



# Mutual authentication of nodes using session token with fingerprint and MAC address validation

Amit Kumar Bairwa, Sandeep Joshi \*

Manipal University Jaipur, Rajasthan, India

## ARTICLE INFO

### Article history:

Received 14 July 2020

Revised 7 February 2021

Accepted 30 March 2021

Available online 24 April 2021

### Keywords:

Trust

MAC address

OTP

Security

Nodes

SHA

Authentication

## ABSTRACT

Security has become an important issue during communication among mobile nodes in an unfavorable condition. The mobile node's property is dynamic, so it isn't easy to manage security policies. These difficulties present a barrier to building multigene security arrangements that accomplish both assurance and attractive network execution. The proposed work suggests the mutual authentication-based protocol, helping in the handshake between two nodes. Once they connected securely through this mechanism, they can interchange the required information. We have a monitoring node that will maintain the access list of the authorized nodes. The monitoring node will keep the nodes' list based on the MAC address of nodes and digital signature key. The key is generated by combining the hash code of the MAC address with the variety of the user's fingerprint file acting as a node. The combination of both will verify the entity. It involves the various subsections that include registering the user, token generation, sending and receiving messages through multiple algorithms. The proposed work is implemented using MATLAB. The analysis of the base work and the proposed work is visualized by structuring the GUI. Due to all the strength of the pattern of session token is further validated using the various online password checking tools, and the results obtained are quite impressive. Secure Hash Algorithm (SHA) is a cryptographic hashing algorithm used to decide a specific bit of information's integrity. In the proposed method, we used different types of keys with additional entropy to check the trust level of password security. The result has been discussed using various entropy graphs that prove improvement over the existing approach.

© 2021 THE AUTHORS. Published by Elsevier BV. on behalf of Faculty of Computers and Artificial Intelligence, Cairo University. This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).

## 1. Introduction

When considering the wireless networks, the network nodes communicate with the other nodes in the network or with the base station. Mobile nodes in the network communicate with each other via single-hop or multi-hop. In MANET, the changes to the network's topology sometimes result in conflicts and disturbances in the network [1]. The several nodes can act as centers or base stations, and also, the number of center nodes will depend on the type

of application for which the MANET is designed [2]. MANET is a wireless network containing the dynamic center nodes, which depends on the application in which MANET is involved [3]. MANET includes a mixture of the different types of networks, for example, cell phone networks, device networks, and more. Self-organizing implies that MANETs can immediately frame a network of mobile nodes or hosts, combined into discrete networks on-the-fly contingent upon the networking needs, and powerfully handle the joining or leaving of nodes in the network. The significant destinations of self sorted out MANET are versatility, unwavering quality, and accessibility [4]. Mobile nodes are low limit self-governing figuring gadgets that are fit for wandering autonomously [5]. Due to the mobility, the nodes' position changes quickly and capriciously from time to time [6]. Every mobile node can act as both host and switch to transfer data to other mobile nodes. The accomplishment of the correspondence exceptionally relies upon the other nodes' collaboration [7]. The nodes themselves are answerable for powerfully finding different nodes to convey in radio range [8]. The main characteristics of MANET

\* Corresponding author.

E-mail addresses: [amitbairwa@gmail.com](mailto:amitbairwa@gmail.com) (A.K. Bairwa), [sjoshinew@yahoo.com](mailto:sjoshinew@yahoo.com) (S. Joshi).

Peer review under responsibility of Faculty of Computers and Artificial Intelligence, Cairo University.



Production and hosting by Elsevier

are: the finished absence of unified control, absence of relationship among nodes, fast portability of hosts, dynamically shifting network topology, shared communicate radio channel, unreliable working condition, physical limitations, and restricted accessibility of assets, for example, CPU handling limit, memory power, battery force, and transfer speed [9,10].

### 1.1. Security in MANET

While working with MANET, one usually thinks about security, accessibility, and integrity. Privacy guarantees that personal data in the network nevermore uncovered to unapproved nodes. For example, it must confirm that information will not be revealed to unauthorized nodes. Accessibility guarantees that the network infrastructure, such as data transfer capacity and availability, are accessible in an ideal way, and the administration will not deny to approved clients. Trust between the nodes ensures that the unmoderated message will exchange between the corresponding nodes. Trustworthiness guarantees that the message or bundle being communicated among nodes are not compromised [11]. It means that a node cannot later deny the information that was sent by it. Node versatility in a MANET presents numerous security issues and powerless against various security attacks than customary wired and wireless networks because of their open medium, dynamic network topology, disseminated collaboration, obliged ability, and absence of away from of protection. The poorly modeled MANETs permits the aggressors for capture attempt, infusion, and obstruction of correspondence. Without legitimate security, mobile hosts are effectively caught, bargained, and captured by noxious nodes. Malicious nodes purposely breach the network to collapse the network infrastructure.

### 1.2. Token

A token is a highly protected format used in a lightweight and self-contained manner to transfer confidential information between two parties. Tokens are also used, whether within a program, to reinforce authentication mechanisms. A token is a small data stream with little meaning or use on its own but becomes a crucial player in securing the application by the proper tokenization method [12]. Token-based authentication works by ensuring that a signed token is followed by any request between nodes, verifying for validity and responding to the request. There are three main components of standard token:

- Header: It is specifying the type of token and algorithm used.
- Payload: which contains useful information and other metadata.
- Signature: That verifies the sender's identity and the message's authenticity.

Nodes should be assured that understanding their private information is handled when confidential data is exchanged via a token. For any financial records, medical details, or login credentials, this is essential. Token-based authentication is an authentication protocol that allows nodes to verify their identity a single time and receive a uniquely generated encrypted token in exchange. The use of tickets has many benefits compared to traditional methods.

- Tokens are stateless. The token is an independent entity and includes all the authentication knowledge that it requires. For scalability, this is perfect as it frees the server from having to store the session state.
- Nodes can produce tokens from anywhere. Token generation is removed from token authentication, enabling you to manage token signing on a different server or another organization.

- Access from a one-time text or email link to an account.
- To open a smartphone using a fingerprint or facial scanning tool.
- Platform-as-a-Service applications are exposing APIs that several platforms and clients can consume.

While unique usernames and passwords remain one of the most used device authentication mechanisms, token-based alternatives are increasingly becoming the standard. This method operates by generating a randomly generated token that can be decoded only by the nodes. The token acts as a mediator. Since the token serves as a password-secure stand-in. By offering a more streamlined and highly protected mechanism, token-based authentication methods will significantly boost efficiency and security. Digital tokens are the best way to reduce login dependence on nodes.

### 1.3. Motivation to the work

Weak security in the MANET may cause the man in the middle attack, a significant security loophole. Dynamic attacks could perform by deleting messages, sending wrong messages, mimic a node, which causes breaking accessibility, trust, authentication, and serving the Denial of Services (DoS). Harmful attacks are performed due to information exchange from inside or outside in the network by the nodes. Due to anonymous nodes in the network, the trust level decreases among different nodes. Because of MANET's physical limitations, security is an important area where several research works have been introduced, but the dynamic security system is still under process. The necessity of security systems should be dynamic and flexible to be salable. The MANET authentication can be categorized into three areas as data, node, and user level. Which can be described as following.

#### 1.3.1. Data authentication

In a wireless network, the recipient needs to guarantee that the data used in any essential root procedure starts from a natural source. Data authentication keeps unapproved parties from sharing in the network, and genuine components should have the option to distinguish messages from the unapproved message and reject them. Measures for guaranteeing dependability are seen as essential to recognize message modification and to leave implanted messages. In symmetric-key cryptography, Message Authentication Code (MACs) are used to give authentication [3]. The sender and the receiver share a riddle key to process a MAC of all assigned data. When a message with a correct MAC shows up, the recipient understands that it almost certainly been sent by the primary sender. In open key cryptography, advanced imprints are used to stamp a message as a technique for authentication. A refined pattern is a numerical arrangement for indicating the validness of a modernized message or a record. A genuine mechanized imprint gives a recipient motivation to acknowledge that a known sender made the message and not adjusted in movement.

#### 1.3.2. Node authentication

Authentication is instant data exchange frames and network administrative endeavors in MANETs like adding a new center point to the networks. A couple of authorities have concentrated on center point authentication before the nodes join the MANET [13]. Such convention relies upon matching conditions and number speculation thoughts to achieve secure authentication among nodes in MANETs. Most research done on the central authentication and critical dissemination acknowledge MANET as a static situation. As such, they focus on the proficient beginning authentication and necessary arrangement.

