurements and average end-to-end latency, as well as good throughput/performance values and calibrated routing load data. Security test results show authentication success rates and spoofed message rejection rates, measured under each type of intrusion attack. Distribution charts (graphs) present average values, along with tail behavior (e.g., delay during an attack) and path distortion behavior (e.g., number of hops in a wormhole scenario).

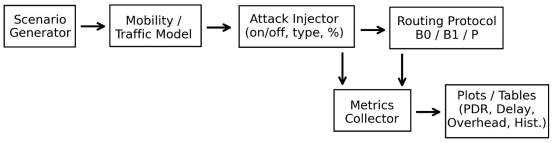

Figure 4: Simulation Pipeline With Attack Injector And Baseline Selection (B0/B1/P)

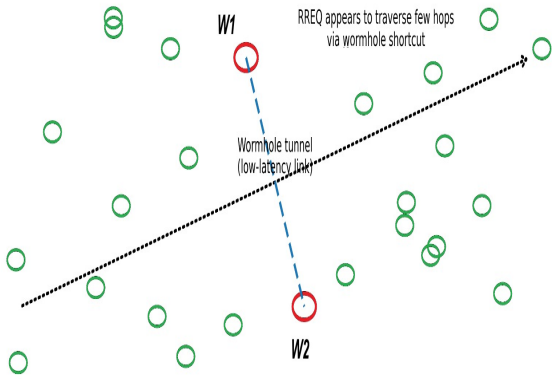

Figure 5: Wormhole Injection Illustration (Colluding Nodes And Low-Latency Tunnel)

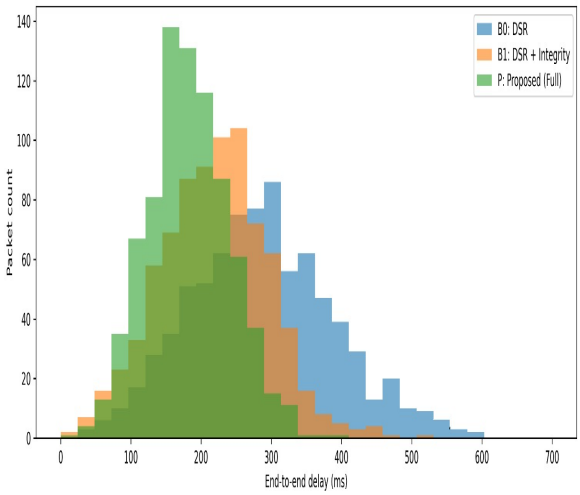

Figure 6: Histogram Of End-To-End Delay Under 20% Malicious Nodes (B0 Vs B1 Vs Proposed)

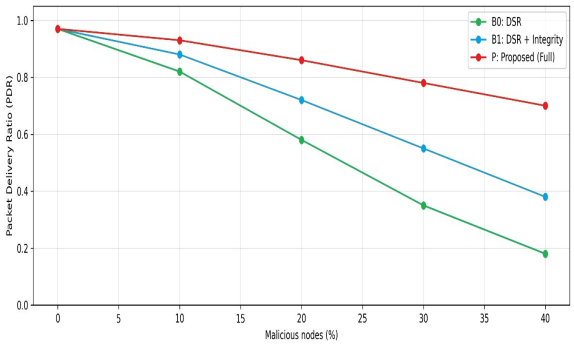

Figure 7: Packet Delivery Ratio Versus Malicious-Node Ratio Under Black Hole Injection (B0/B1/Proposed)

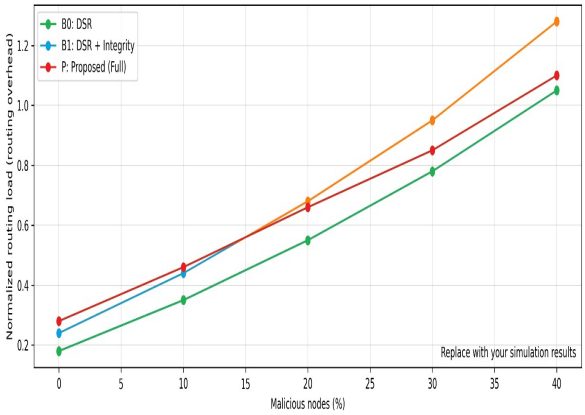

Figure 8: Normalized Routing Overhead Versus Malicious-Node Ratio Under Dos/Fabrication Injection (B0/B1/Proposed)

Simulation Parameters

Table 3 presents standard parameter settings that researchers can use in simulation experiments with NS-2/NS-3/OMNeT++. These values can be modified to achieve the deployment range and mobility assumptions specified in the research paper.

Table 3: Simulation Parameters (Recommended Defaults; Adjust As Needed)

Parameter	Value
Number of nodes	50 (also report 25/75/100 for scalability)
Terrain size	1000 m x 1000 m
Radio range	250 m
MAC/PHY	IEEE 802.11
Mobility model	Random Waypoint
Node speed	0-20 m/s
Pause time	0-30 s
Traffic model	CBR/UDP
Packet size	512 bytes
Offered load	10 flows; 4 packets/s per flow
Simulation duration	900 s
Repetitions	10 random seeds; report mean ± std (or 95% CI)

The results section begins with baseline curves illustrating security costs before presenting attack injection curves for each attack type. The study requires researchers to test each attack with varying percentages of malicious nodes, ranging from 0% to 40%. They are also required to provide a graph showing the distributional effects at 20% for each attack with different percentages of malicious nodes.

