I. J. Computer Network and Information Security, **2024, 6, 56-68**
Published Online on December 8, 2024 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2024.06.05

Two-factor Mutual Authentication with Fingerprint and MAC Address Validation

J.S. Jolin
Department of Computer Science and Engineering, Karunya Institute of Technology and Sciences, Coimbatore, Tamil Nadu, India
E-mail: jolinjs608@gmail.com
ORCID iD: https://orcid.org/0000-0002-2250-7246

A. Theophilus
Department of Computer Science and Engineering, Karunya Institute of Technology and Sciences, Coimbatore, Tamil Nadu, India
E-mail: theophilusa451@gmail.com
ORCID iD: https://orcid.org/0000-0002-4353-1931

A. Kathirvel*
Department of Computer Science and Engineering, Tagore Engineering College, Vandalur Rd, Chennai, Tamil Nadu, India
E-mail: kathirvela158@gmail.com
ORCID iD: https://orcid.org/0000-0002-1617-5564

Received: 05 May 2023; Revised: 12 July 2023; Accepted: 02 October 2023; Published: 08 December 2024

Abstract: Mobile Ad hoc NETworks (MANET), unlike typical wireless networks, may be used spontaneously without the need for centralized management or network environment. Mobile nodes act as mediators to help multi-hop communications in such networks, and most instances, they are responsible for all connectivity tasks. MANET is a challenging endeavor because these systems can be attacked, which can harm the network. As a result, security concerns become a primary factor for these types of networks. This article aims to present an efficient two-factor smart card-based passcode authentication technique for securing legitimate users on an unprotected network. This scheme enables the password resetting feature. A secured mechanism for sharing keys is offered by using the hash function. We present a new two-factor mutual authentication technique based on an entirely new mechanism called the virtual smart card. Compared to authentication, the proposed method has fewer computation processes but is more time efficient since it is based on a hash function. Additionally, this approach is resistant to most attacker behaviors, such as Mutual authentication, Gateway node bypassing attacks, DoS attacks, replay attacks, Man in the middle attacks, and stolen smart device attacks. Experimental results validate the efficiency of this scheme, and its security is also analyzed.

Index Terms: Authentication Protocol, Mobile Ad hoc Networks, Smart Card, Security and Privacy, Two-factor Authentication.

1. Introduction

Mobile ad hoc networks (MANETs) have been extensively utilized in recent years for various dynamic purposes, including search and rescue operations and disaster relief efforts. Most apps rely on peer-to-peer networking. Messages from mobile nodes are sent via radio waves [1-3]. In an ad hoc network, the communication link used is broadcasted. It is a kind of multicast where the message is sent from source to destination. Multicasting is the method of sending messages from one node to another [4, 5]. This route is often used in corporate audio/video conferencing, collaborative communications, groupware systems, etc. A continuous flow of data packets may be shared across many destinations and when packets are retransmitted [6, 7].

Security is a key issue in MANETs due to the lack of infrastructure, which introduces several security concerns [8, 9]. Black hole attacks, spoofing attacks, Sybil attacks, Alteration, fabrication assaults, denial of service, jamming attacks and replay attacks are considered dangerous threats in MANET. MANETs need security services to minimize these threats: anonymity, authenticity, secrecy, availability, integrity, privacy and lack of reputation [10, 11].

Authentication and critical pre-distribution are used to deal with security threats in MANET [12, 13]. The message digest-5 (MD5) algorithms and secure hash algorithm-1 (SHA-1) provide a symmetric key-based authentication system. To design a route that is free of hostile nodes, secure route selection uses fuzzy logic. For malicious node identification, the node behavior assessments are examined. For addressing a dynamic environment in MANET, cluster-based routing methods are successful [14, 15]. Before forming a cluster for network management nodes, the nodes are authorized and grouped based on the received signal strength indicator (RSSI) and angle of arrival for network security. In a MANET system, lightweight cryptographic and trust-based routing approaches improve security. Cryptography methods maintain the confidentiality of transmitted data, while trust assessment methods determine the nodes' behavioral patterns [16, 17].

Numerous functional aspects listed below are critical in MANETs for enhancing privacy issues in the distributed system [18- 20].

- Authentication: The purpose of authentication was to verify statements regarding the validity of the data source.
- Confidentiality means only authorized persons or devices may access or execute secured systems and information.
- Integrity: Integrity refers to data that has not been altered or destroyed by unauthorized users.
- Availability refers to a network's ability to supply services when needed.