### 1.3.3. User authentication

User authentication is a means of recognizing the user and confirming that the user can get to some local administrations. User authentication means working up a connection between nodes and some characters. A character is the peculiarity property of a node, which ideally can't be fabricated or copied. Before long, personalities are completed by things which user know (passwords), have (puzzle keys or security tokens) or properties which they have (bio-metrics) [14]. This understanding of the organization's workplaces will make the recognized data accessible to explicit people, generally those who pay to get the administration. For this situation, a MANET should, in all likelihood, perceive real nodes from the strange ones. In authentication, a node sends his ID (e.g., name, IP address) and verifies his character to a sensor to pick whether the sender is genuine and has a spot with that name's node. Upon productive authentication, the sensor approves the node that is enabled access to the data. Some of the authentication factors can be bio-metric, DNA, fingerprints, voice reorganization, retina detection, etc.

### 1.4. Device fingerprinting in wireless networks [15]

With the increasing demand for new network technologies like the Internet of Things (IoT), MANET, Li-Fi, etc., to provide connectivity anytime at a cheaper cost. On the other side of this wireless network, it can have so venerable that it can impact overall communication integrity and confidentiality and compromise the Quality of Services (QoS). There are so many different types of cryptographic methods available to handle such issues in the wireless network. But they are not able to handle the DDoS attacks, including service jamming. Wireless device access is readily available, and it can be elementary for the attackers to exploit them and once they are part of the wireless network. It is a fact that mobile devices can be easily compromised if they are configured with a weak security mechanism.

Therefore, new low-complexity approaches are of considerable value for detecting legitimate users' accurate detection to identify possible threats by harmful threads. In our proposed policy, system fingerprinting has arisen as a promising approach to reduce the susceptibility of wireless networks to node forgery or insider attacks, the method of collecting device information to produce device-specific signatures and using them to distinguish individual devices. The basic concept is to passively or actively retrieve specific patterns observed from target devices during the wireless communication process. Several parts can be collected and used from physical layer attributes, medium access control (MAC) layer features, and upper layer features. Successful system fingerprints must fulfill two properties: First is that they are difficult or impossible to forge, and Second, the characteristics should be robust to handle the environmental changes and node mobility. The first specification contains identifiers such as IP addresses, MAC addresses, etc.

Although many modern security mechanisms are interested in fingerprinting wireless devices and their ability to enhance wireless security. This paper introduces a method that can be used in wireless devices by fingerprinting.

### 1.5. Research gap

1. Traditional passwords have one tremendous weakness: humans create them. Passwords made by human beings tend to be weak and easy to break. Time and again, we have all repeated old codes because they are easy to recall. Not just that, but a login scheme built on a password allows users to enter and re-enter their passwords continuously, wasting precious time in essence.

2. It is a glitch and loses time for the nodes, those who repeatedly enter their credentials to complete several tasks. Every node has better things to do in a tedious and wasteful operation than to waste their time. Plus, the above login scheme is possibly already insecure since, to begin with, the weak password. Every login stage in this basic authentication setup is a weak connection that is open to attack.
3. Token based authentication is more secure than the traditional system. On the other hand, token-based authentication uses ultra-secure codes to show that you have been authenticated already. The consumer, the particular login session, and the device's authentication algorithm are specific to them. In other words, at every stage, the server can detect whether a token has been tampered with and can block entry. Tokens act as an additional layer of authentication and function as a temporary stand-in for the user's password. Tokens are, most notably, machine-generated. Machine-generated encrypted code is considerably more reliable than any password created manually.
4. Token based authentication offers a streamlined process. Instead of re-verifying identity any time, tokens are temporarily stored for a given duration, providing access to domain knowledge. This helps to switch between a node to node without being delayed by the mechanism of authentication. They have to log out when the nodes end their session, and the saved Token is lost forever. Nodes should not fear keeping their accounts open for the attack in this manner.

### 1.6. The objective of work

1. In the mutual authentication based protocol, the MAC address and fingerprint will form the basis of the determination of node, which is the dual authentication basis of node identification.
2. Randomization session for transfer by the Generation of Token. Each time the transfer occurs, a new session token is required to be generated to provide more security in the data transfer. To repeat the token generation process, the communicating nodes' MAC addresses will be needed in the token generation process.
3. Dual Security in the data transfer with the generation of OTP and Transaction ID for the receiver's validation.
4. Validating the integrity of the data received with the Hash generation for the message received and comparing it with the hash send.

This paper is organized into five sections where. Section 4 introduces the concept of the MANET and its security constraints and provides the theoretical overview. Section 2 will examine the reviews as well as the research papers by the other authors and explains, in brief, the work done by them. Section 3 describes the proposed work and explains the process which is presented in the dissertation work. Section 4 is an analysis of the proposed work that contains the implementation part and explains the technology used for implementing the dissertation work and the result analysis explaining the performance of the proposed work. Section 5 is having the details of model performance. Section 6 is defining the conclusion and future scope. It describes the overall summary of the proposed work, concluding with the performance and future scope.

## 2. Literature review

This section includes the research by the various authors in the same domain and this we have in short explanation of the work performed by various researchers.

## 2.1. Related work

S. S. Rajput et al. [25] presented a security improved Zone Routing Protocol (SEZRP). In this study, routing in ZRP is verified using the authentication method against any possible attacks. MAC is utilized for keeping up the privacy of the messages. The essential pre-dissemination procedure is additionally used at the run time in this technique to manage the overhead generated due to sharing the secret key.

M. Patidar et al. [26] found that Kerberos is a confided in outsider authentication protocol widely utilized for security in PC networks. This calculation prompts huge deferral in the activity; consequently, it is awkward to apply Kerberos to protect during asset partaking in MANET. This research proposes a staggered security authentication (MLSA) that provides asset experiencing in MANET.

Zhu Xingliang et al. [27] proposed another proficient authentication procedure in the mobile network. This method is based on the pool of certificates located in the server to give mobile node's Diffie-Hellman open secret key, based on which versatile behavior of mobile nodes requiring correspondence executes shared authentication in Diffie-Hellman critical understanding method. After node authentication, the necessary exchange could embrace evenness cryptanalysis, bringing down calculation and spare asset of the MANET.

S. Neelavathy Pari et al. [28] comes up short on an all-around characterized security component, thus increasingly powerless against malignant attacks. The trust model method is created using the SHA1, which is one of the key-based encryption methods. This system is designed to recognize and keep away from vindictive nodes in the network. The trust is constructed based on past attacks and suggestions of different nodes in the network.

R. Dilli et al. [29] Creators have utilized Hashed Message Authentication Code (HMAC) to accomplish information trustworthiness and authentication. The half breed routing method which creators have used was Zone Routing Protocol (ZRP). This paper executes an HMAC-SHA3-512 calculation in ZRP, which prompts higher throughput and parcel conveyance portion yet to the detriment of the expanded start to finish delay. From their exhibition investigation utilizing a 64-bits Intel Processor, it shows that the expense of executing an HMAC-SHA3-512 calculation gives half execution improvement over comparative usage of HMAC-SHA3-256.

D. Ravilla et al. [30] drive a hash limit is to make a "one of a kind imprint" of data for authentication. The length of the hash code made it more secure and protected data from malicious attacks. Building up the Message Authentication Codes (MAC) from Cryptographic hash limits (SHA-256) gives excellent execution in programming than symmetric square figures like Data Encryption Standard (DES) and the library code for cryptographic hash limits are commonly available. Here authors executed the HMAC-SHA-256 for authentication of the message. Mobile system condition and the show of the protocol are penniless somewhere near figuring throughput, bundle movement allocates and beginning to end the system's deferments. The authors analyzed an improvement in throughput and package movement extent to the detriment of getting ready time (see Table 1).

S. Choochotkaew et al. [14] presented a standard to picking an authentication model for a particular MANET's application. The authors review and separate existing authentication models for organizing the overall decision method. The proposed model depends upon systems, the charming trusted properties, and the essentials for execution and security (see Table 2).

P. Yadav et al. [31] proposed an essential instrument to verify the AODV routing protocol. This component empowers node authentication before the course foundation by installing the

advanced certificate in the HELLO bundle, with the goal that any unapproved substance can't take part in the routing procedure. In this way, the execution of the AODV protocol improves because of the evasion of various attacks, for example, wormhole attack, Sybil attack, and so forth.

H. Yang et al. [32] proposed an authentication system to give individual correspondence by expanding the unwavering quality of the nodes. The bunch structure is utilized for the proposed procedure's authentication method, and the group head goes about as a certificate authority. It is overseen authentication information of part nodes (see Table 3).