7. CONCLUSION

Current research on MANET network security is still in its early stages. Existing methods are beginning to reveal numerous security vulnerabilities, leading either to improvements in existing protocols or the creation of entirely new security protocols. This paper will present the most significant attacks on routing protocols, along with our secure methods for defending against them. The proposed system provides a higher level of security between nodes by improving authentication and enhancing data confidentiality protection. The proposed concept is based on hashing functions that enable the use of digital signatures. The system utilizes a hash function and a random (nonce) value with a secret value, and we explain how our system works within the Dynamic Source Routing (DSR) protocol. Our solution expands the security scope and provides more authentication services between nodes in MANET networks.

Acknowledgements: The authors are grateful to the Deanship of Scientific Research at Jadara University for providing financial support for this publication".

REFERENCES:

[1] B. K. Tripathy, S. K. Jena, and P. Bera, "An Adaptive Secure and Efficient Routing Protocol for Mobile Ad Hoc Networks," Wireless Personal Communications, vol. 114, no. 2, pp. 1339–1370, 2020.

[2] H. Yang, "A Study on Improving Secure Routing Performance Using Trust Model in MANET," Mobile Information Systems, vol. 2020, Article ID 8819587, 2020.

[3] N. Panda and B. K. Pattanayak, "ACO-Based Secure Routing Protocols in MANETs," in New Paradigm in Decision Science and Management, Springer, 2020.

[4] M. Sirajuddin, C. Rupa, C. Iwendi, and C. Biamba, "TBSMR: A Trust-Based Secure Multipath Routing Protocol for Enhancing the QoS of the Mobile Ad Hoc Network," Security and Communication Networks, vol. 2021, Article ID 5521713, 2021.

[5] N. Arappali and G. B. Rajendran, "MANET Security Routing Protocols Based on a Machine Learning Technique," Journal of Ambient Intelligence and Humanized Computing, vol. 12, pp. 6317–6331, 2021.

[6] V. K. Quy, V. H. Nam, D. M. Linh, et al., "Routing Algorithms for MANET-IoT Networks: A Comprehensive Survey," Wireless Personal Communications, vol. 125, pp. 3501–3525, 2022.

[7] P. Singh, A. P. Singh, and A. Gupta, *"Design Strategies for Mobile Ad-hoc Network to Prevent from Attack,"* Proceedings of the 3rd International Conference on Advanced Computing and Software Engineering (ICACSE 2021), pp. 194–201, 2022.

[8] Ashwini Pillai, Anurag Kumar, and Ajina, *"A Survey of Network Security in Mobile Ad-Hoc Network,"* IOSR Journal of Computer Engineering (IOSR-JCE), vol. 18, no. 5, pp. 29–36, Sep.–Oct. 2016.

[9] Shajin Nargunam A., Jebin Bose S., and Samuel Blessed Nayagam P. V., *"BioTrust-QoS: A Bio-Inspired, QoS-Aware, and Secure Routing Protocol for IoT-Based Mobile Ad Hoc Networks,"* International Journal of Engineering Research & Technology (IJERT), Vol. 15, Issue 04, April 2026.

[10] A. Alomari, *"Mutual Authentication and Updating the Authentication Key in MANETs,"* *Wireless Personal Communications*, vol. 82, no. 1, pp. 31–42, 2015. DOI: https://doi.org/10.1007/s11277-014-2169-1

[11] A. Altaweel, S. Aslam, and I. Kamel, *"Security Attacks in Opportunistic Mobile Networks: A Systematic Literature Review,"* *Computer Networks*, vol. 220, Article 109467, 2023.

[12] Baird, I. Wadhaj, B. Ghaleb, and C. Thomson, *"Impact Analysis of Security Attacks on Mobile Ad Hoc Networks (MANETs),"* *Future Internet*, vol. 16, no. 9, Article 321, 2024.

[13] Z. Kartit and O. Diouri, *"Security Extension for Routing Protocols in Ad hoc Mobile Networks: A Comparative Study,"* Proceedings of the International Conference on Advanced Intelligent Systems for Sustainable Development (AI2SD), ACM, 2019.

[14] M. Thakur and M. Kaur, *"Ad-Hoc Network Routing Protocols for Wireless Body Area Network,"* International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), 2017.

[15] S. K. Mishra and R. Gupta, "Secured Scheme for Privacy Preserving and Node Authentication Mechanism for a Special Mobile Ad hoc Network," International Journal of Computer Applications, 2018.

[16] M. Sirajuddin, C. Rupa, C. Iwendi, and C. Biamba, "TBSMR: A Trust-Based Secure Multipath Routing Protocol for Enhancing the QoS of the Mobile Ad Hoc Network," Security and Communication Networks, vol. 2021, Article ID 5521713, 2021.

[17] P. Rajendra Prasad and K. Shivashankar, "Enhanced Energy Efficient Secure Routing Protocol for Mobile Ad Hoc Network," Global Transitions Proceedings, vol. 3, no. 2, pp. 412–423, 2022.

[18] U. Srilakshmi, S. A. Alghamdi, V. A. Vuyyuru, N. Veeraiah, and Y. Alotaibi, "A Secure Optimization Routing Algorithm for Mobile Ad Hoc Networks," IEEE Access, vol. 10, pp. 14378–14393, 2022.

[19] S. Aluvala, et al., "Secure Routing in MANETs Using Adaptive Cuckoo Search and Entropy-Based Signature Authentication," Wireless Personal Communications, vol. 130, 2023.

[20] M. T. Rahman, M. Alauddin, U. K. Dey, and S. Saifullah, "Adaptive, Secure and Efficient Routing Protocol to Enhance the Performance of Mobile Ad Hoc Networks," Applied Computer Science, vol. 19, no. 1, pp. 134–150, 2023.

[21] Alomari, A. Fully distributed certificate authority based on polynomial over elliptic curve for MANET, International Journal of Networked and Distributed Computing, Vol. 2, No. 2 (April 2014), 70-77, DOI: https://doi.org/10.2991/ijndc.2014.2.2.1