To improve the security of MANETs, a unique node authentication approach is proposed. Two-factor authentication (2FA) is presented as a solution using a unique idea known as a virtual smart card. Two-factor authentication is a way of authenticating a user's claimed identity by combining two distinct factors: 1) something they have, 2) something they know, or 3) something they are, i.e., a fusion of physical entities and passwords such as fingerprints, mobile phones, tokens or smart cards. However, when a physical item is employed as the second authentication factor, several more operation steps are introduced, making two-factor authentication difficult for users compared to password-based single-factor authentication. The scheme satisfies all major security standards.

The main contributions of the paper are the following:

- We present a new two-factor mutual authentication technique based on an entirely new mechanism called the virtual smart card.
- The fingerprint and MAC address will form the foundation of node determination in the mutual authentication-based protocol based on dual authentication.
- The TOTPS Algorithm is a new proposed technique that provides a time-based OTP for secure information exchange.
- Sha-512 is proposed to generate the hash code.

The remainder of the paper is structured as follows. Section 2 presents related work in the field of smart card-based authentication schemes. A secure smart card-based authentication scheme is proposed in Section 3. Section 4 includes a security analysis. Section 5 is an evaluation of the designed framework, which includes the implementation part, that discusses the technology employed to execute the dissertation work and the outcome analysis, which describes the proposed work's efficiency. Finally, Section 5 concludes the paper.

2. Literature Survey

Many researchers are experienced with various IDS for protecting the MANET. In this section, we review some of the prior network security techniques relevant to our proposed techniques. Kumari et al. [21] suggested an authentication scheme based on enhanced ECC for the same scenario. The suggested scheme ESEAP has protected resilience due to several attractive privacy features and functions such as timely typo, no password exposure, sound reparability, parallel attack, message authentication, insider attack, forward secrecy, lack of clock synchronization attack, server spooling attack, impersonation attack, replay attack, anonymity, mutual authentication, smart card loss attack, lack of a password verifier table and off-line password guessing attack. Additionally, the study illustrates a formal security assessment of the ESEAP using a random oracle model.

Integrating PUFs and fingerprint biometrics, Bian et al. [22] demonstrated a secured and lightweight 2FA and essential agreement technique. They suggested using PUFs as an additional authentication factor, in addition to the user's biometrics, to enable two-factor authentication to remote authentication schemes. PUFs are used in our scheme to improve the design's security, inspired by PUF-based lightweight mutual authentication in IoT systems. Additionally, the user may log into the remote network using his fingerprint, eliminating the need for passwords. As a result, the user is relieved of the responsibility of memorizing and updating their password. Their suggested approach, which combines PUFs with fingerprint biometrics, addresses the aforementioned issues while also maintaining the required security and efficiency criteria.

Singh et al. [23] designed a smart card authentication system based on the elliptic curve Signcryption that includes security properties such as forward security, availability, anonymity, mutual authentication, message integrity, non-repudiation and message confidentiality. Moreover, the analysis of security features reveals that the protocol developed

and explained in this work is secure from known key attacks, man-in-the-middle attacks, insider attacks, replay attacks, de-synchronization attacks, user and server impersonation and password guessing attacks.

Hossain et al. [24] devised the ICAS system, a two-factor-based identity-concealed authentication technique. ICAS protects the user's identity from attackers, avoids leaking personal information, and protects against device loss threats. They provide a strong security model in the random oracle and show ICAS security. Additionally, they present a detailed performance review that demonstrates ICAS's efficiency.

To address the security issues in their method, Sudhakar et al. [25] developed a new secured, mutually authenticated key-sharing mechanism for the multi-server scenario. They formalize the suggested scheme's strong authentication using Burrows–Abadi–Needham logic and assess threats utilizing automated web security protocol and app tool testing. The latest 2FA system is extensively cryptanalyzed and determined to be vulnerable to man-in-the-middle attacks, stolen smart cards, user impersonation, replay and offline password guessing.

Wu et al. [26] suggested a lightweight mutual identity authentication system using the SM2 digital signature and public key encryption. After authentication and key agreement, this approach generates a secured secret session key. Additionally, it can withstand numerous cyber-attacks, including MITM and replay threats.

Chilveri et al. [27] developed an ECC-based security mechanism in the prime area. The hash function provides a secure method to exchange keys. Before sending a message from one node to another, it must be determined whether the receiving node is permitted. A unique authorizing method based on two servers, a normal server and a master, is devised. As a result, compromising one of the servers never compromises the whole authentication system. Initially, a node must register its credentials with the registration center, which then distributes them to the server via a secured distribution method.