Y. P. Singare et al. [33] proposed a practical starting access authentication component over MANET that is more efficient than other message authentication technique. The proposed strategy's critical thought is to give an efficient method to provide secure messages between the mobile client and the authentication server.

### 2.1.1. Research gaps

1. There is no security arrangement available for the authentication of source and destination.
2. Most of the security instruments are not dynamic.
3. The legitimate working of the Intrusion Detection Technique isn't yet characterized.
4. The general framework for authentication of nodes in MANET is still to create.

## 3. Proposed method

### 3.1. One-Time Password (OTP) Models

OTP based security devices are the smart concept based cards that consist of the chip-based security model, which generates the numeric or even the alphanumeric combinations of the characters to validate access to the system or in case of the transaction. The concept of the security chip models is designed so that the generated OTP pattern changes every 30 or 60 s. The validity of the OTP developed for the particular transaction will range based on its importance. The common application of the OTP is the various mobile-based applications where the user validation is checked using the OTP and various mail-exchange applications like GMAIL etc. Also, use the two-step validation of the users using the concept of the randomly generated OTP.

To access the gadget's service, the server governing the transaction of the access will generate the secret and random One-Time Password. The server can also act to validate or sequencing a particular service's usage by generating the OTP as the token for accessing the service or sequencing the service's use. Several organizations are using SMS messages to validate their users. For this purpose, they use the SMS gateway via accessing the Cellular networks and sent the transactional SMS related to the transactional password to access the service. In the proposed work, we also utilized the SMS gateway for the validation of the node. A two-Factor assurance on a general basis, the verification is done using the generation of the two OTP or the passwords. The first OTP will validate the user's identity, accompanied by the phone number or the email id to validate the user's authenticity. After passing the first phase of the validation, the second phase may involve the generation of another OTP so that the authorized user can access the service requested by the user. The OTPs used for this purpose can be of various types like Hash-Based OTP, Time Based OTP. A timestamp is linked, which qualifies that such OTP automatically expires after the particular time frame when the OTP is generated. The proposed work, which used such OTP generation, also the OTP expires after the specific time frame.



**Table 1**  
Authentication methods presentation and description.

Presentation	Abbreviation	Description	References	Year
AM1	MD5	Message-Digest Algorithm	[16]	2014
AM2	TLS	Transport Layer Security	[17]	2014
AM3	TTLS	Tunneled Transport Layer Security	[18]	2008
AM4	PEAP	Protected Extensible Authentication Protocol	[19]	2018
AM5	LEAP	Lightweight Extensible Authentication Protocol	[20]	2019
AM6	FAST	Flexible Authentication via Secure Tunneling	[21]	2019
AM7	SPEKE	Simple password exponential key exchange	[22]	2013
AM8	TLS-SEM	TLS Security-Enhanced Mechanism	[23]	2013
AM9	Double-TLS	Double-TLS Transport Layer Security	[23]	2013
AM10	SRP	Secure Remote Password	[23]	2013
AM11	SSC	Secure Services Client	[22]	2013
AM12	Park	Park's Authentication Protocol	[24]	2013
AM13	Proposed Method	Session Token using Fingerprint and MAC Validation	AK Bairwa, S Joshi	2021

**Table 2**  
Password entropy.

Parameter	Description
$E_x$	Entropy of Password
$R_p$	Number of Unique Characters in password
C	Total number of characters in password
$R_p^C$	Numbers of Possible Passwords
$\log_2(R_p^C)$	Numbers of Bits of Entropy

**Table 3**  
Password types based on the entropy.

Entropy range	Password type
0–28 bits	Very Weak
24–31 bits	Reasonable
57–127 bits	Strong
128 + bits	Very Strong

### 3.1.1. Concept of OTP

A One-Time Password (OTP) is commonly expressed as the combination or sequence of the alphanumeric characters used to verify the user's identity or the validity access of the transaction or session. An OTP is comparatively more precise and secure than that of the static password, particularly a user-made password, which can be weak and reused over various records. OTPs can be used as the medium of verification of the individual user at the login time. They will furthermore add the layer of security in the process of authentication and verification.

### 3.1.2. OTP types

There is a wide range of kinds of one-time password (OTP) authentication techniques that can use for multi-factor authentication. OTP authentication tokens are two principal sorts: equipment tokens (regularly referred to just as 'hard tokens') and programming tokens (frequently referred to only as 'delicate tokens'). A hard token is a physical gadget that delivers an OTP, for example, the YubiKey or SecurID tokens. However, these are exceptionally secure will users to bear them to get to two-factor authentication empowered records. On the other hand, Delicate tokens enable users to get an OTP with programming, for example, through an instant message on a cell phone or an OTP conveyed using email. This is anything but difficult to use since many people consistently have a cell phone on them at some random time. These techniques include SMS authentication, the YubiKey based security, the PassiveKey based security, SIP Authentication service, Email validations, and the Google Authenticator. Any of discussed techniques can be utilized inside PortalGuard with any combination of strate-

gies set up together. This makes it simple to pick and pick what methods would be best for you to actualize them.

### 3.1.3. Advantages of a One-Time Password

The main advantage of using the One-Time-Password is that the user must not remember any particular sequence or the particular password pattern to access the specific service or system. And similarly, each time, a different combination of the password's alphanumeric design is generated for the particular user, so it will be difficult for the hackers to break the password as no longer it's a single and static password.

### 3.2. Single Sign-On (SSO)

Single Sign-on enables the end-user to log into a single entry-way and consistently access multiple applications with only one accreditation. Single Sign-on builds security, decreases various logins, and furnishes end-users with a convenient, usable technique for getting to most of their records.

### 3.3. Two Factor Authentications

Two Factor Authentication (2FA) is a more secure approach to verify logins. Rather than utilizing one type of authentication, for example, a password, two-factor authentication utilizes at any rate two types of authentication to confirm a user. This makes a substantially more secure environment for a user. Regardless of whether a password gets traded off despite everything, they have an additional protection layer to ensure their information is secure.

### 3.4. Hashing

It's one of the best methods to transform any length of string into a fixed-length series. This method is more famous for the recovery of the information to limit the size of the series. For example, suppose you have a person's DNA test, this would consist of a lot of information (about 2.2–3.5 MB), and you might want to discover the belonging DNA test. You could take all examples and contrast 2.2 MB of information with all DNA tests in the database, yet looking at 2.2 MB against 2.2 MB of information cannot take a long time, particularly when you have to cross many examples. The place hashing can prove to be useful, rather than looking at the information. Few hashes will be determined for the various locations on the chromosomes, yet for the model, we should accept that it's one hash), which will restore a fixed-length estimation of, for example, 128 bits. It will be simpler and quicker to inquiry about a database for 128-bits than for 2.2 MB of information.

### 3.5. Random numbers

It's a number created utilizing a considerable arrangement of numbers and a scientific algorithm that gives an equivalent likelihood to all numbers happening in the predefined distribution. Random numbers are most commonly created with the assistance of a random number generator. Random numbers have significant applications, particularly in cryptography, where they go about as fixings in encryption keys. One of the most significant essentials of a random number is free, to build up no correlations between progressive numbers. It must be guaranteed that the recurrence of the event of these random numbers ought to be the equivalent roughly. Thus, hypothetically, it is challenging to produce a long random number. The random numbers can be generated with the help of programming and equipment. PC made random numbers are now and again called pseudorandom numbers. There are numerous techniques, for example, the direct congruence strategy for creating pseudorandom numbers. Random numbers created by equipment or physical phenomenon are considered genuinely lucky produced numbers. Be that as it may, if one somehow happened to be given a number, it is difficult to check whether a random number generator delivered it or not. To think about the randomness of such a generator's yield, it is significant to consider groupings of numbers. It is straightforward to characterize whether an arrangement of unbounded length is random or not. This arrangement is random if the amount of information it contains – in the feeling of Shannon's information hypothesis – is likewise boundless. It must not be workable for a PC program, whose length is limited, to deliver this arrangement. Strikingly, an interminable random grouping contains all conceivable limited successions. Such an endless series accomplishes, for instance, including the Microsoft Windows source code or the Geneva conventions' content. Tragically, this definition isn't valuable, as it is unimaginable by and by to create and process interminable arrangements. On account of a limited grouping of numbers, it is officially difficult to confirm whether it is random or not. It is only conceivable to watch that it shares a random grouping's measurable properties – like the equiprobability, all things considered – yet this a troublesome and dubious assignment. To show this, let us, for instance, consider a twofold random number generator creating arrangements of ten bits. Even though it is as likely as some other ten bits successions, 1 looks less random than 0 1 0 1 0 1 0. The definitions have been proposed to portray “down to earth” random number arrangements. Knowing one of the numbers of succession must not resist anticipating different ones. The random numbers are mentioned in this paper; they will be expected to satisfy these “reasonable” definitions. Measurable randomness tests target deciding if a random number generator created a specific succession of numbers. The methodology is to ascertain exact measurable amounts and contrast them, and standard qualities acquired based on a random sequence. These ordinary qualities are obtained from calculations performed on the model of a perfect random number generator. Testing randomness is an exact errand. There exist various tests, every last one of them uncovering a specific kind of imperfection in a grouping.