3. Methodology

MANET authentication is classified into data, node, and user. The proposed technique is based on the following process:

- Pre-deployment phase
- Registration phase
- Destination MAC Address Validation
- Login phase
- Mutual Authentication phase
- Biometric change phase
- Sender Module
- Receiver Module

Table 1. Notations

Notation	Description
SID_j	$S_j's$ identity
GWN	Gateway node
U_i	User i
UID_i	$U_i's$ identity
$GWNP\_U_i$	Secure passkey of GWN shared with U_i
MID_i	Masked identity of use
BIO_i	Biometric feature of User U_i
$\oplus$	Performing XOR operation
$\|\|$	Concatenation operation
Xg	The secret key is only known to the gateway, GW
Xgw	Shared secret with the user by the gateway
S_k_GWN	Secret key of GWN
$TOTP_i$	Generated One one-time password for the user
TSM_1	Timestamp
ΔT	Allowed transmission delay
DoS	Denial of Service

During the registration process, the user selects their login credentials and completes a registration form, giving the server certain personal information. The *GWN* provides a smart card that may include certain personal information. The user will be allowed to access the *GWN* during the authentication process after completing the registration phase. The dual-factor protocol assures that the *GWN* can verify only the user who holds a valid smart card and the relevant passcode.

Table 1 shows the notations used to describe the authentication mechanism.

3.1. Pre-deployment Phase

This phase is configured offline by the network administrator using a configuration server. Each sensor node is assigned a unique identifier SID_j . Each node has a legitimate MAC address, which is shared with the *GWN* through proper cryptographic mechanisms, especially during the offline mode.

3.2. Registration Phase

$MID_i=h(UID_i||r_i)$ is calculated by the node U_i, where r_i is a random number. We employed time-based-One Time Password (TOTP) authentication in this step to verify that Gateway *GW* communicates with the correct user U_i, who claims to be that node U_i is authorized by Gateway. The network's sensor nodes are supposed to have a maximum count of *m*. Additionally, *GWN* stores SID_j . Gateway creates a smartcard for the User upon authentication. This smartcard will be used for further authentication when nodes seek to interact. *GWN* does the following operations sequentially. $MXIP_i = GWNP\_U_i$ and $X_i = h(MID_i||S_k\_GWN)$ is computed first. After calculation, these variables $\{MXIP_i, X_i, h(.)\}$ are securely stored on the smart card USC_i and sent to the user U_i. After obtaining the smart card USC_i, user U_i recovers his secret by calculating $GWNP\_U_i = MXIP_i \oplus h(MID_i)$, imprinting the biometric parameter BIO_i at the sensor, and evaluating $img_x = BH(r_i \oplus BIO_i)$, $V_i = h(GWNP\_U_i||img_x)$ and $A_i = h(UId_i) \oplus r_i$. Finally, each of these data $\{MXIP_i, X_i, BH(.), h(.), V_i, A_i\}$ are put onto the smart card USC_i. Finally, a MAC address is produced and saved in the GWN using the SHA-512 method.

The Gateway and User steps are given below:

Step 1: The node U_i creates its identity ID_i, biometric information BIO_i, and a number $r_i=h(UId_i)||X_{gwn})$. Then, the node calculates masked identity $MID_i = h(UId_i||r_i$, masked biometric $MID_i = h(BIO_i||r_i)$.

Step 2: Next, the node transmits a request message with the data $<MID_i, MBIO_i, TSM_1>$ to the gateway node, *GWN*.

Step 3: When the message is received, the gateway *GWN* examines the timestamp $|TSM1 - T|<\Delta T$. If the time interval for transmitting delays ΔT is smaller than the time interval for message receiving, the information has not been intercepted by the intruder. The gateway will then create a Time-based One Time Pad $TOTP_i$ for the user. The following gateway calculates $r_i = h(MID_i || X_g)$, $y_i = h(MBIO_i || X_{gwn})$ *and* $z_i = r_i \oplus TOTP_i$. The $TOTP_i$ is then stored by the gateway for subsequent verification.

Step 4: The message $<r_i, y_i, z_i, TSM_2>$ is then sent to the user through a secure channel via the gateway.

Step 5: The destination node verifies the timestamp for message interception when the message is received. If the communication is not intercepted, $TOTPi = r_i \oplus z_i$ is extracted, and $e_i = TOTP_i \oplus y_i$ is calculated.

Step 6: The message $<e_i, y_i>$ is now sent to the gateway by the source node.

Step 7: The gateway then determines $TOTP_i* = e_i \oplus y_i$. The gateway subsequently verifies if the original stored $TOTP_i$ and OTP_i* are identical. If $TOTP_i == TOTP_i*$, it indicates that the user U_i who originated the transaction is authorized for gateway registration. Now, the gateway builds a smartcard for the source node, saves it in memory, and calculates $f_i=USC_i, \oplus TOTP_i$. After registering the user, the gateway deletes the $TOTP_i$ from its storage.

Step 8: In this case, the gateway provides the user with other data $<MID_i, r_i, y_i, z_i, f_i>$.