### 3.6. Entropy

Entropy can be defined as a scale to measure the password's difficulty, either generated by humans or machines. The method to calculate the entropy is shown in Eq. 1.

$$E_x = \log_2(R_\beta^L) \quad (1)$$

Entropy is the opposite of a systematic pattern. Entropy is considered acceptable the more significant E's value, the harder a password is to crack.

Let's understand the concept of entropy using a scenario. Suppose in a particular machine, a keyboard has 96 unique characters, and you are randomly constructing a password from that whole set, then  $R = 96$ . If you have a 14 character password, then  $L = 14$ .

$$(R^L) = 5,64,67,33,12,35,51,13,60,24,52,65,85,856.$$

It's observed that the total no of passwords generated using the provided value of R and L. This is a vast number and not as easy task for the attacker to crack it.

$$\log_2(R^L) = \ln(5,64,67,33,12,35,51,13,60,24,52,65,85,856)/\ln(2).$$

So the value of  $\log_2$  is 92.19 approximately, which is similar to  $2^{92.19}$ .

In terms of the password security level, it's 92.19 bits of entropy. It will be required a lot of time to crack by the attackers.

### 3.7. Proposed Algorithm

The proposed algorithm is the joint or associated algorithm that performs the work based on the sub-algorithms; which are used in the process are as follows:

- Registering the User in Network
- Destination MAC Address Validation
- Generation of Token for Message Exchange
- Module for Sender End
- Module for Receiver

#### 3.7.1. Algorithm for Registration

---

##### Algorithm 1: Algorithm for Registration

---

**Input:** MAC Address, FingerPrint

**Output:** Success and Details of node Saved, Unique node Number Generated

- 1: Read MAC Address, Fingerprint of the user which is being pretended as the node.
  - 2: Generate the Hash Code for the Fingerprint using the SHA-256 algorithm and store it in SHAFIQ.
  - 3: Generate the Hash Code for the MAC Address using the SHA-256 algorithm and store it in SHAMAC.
  - 4: **if** MAC Address exists or DIGSIG exists in Database **then**
  - 5:   Write “node Already Exists”
  - 6: **else**
  - 7:   (a) Write “node Details Saved”.
  - 8:   (b) Store the Details in the Database and new node Number Generated
  - 9: **end if**
  - 10: Stop.
- 

#### 3.7.2. Algorithm for Destination MAC Address Validation

This algorithm is used for the validation of the Destination MAC Address.

**Algorithm 2:** Algorithm for Destination MAC Address Validation**Input:** Destination node Number.**Output:** Success Return MAC Address of node.

- 1: Establish the connection with node Database.
- 2: Perform the Search Operation in Database for the node.
- 3: **if**Data Exist**then**
- 4: Fetch the Details of Destination node from Database
- 5: **else**
- 6: Write “No Details of node Exists.”
- 7: **end if**
- 8: Stop.

**3.7.3. Generation of Token for Message Exchange**

In this module, generate the token for the first phase of data transfer.

**Algorithm 3:** Generation of Token for Message Exchange**Input:** Sender MAC Address, Destination MAC Address**Output:** SESSION\_TOKEN

- 1: Set RND1:= RAND (0:9).
- 2: Set RND2:= RAND (0:9).
- 3: Set RND3:= RAND (0:9).
- 4: Set RND4:= RAND (0:9).
- 5: Set RND5:= RAND (0:9).
- 6: Set RND6:= RAND (0:9).
- 7: Set RND7:= RAND (0:9).
- 8: Set RND8:= RAND (0:9).
- 9: Set RND9:= RAND (0:9).
- 10: Set RND10:= RAND (0:9).
- 11: Generate Hash Code using SHA-256 for Sender MAC address and extract the first 20 characters from it and store it in SHASENDER.
- 12: Generate Hash Code using SHA-256 for Destination MAC address and extract the first 20 characters from it and store in SHADEST.
- 13: Combine random numbers generated with SHASENDER and SHADEST to form SESSION\_TOKEN.

**3.7.4. Module for Sender End**

This algorithm explains the OTP and transaction ID generation at the sender end.

**Algorithm 4:** Module for Sender End**Input:** Sender MAC Address, Destination MAC Address, SESSION\_TOKEN**Output:** OTP and Transaction ID

- 1: Read Sender MAC Address, Destination node Number.
- 2: Perform the SESSION\_TOKEN validation.
- 3: If SESSION\_TOKEN is Valid then:
- 4: Perform process for OTP generation.
- 5: Set RND1:= RAND (0:255).
- 6: Set RND2:= RAND (0:255).
- 7: Set RND3:= RAND (0:255).
- 8: Set RND4:= RAND (0:255).
- 9: Set RND5:= RAND (0:255).
- 10: Set RND6:= RAND (0:255).
- 11: Set RND7:= RAND (0:255).

**Algorithm 4:** Module for Sender End

- 12: Set RND8:= RAND (0:255).
- 13: Get Character corresponding to random numbers RND1, RND2, RND3, RND4, RND5, RND6, RND7, RND8, RND9, and RND10. Then, combine all characters to get the pattern for OTP.
- 14: Store the Details of this transaction.
- 15: Message Encryption is performed using OTP.
- 16: Generate SHA-512 Hash for Message and store with the transaction details.
- 17: Generate the Transaction ID, which is unique for the particular transaction.
- 18: Stop.

**3.7.5. Module for Receiver**

In this module, the receiver ends. the message is routed to the receiver and then data is decrypted.

**Algorithm 5:** Module for Receiver**Input:** Sender MAC Address, Destination MAC Address, OTP, Transaction ID**Output:** Message Decrypted, Success

- 1: Read the Transaction ID and OTP
- 2: Establish a connection with the network database.
- 3: **if** Details Correct **then**
- 4: (a) Read the Encrypted Data.
- 5: (b) Decrypt the Data using the OTP.
- 6: (c) Generate the SHA-512 hash for the decrypted data.
- 7: (d) Fetch the HASH received from Sender.
- 8: **if** HASH matches **then**
- 9: Write “Data is OK, Use It”.
- 10: **else**
- 11: Write “Data is Corrupted or Manipulated”
- 12: **end if**
- 13: **else**
- 14: Write “Invalid Details”
- 15: **end if**
- 16: Stop

**4. Result and discussion****4.1. Simulation environment**

The planned work is structured utilizing MATLAB, and the information network is finished utilizing the MSACCESS. The GUI section of the MATLAB used is employed used for structuring the planning of the structures that square measure used for the usage reason.

**4.2. Implementation of proposed work**

The re-enactment of the base desk work and the proposed work is finished by structuring the GUI. The GUI part of the MATLAB lets us make the screens by hauling the controls on the workspace.

Fig. 1 shows the registration form, which will be the starting point of our work. To further proceed to the simulation of the mutual authentication, we require the node to be registered.

For the registration phase, we require to enter the following details: the user name, email, MAC Address, and Finger Print. The



The registration form is titled "Network New Node Registration". It contains the following fields and buttons:

- User Name:** Input field with "duser1" entered.
- Email ID:** Input field with "duser1@gmail.com" entered.
- MAC Address:** Input field with "00:1B:44:11:3A:B7" entered.
- Load Finger Print File ...:** Button next to a file path: "D:\Program Files\MATLAB2\R2011a\works\NewMACproj1\_1.png".
- Generate Password:** Button next to a password field containing "d62eb3edfa-b1bc032666".
- Save Record:** Button.
- Clear All:** Button.
- Back to Login Form:** Button.

Fig. 1. Registration form.

password is then generated using the SHA –256 algorithms, which developed the hash corresponding to the MAC address and the fingerprint. These details are then stored in the user data table, and the structure of the same is listed in Table 4.

Fig. 2 shows the Login form, which is how to authenticate the validated users. The users' details for the validation purpose enter are as follows, user name, MAC address, and fingerprint. The Hash is then again generated using the SHA-256 algorithm, and then details are then verified with the users' information, which is stored in the table named UserData. If the details are found correct, then the user is granted access to the communication system (see Fig. 3).

The Fig. 4 shows the user control panel, which provides the two direction path, "Transfer Data After Validation," which is used to send the data to the other node. The option "Receiver Data After Integrity Check," this option is used for receiving the data transmitted by another node.

The Fig. 5 shows the form used for sending the data to the other node. Here, the user who has login will automatically be fetched based on the points which are entered at the time of the login. When a form is opened for information like the user name of the user or node sending the data will get displayed, and the MAC address of the node which is sending the data.

This form works in the various phases of the validation. When the nodes are registered at the registration phase, the node's entry is stored in another table, which is the Network nodes table. It contains the node number and the MAC address of each of the nodes registered at the network. The Table 5 shows the structure of the table 'Network nodes,' which contains the field NodeNo for the network node number. It's an auto-incremented area, which increments automatically as the record is inserted. Other is for stored MAC address, managers.

So, using this table the first phase verification is done, here the user who want to send the data to the other node, first require to enter the node number and if the node number is valid then the MAC address is fetched from the 'Networknodes' table and the screen will look like as shown in the Fig. 6.

**Table 4**  
Registration table 'User Data'.

Fieldname	Description
Uname	Representation of the node
Emailid	Emailid which is the registered emailid
FPath	File Pat stores the location of fingerprint
Passwd	Password which is the combination of hashes
Macadrs	MAC address of the node

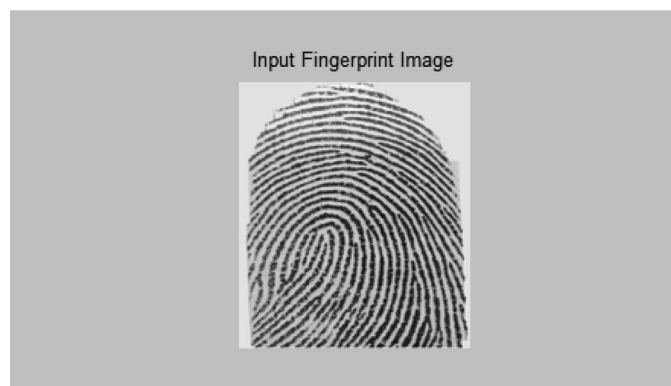


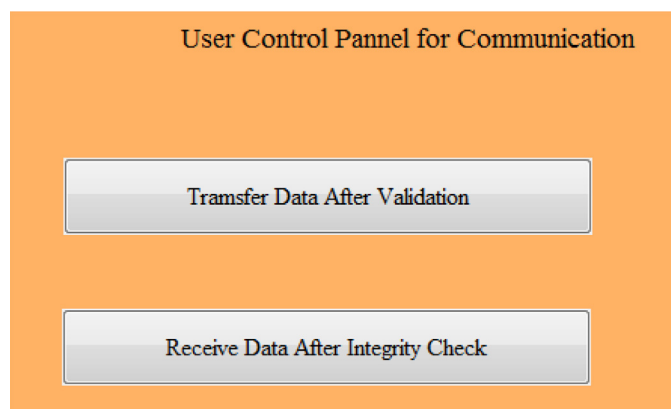
Fig. 2. Fingerprint input.



The login form is titled "Node Login". It contains the following fields and buttons:

- User Name:** Input field with "duser1" entered.
- MAC Address:** Input field with "duser1@gmail.com" entered.
- Load Finger Print File ...:** Button next to a file path: "D:\Program Files\MATLAB2\R2011a\works\NewMACproj1\_1.png".
- Generate Password:** Button next to a password field containing "d62eb3edfa-b2a952a287".
- Login:** Button.
- Clear All:** Button.

Fig. 3. Login form.



The User Control Panel for Communication contains two main buttons:

- Transfer Data After Validation**
- Receive Data After Integrity Check**

Fig. 4. User control panel.

After the destination node, the MAC address is fetched, then the step is to generate the session key. The session key is developed using the random numbers, SHA hash of the Sender MAC address, and SHA hash Destination MAC address. The session key details are stored in the session data Table 6. The structure of the 'SessionData' table is shown in the table. It contains the fields related to the sender MACadrs, and the session key used for storing the generated session key.

In Fig. 7, the session key generated and details will get stored in the SessionData table (see Fig. 8).

Now, in the next phase, the user must enter the session key and message, which is to be sent to the destination node. The session key is validated using the session data table, and if the details are found correct, then the communication process will proceed



Fig. 5. Initial display of the data sending form.

**Table 5**  
Nodes of network.

Fieldname	Description
NodeNo	Store the auto-incremented node number
MACAdrs	Store the MAC address of the node.

Fig. 6. Destination node MAC address fetched.

**Table 6**  
Session data table.

Fieldname	Description
MACAdrs	Stored the MAC address of the sender node.
SessionKey	Stores the generated session key

Fig. 7. Session key generation process.

Fig. 8. OTP generation.

further. So, in the last phase, OTP is generated using a series of random numbers. OTP will encrypt the message we are sending, and SHA –512 hash corresponding to the message is also developed for the validity cheek. All these details are stored in the data log's table, and the structure of the data logs table is shown in Table 7 (see Fig. 9).

The unique transaction ID is formed for each transaction, indicating the data exchange between the sender and the destination nodes.

Now, the sender enters the details are fetched after validation and integrity cheek, for which the destination node is required to enter the transaction ID and OTP. After the validation, the data is fetched from the data logs table (see Fig. 10).

#### 4.3. Testing the strength of proposed work

SHA, which represents a secure hash algorithm, is a cryptographic hashing algorithm used to decide a specific bit of information's trustworthiness. SSL authentication specialists regularly utilize variations of this algorithm to sign declarations. This algorithm help guarantees that data isn't changed. It does as such by creating unique hash esteems from a specific record/variation of a document. Considering this hash esteems, it tends to be resolved whether the document has been adjusted by contrasting the standard hash an incentive with the hash worth getting (see Fig. 11).

SHA1: d a 3 9 a 3 e e 5 4 1 b 4 b 0 d 3 2 5 5 b f e f 9 5 6 0 1 8 9 0 a f d 8 0 7 0 9 SHA256: e 3 b 0 5 c 1 2 2 9 8 f c 1 c 1 4 9 a f b f 4 c 8 9 9 6 f b 9 2 4 2 7 a e 4 1 e 4 6 4 9 b 9 3 4 c a 4 9 5 9 9 1 b 7 8 5 2 b 8 5 5

With an online hash generator instrument, you can rapidly produce a SHA256 hash for any string or information esteem. Essentially enter a series an incentives into the infobox and select Generate. At that point, the device will produce an interesting 64-digit hash for the worth you indicated [34] (see Fig. 12).

**Table 7**  
Datalogs.

Fieldname	Description
Fuser	Sender node MACAddress
Tuser	Destination node MACAddress
Data	Message to be Sent
OTP	The generated OTP
Tid	Transition ID and unique for each transaction

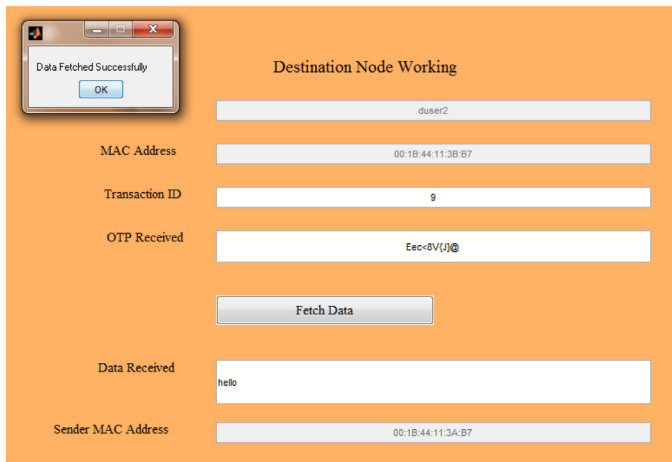


Fig. 9. Receiving data.

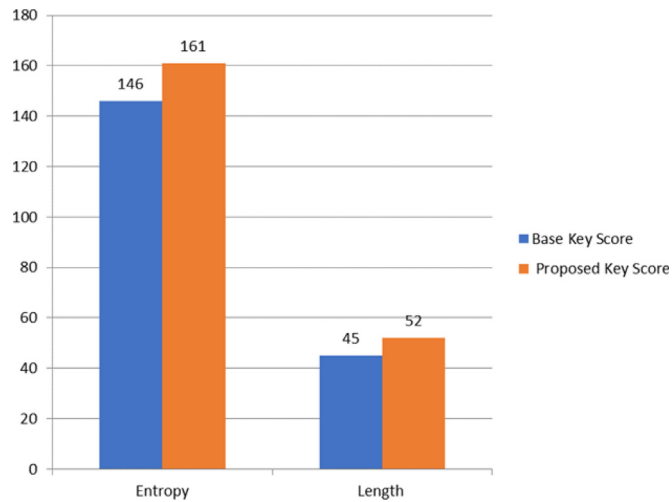


Fig. 10. Graphical comparison Test Case 1.

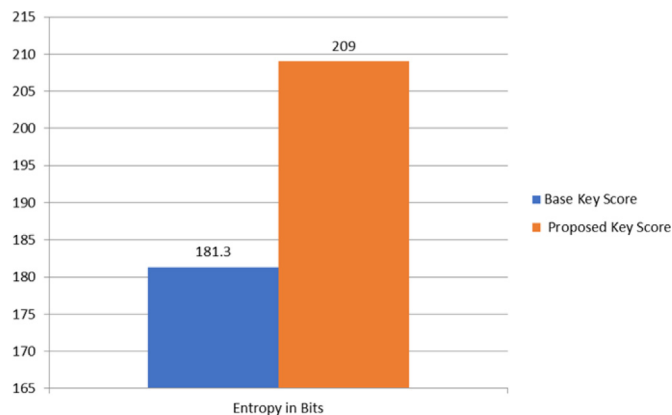


Fig. 11. Graphical comparison Test Case 2.

The key which is generated from the author paper is, 4 1 1 2 d f 5 3 c a 2 6 8 2 4 0 c a 7 6 6 7 0 9 2 4 6 4 5 b 3 e 3 4 5 a 6 0 0 b f a 1. The proposed work which we have implemented have to follow differences,

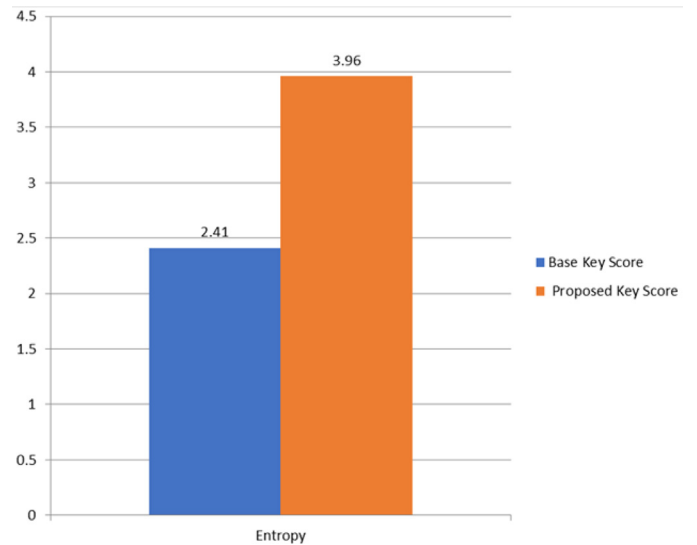


Fig. 12. Graphical comparison Test Case 3.

1. 8 Digit OTP generated on the Random Basis, which is sent on Mail and SMS to authentication the node in the first phase.
2. SHA 256 algorithm is used, and it generates 64 characters hash code. The 32 characters SHA 256 extract for the sender MAC address and 32 characters SHA-256 extract for the receiver MAC address, and the 8 Digit new random number.

Example of session key generated using the proposed approach.  
1 9 9 4 8 1 4 9 7 9 b 1 b c 8 3 2 6 6 6 1 1 2 8 e 4 4 8 f 7 3 d 5 f 5 d d 1  
2 9 4 f a 8 7 d 2 0 0 a Testing the strength of the Session Keys Base:  
4 1 1 2 d f 5 3 c a 2 6 8 2 4 0 c a 7 6 6 7 0 9 2 4 6 4 5 b 3 e 3 4 5 a 6 0 0  
b f a 1 Proposed: 1994814979 b1bc832666- 1128e448f7- 3 d 5 f 5  
d d 1 2 9 4 f a 8 7 d 2 0 0 a

#### 4.3.1. Tool 1: How Secure My Password [35]

Following is the password strength analyzer using the online tool [35]. The testing method uses dictionary words, Recognizable patterns, and other dynamic methods to guess the passwords to check the entropy. This entropy method is using a random approach to match the password. So te the results may vary at every time (see Fig. 13).

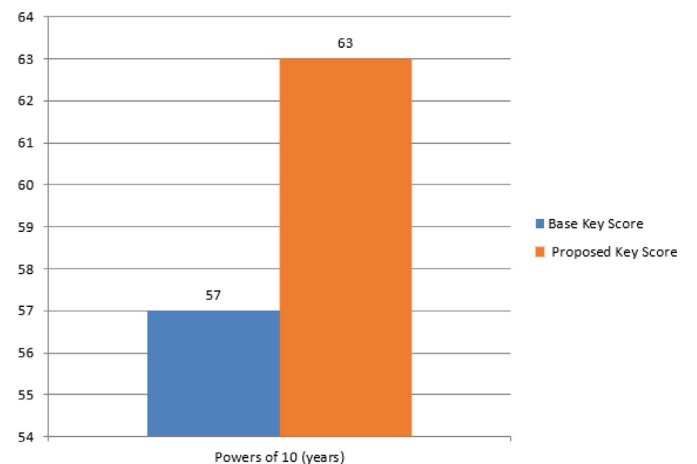


Fig. 13. Graphical comparison Test Case 4.

#### 4.3.2. Tool 2: Runkim Test [36]

The tool named Runkin also tests the password strength, calculates the entropy, and determines the length of the string.

#### 4.3.3. Tool 3: Cryptool [37]

CrypTool is an open-source venture. The primary outcome is the free e-learning programming CrypTool showing cryptographic and cryptanalytic ideas. As indicated by "Hakin9", CrypTool is worldwide the most across the board e-learning programming in the field of cryptology.

#### 4.3.4. Tool 4: How secure is my password [37]

HowSecureisMyPassword.net is the website that is used for checking the strength of the password or string. This online tool will return the number of years require to break or crack the password. Based on the years, which is more, we can judge that more need is the password. We are expressing the years into exponential form to compare in terms of the powers to 10.

#### 4.4. Discussion on results

Security has become an essential worry to give ensured correspondence between mobile nodes in a negative situation. Like the wireless networks, one of a kind attributes of MANET represented various difficulties to the security plan. These difficulties present a defense for building multigene security arrangements that accomplish both assurance and attractive network execution. The proposed work involves the following subsections.

##### 4.4.1. Registering the user

In the mutual authentication-based protocol, we have a monitoring node that will maintain the access list of the authorized nodes. The monitoring node will keep the nodes' list on the basics of the mac address of nodes. The digital signature key, which is generated as the combination of the hash code of MAC Address, with the variety of the fingerprint file of the user acting as node and combination of both, will verify the entity.

##### 4.4.2. Generation of token

The authenticating node will generate a token containing six digits random numbers with the SHA-256 Hash parts of the Sending and Receiving node's mac addresses to validate the identity.

##### 4.4.3. Sending message

Now, when the session token is generated and validated, then the message initiation will start. The Sender will ping the receiver with the Message Transaction ID and OTP, which is the combination of random numbers and some hash extract of the message sent.

##### 4.4.4. Receiving message

At the receiver end, to decrypt the message, the receiver will enter the message transaction ID and OTP. After that receiving the message, it will confirm the receiver of the message, which is the SHA code of the message. The receiver will check against the SHA code of the message sent and if both are the same then the confirmation is achieved that the message is received correctly.

**Table 8**  
Security strength Comparison 1.

Parameter	Base key score	Proposed key score
Entropy	146 bits	161 bits
Length	45	52

And above all, the session's strength token pattern is further validated using the various online password checking tools, and the results obtained are quite impressive (see Table 8).

#### 5. Model performance

We performed an in-depth evaluation to check the legitimacy and consistency of our trust model. As per the studies, nodes present two types of behaviors, e.g., malicious and trustworthy. A particular node offers adequate support in interaction through reliable actions. Three well-known methods LWTR [38], STWSN [39] and LTQR [40] are used to compare the proposed method.

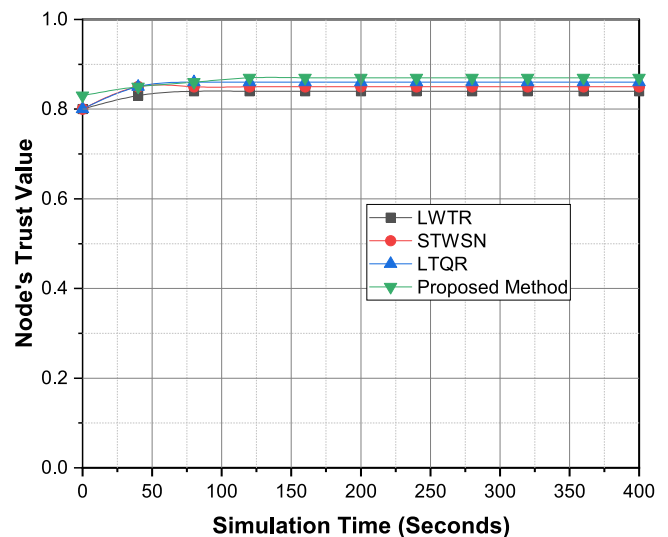
As shown in Fig. 14, network interaction satisfaction ratios run as a function of the simulation time. In the initial stage of simulation, all confidence models' satisfaction ratios increase, then remains constant. Trust models can take advantage of the trust principle, eventually identify deceptive agents in the simulation process, and guarantee that only trustworthy agents can communicate.

A more extended period of the malicious node would result in more significant harm to the simulation environment. Our model has better outcomes. A malicious node can perform well in a particular period to scam a high reputation and then act maliciously (see Table 9).

Our model performs better than the other models in combating cheating threats, as seen in Fig. 14. Gains from the trust attribute 'historical trust recommendation' 2. A malicious node is identified by various trust models, respectively, with the increase of simulation steps. Our model has greater, earlier, and more detailed results. This node performs well in the time interval (130s, 160s) after a penalty interval to gain a good reputation.

The proposed model will effectively minimize the risk, benefiting from the trust attribute 'historical trust recommendation' as seen in Fig. 15. The node's trust value is flat, while other models' trust values have more significant variance. This experiment also shows that confidence is hardly acquired when losing quickly. Our model will also counter grey hole, black hole, and alteration attacks based on the attribute 'subjective observation'. It can also handle DoS attacks, collusion attacks, and hybrid methods, as it is a deformation of the neighborhood sensing trust computing system (see Table 10).

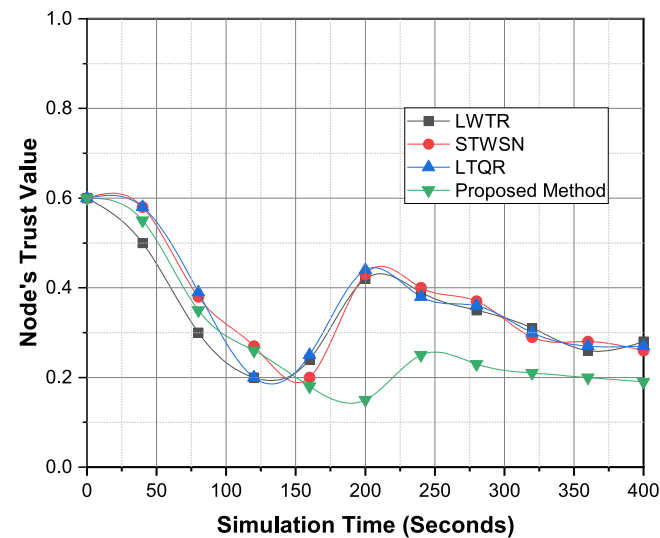
Fig. 16 illustrates the contrast of various trust models' convergence period. A quicker convergence time is available for our cur-



**Fig. 14.** Satisfaction ratios of different trust models.

**Table 9**  
Security strength Comparison 2.

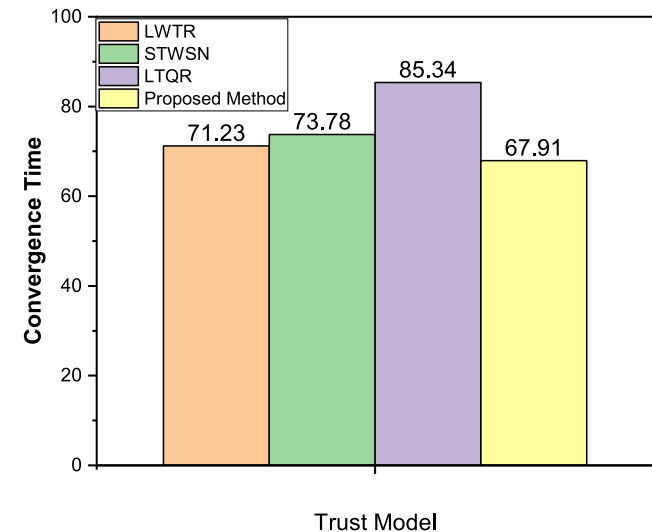
Parameter	Base key score	Proposed key score
Entropy	181.3 bits	209 bits



**Fig. 15.** Node's trust values in different models.

**Table 10**  
Security strength Comparison 3.

Parameter	Base Key Score	Proposed Key Score
Entropy	2.41 value	3.96 value



**Fig. 16.** Convergence period of trust models.

**Table 11**  
Security strength Comparison 4.

Parameter	Base Key Score	Proposed Key Score
Entropy	54x10 <sup>5</sup> 7	49X10 <sup>6</sup> 3

rent trust model. The explanation for this is that the currently proposed system adopts an iterative method of estimation, and the confidence level updating procedure is only linked to the latest trust information (see Table 11).

The benefits of the proposed method are:

1. Three trust characteristics (i.e., Subjective Observation, Link Propagation Capacity, and Historical Trust Recommendation) are added to reflect the trust relationship's difficulty and ambiguity.
2. It uses small computing resources and has high extensibility.
3. We suggest the SCGM (1,1)-weighted Markov stochastic chain approach after performing a thorough analysis to predict the spectrum of random fluctuations accurately and further optimize the results.
4. The weight issue of multiple attributes has been correctly solved by our model. The weight vector is determined by the simple AHP system, which makes our model more rational.

A proposed trust mechanism, which is divided into trust creation and trust estimation. We used an illustration to demonstrate our trust prediction process and subsequently performed a detailed trust model evaluation.

Possible tests have been conducted to simulate and present the feasibility of this new trust model. We intend to perform an in-depth analysis of trustworthy routing strategies in future work, considering the criteria for problems in the implementation field, network implementations, and security standards. Trust calculations and management can also be an appealing objective for attackers, based on these trust calculations. A malicious node will act well towards one group of nodes and badly towards another group; this is an assault of opposing behavior. The most reliable routing decisions in MANETs, defense mechanisms are needed to guarantee trustworthy knowledge, confidentiality, and integrity.

## 6. Conclusion

Successful authentication is crucial to ensuring the secure and effective execution of the supported application in mobile ad hoc networks. New authentication based scheme explicitly designed for the MANET nodes. The primary purpose of organizing such an algorithm is to provide a robust trust-based authentication mechanism for adopting the frequently changing topology. Such network protocol schemes are designed especially for the authentication of the new member in serverless computing. It involved the various subsections that include Registering the user, Generation of Token, Sending Message, and Receiving Message through different algorithms developed. The execution work is performed on the MATLAB. The re-enactment of the base work and the proposed work is finished by structuring the GUI. A session token is further validated using the various online password checking tools and the results obtained are quite impressive. SHA, which represents a secure hash algorithm, is a cryptographic hashing algorithm used to decide the trustworthiness. The various entropy graphs represent results with the improvement in reliability. And above all, the session's strength token pattern is further validated using the different online password checking tools and the results show improvement over others.

Improvement of the security methods in the network is a continuous process. We will first aim for the practical and live implementation of the work we have proposed in the future. We will then like to work on the security enhancement of the proposed work, with the extension of the security by addition of DNA-based safety and Retina-based security with associating the users with the nodes.



## Declaration of Competing Interest

We will then like to work on the security enhancement of the proposed work, with the extension of the security by the addition of DNA-based safety and Retina-based security.

## References

- [1] Kumar A, Dadheech P, Singh V, Poonia RC, Raja L. An improved quantum key distribution protocol for verification. *J Discrete Math Sci Cryptogr* 2019;22(4):491–8. doi: <https://doi.org/10.1080/09720529.2019.1637153>.
- [2] Gomathi K, Parvathavarthini B. An efficient cluster based key management scheme for MANET with authentication. In: *Proceedings of the 2nd international conference on trendz in information sciences and computing TISC-2010*. p. 202–5. doi: <https://doi.org/10.1109/TISC.2010.5714639>.
- [3] Nguyen DQ, Toulgoat M, Lamont L. Impact of trust-based security association and mobility on the delay metric in MANET. *J Commun Netw* 2016;18(1):105–11. doi: <https://doi.org/10.1109/JCN.2016.000013>.
- [4] Chandramohan D, Sathian D, Rajaguru D, Vengattaraman T, Dhavachelvan P. A multi-agent approach: to preserve user information privacy for a pervasive and ubiquitous environment. *Egyptian Inf J* 2015;16(1):151–66. doi: <https://doi.org/10.1016/j.eij.2015.02.002>. URL: <http://www.sciencedirect.com/science/article/pii/S110866515000067>.
- [5] Homomorphic encryption systems statement. Trends and challenges. *Comput Sci Rev* 2020;36. doi: <https://doi.org/10.1016/j.cosrev.2020.100235>.
- [6] Alaya B. Efficient privacy-preservation scheme for securing urban p2p vanet networks. *Egyptian Inf J*. doi: <https://doi.org/10.1016/j.eij.2020.12.002>. URL: <http://www.sciencedirect.com/science/article/pii/S110866520301614>.
- [7] Alaya B, Zidi S, Touil S, Chouchane WA. Resource reservation and dynamic admission control for distributed multimedia systems..
- [8] Safdar GA, O'Neill MP. Performance analysis of novel randomly shifted certification authority authentication protocol for MANETs. *Eurasip J Wireless Commun Network* 2009. doi: <https://doi.org/10.1155/2009/243956>.
- [9] Alaya B, Khan R. QoS enhancement In VoD systems: load management and replication policy optimization perspectives. *Comput J* 2020;63(10):1547–63. doi: <https://doi.org/10.1093/comjnl/bxaa060>.
- [10] Liu L, Yin L, Guo Y, Fang B. Bargaining-based dynamic decision for cooperative authentication. In: *MANETs, Proceedings – 2014 IEEE 13th international conference on trust, security and privacy in computing and communications, TrustCom 2014; 2015*. p. 212–20. doi:10.1109/TrustCom.2014.32..
- [11] Amit Kumar Bairwa SJ. An agent based routing search methodology for improving qos in manet. *Ingeniare Revista chilena de ingeniería* 2020;28(04):558–64.
- [12] Amit Kumar Bairwa SJ. Mla-rpm: A machine learning approach to enhance trust for secure routing protocol in mobile ad hoc networks. *Int J Adv Sci Technol* 2020;29(04):11265–74.
- [13] Amin U, Shah MA. A novel authentication and security protocol for wireless adhoc networks. In: *ICAC 2018 - 2018 24th IEEE international conference on automation and computing: improving productivity through automation and computing (September)*. p. 6–7. doi: <https://doi.org/10.23919/ICAC.2018.8748982>.
- [14] Choochotkaew S, Piromsopa K. An analysis of authentication models for MANETs. In: *Proceedings – 2014 international conference on information science, electronics and electrical engineering, ISEEE 2014*, vol. 3; 2014. p. 1956–60. doi:10.1109/InfoSEEE.2014.6946265..
- [15] Xu Q, Zheng R, Saad W, Han Z. Device fingerprinting in wireless networks: challenges and opportunities. *IEEE Commun Surv Tutor* 2016;18(1):94–104. doi: <https://doi.org/10.1109/COMST.2015.2476338>.
- [16] Mohammed Ali A, Kadhim Farhan A. A novel improvement with an effective expansion to enhance the md5 hash function for verification of a secure e-document. *IEEE Access* 2020;8:80290–304.
- [17] Ranjan AK, Kumar V, Hussain M. Security analysis of tls authentication. In: *2014 International conference on contemporary computing and informatics (IC3I)*. p. 1356–60.
- [18] Blake-Wilson S. Extensible authentication protocol tunneled transport layer security authenticated protocol version 0 (eap-tlsv0).
- [19] Alamri N, Chow CE, Aljaedi A, Elgzil A. Ufap: Ultra-fast handoff authentication protocol for wireless mesh networks. In: *2018 Wireless Days (WD)*. p. 1–8.
- [20] Lu Z, Wang Q, Chen X, Qu G, Lyu Y, Liu Z. Leap: A lightweight encryption and authentication protocol for in-vehicle communications. In: *2019 IEEE Intelligent Transportation Systems Conference (ITSC)*. p. 1158–64.
- [21] Zegeye W, Moazzami F. Authentication of iot devices for wifi connectivity from the cloud. In: *2019 53rd Annual conference on information sciences and systems (CISS)*; 2019. p. 1–6..
- [22] Fan C, Lin Y, Hsu R. Complete eap method: User efficient and forward secure authentication protocol for ieee 802.11 wireless lans. *IEEE Trans Parallel Distrib Syst* 2013;24(4):672–80.
- [23] Fan C, Lin Y, Hsu R. Complete eap method: User efficient and forward secure authentication protocol for ieee 802.11 wireless lans. *IEEE Trans Parallel Distrib Syst* 2013;24(4):672–80.
- [24] Zhang K, Lu R, Liang X, Qiao J, Shen XS. Park: A privacy-preserving aggregation scheme with adaptive key management for smart grid. In: *2013 IEEE/CIC international conference on communications in China (ICCC)*. p. 236–41.
- [25] Rajput S, Trivedi MC. Securing zone routing protocol in manet using authentication technique 2014:872–7. doi: 10.1109/JCN.2014.184. URL: <https://doi.ieeecomputersociety.org/10.1109/JCN.2014.184>.
- [26] Patidar M, Sharma MK, Bunglowala A. Multilevel authentication for resource allotment in MANET. In: *Proceedings of the 2014 conference on IT in business, industry and government: an international conference by CSI on Big Data CSIBIG 2014*. p. 49–52. doi: <https://doi.org/10.1109/CSIBIG.2014.7056937>.
- [27] Zhu Xingliang Xu. Shilian: A new authentication scheme for wireless ad hoc network 2012:312–5.
- [28] Neelavathy Pari S, Jayapal S, Duraisamy S. A trust system in manet with secure key authentication mechanism. In: *International conference on recent trends in information technology, ICRITIT 2012*. p. 261–5. doi: <https://doi.org/10.1109/ICRITIT.2012.6206818>.
- [29] Dilli R, Reddy PCS. Trade-off between length of the Hash code and performance of hybrid routing protocols in MANETs. In: *Proceedings of the 2016 2nd international conference on applied and theoretical computing and communication technology iCATcCT 2016*. p. 732–5. doi: <https://doi.org/10.1109/ICATcCT.2016.7912096>.
- [30] Ravilla D, Putta CSR. Implementation of HMAC-SHA256 algorithm for hybrid routing protocols in MANETs. In: *International Conference on Electronic Design, Computer Networks and Automated Verification, EDCAV 2015*. p. 154–9. doi: <https://doi.org/10.1109/EDCAV.2015.7060558>.
- [31] Yadav P, Hussain M. A secure AODV routing protocol with node authentication. In: *International conference on electronics, communication and aerospace technology*. p. 489–93.
- [32] Yang HS, Yoo SJ. Authentication techniques for improving the reliability of the nodes in the MANET. In: *International conference on IT convergence and security, ICITCS 2014*. p. 1–3. doi: <https://doi.org/10.1109/ICITCS.2014.7021743>.
- [33] Singare YP, Tembhurkar M. Design of an efficient initial access authentication over MANET. In: *International conference on industrial instrumentation and control, ICIC 2015 (Icic)*. p. 1614–9. doi: <https://doi.org/10.1109/IIC.2015.7151008>.
- [34] Sachin Malhotra MCT. doi:10.1007/978-981-10-5523-2\_16..
- [35] Test password entrop. URL: <https://password.blue/test.html>.
- [36] Test password entrop. URL: <http://rumkin.com/tools/password/passchk.php>.
- [37] Test password entrop. URL: <https://www.cryptool.org>.
- [38] Marchang N, Datta R. Light-weight trust-based routing protocol for mobile ad hoc networks. *Inf Secur IET* 2018;6:77–83. doi: <https://doi.org/10.1049/iet-ifs.2010.0160>.
- [39] Khatoun R, Begriche Y, Juliette D, Khokhi L, Serhrouchni A. A statistical trust system in wireless mesh networks, annals of telecommunications - annales des télécommunications 71. doi:10.1007/s12243-015-0488-1..
- [40] Wang B, Chen X, Chang W. A light-weight trust-based qos routing algorithm for ad hoc networks 2014;13:164–80. doi: <https://doi.org/10.1016/j.pmcj.2013.06.004>.