Step 9: The destination node U_i decrypts this message, which includes device information such as a 48-bit MAC address destination and source addresses.

3.3. Destination MAC Address Validation

Since every node U_i needs to be registered with the *GWN* after the deployment phase through the MAC addressing scheme *where i=1,2,3,….n and j=1,2,3….m such that m < n.* Moreover, every *GWN* maintains a record for registrations, i.e., *MACTable*, where member node information is stored, i.e., $U_i \in GWN$. A device/node U_i can trigger the communication process with a particular *GWD* ***iff*** U_i is registered with $U_i \in MACTable(GWN)$.

3.4. Login Phase

Login phase U_i selects a random S_j and performs the login procedure by providing $TOTP_i^*, USC_i$ computes $MP_i^* = h(r_i||TOTP_i^*), x_i = e_i \oplus f_i$ *and* $x_i^* = h(MP_i^*||GWNP\_U_i). If\ x_i^* =? x_i$ satisfies, then the user or node is logged in successfully and smart card selects a nonce K_i, and evaluates $N_i = h(x_i || |GWNP\_U_i| || |T_1)$, $Z_i = K_i \oplus f_i$. Then it sends the login request message $\{MI_i, e_i, N_i, Z_i, T_1\}$ to the chosen S_j through a public channel.

3.5. Mutual Authentication Phase

Nodes seek to interact with one another at this phase. Mutual authentication is performed via the proposed protocol between the destination and source nodes. The steps involved in mutual authentication are as follows:

Step1: Source node computes $a_i=h(MID_i||MBIO_i||TOTP_i)$, $b_i=a_i \oplus GWNP\_U_i$

Step 2: Source node sends $<b_i, TSM_1, n_u>$ to the destination node. The source node sends its smart card to the destination node for authentication.

Step 3: On receiving parameters, the destination node computes $a_i=H(MID_i||TOTP_i)$, $b_i=a_i \oplus GWNP\_U_i$.

Step 4: The destination node sends the source node smartcard to the gateway for verification that the node is registered because only the gateway knows the information and MAC address of the nodes. So the destination node sends $<b_i,n_i>$ to the gateway.

Step 5: The destination node sends $<b_i,n_i>$to the gateway to verify the source node registration status.

Step 6: After receiving messages from both the client and the device, the gateway computes $a_i^*=H(MID_i||MBIO_i||TOTP_i)$, $GWNP\_U_i^*=a_i^* \oplus b_i$ and $a_i^*=h(MID_i||n_i)$, $GWNP\_U_i^*=a_i^* \oplus b_i$. Gateway then checks if $GWNP\_U_i^*=GWNP\_U_i$ (at the registration phase, smartcard-based fingerprints for both source and destination nodes were stored). The gateway notifies the device that the node has been enrolled and authorized, as well as notifies the user that the sensor has been enrolled and verified.

3.6. Biometric Change Phase

The node submits its UId_i and the old biometric feature $UBIO_i^{OLD}$ which is the current feature of the smart card reader. USC_i computes $MP_i^* = h(r_i||\text{UBIO}_i^{\text{OLD}})$, $MI_i^* = h(r_i||UId_i), x_i^* = h(MP_i^*||GWNP\_U_i)$ and $x_i^* = h(MP_i^*||GWNP\_U_i)$ and $x_i^* = x_i$ is true, U_i inputs the new biometric feature $UBIO_i^{NEW}$. Now USC_i computes $MP_i^* = h(r_i||\text{UBIO}_i^{\text{NEW}})$, $MI_i^{NEW} = h(r_i||UId_i), e_i^{NEW} = f_i \oplus x_i^{NEW}$. Finally, USC_i replaces the old value of e_i with e_i^{NEW} in its memory.

3.7. Sending Message

Following validation, the initiation of the message process begins. The transmitter will send the recipient with the Message Transaction Identity and TOTP which is a collection of random integers and a message hash extraction.

3.8. Receiving Message

At the recipient's end, the receiver will input a message transaction ID and TOTP to decode the message. Following that, it will validate the message's recipient using the message's SHA-512 code. The receiver will compare the received message's SHA-512 code to the message's SHA-512 code, and if both are identical, the message is confirmed to have been received successfully. The generated MAC address and fingerprint are hashed and saved in the gateway node using SHA-512 coding. Additionally, this may be utilized as a component of mutual authentication.

4. Security Analysis

The two-factor mutual authentication technique provided here may withstand the following attacks:

4.1. Mutual Authentication

Mutual authentication occurs when both the users and the device authenticate. The proposed protocol meets this. Before exchanging data, both the user and the sensor are authorized.

4.2. Gateway Node Bypassing Attack

The presented protocol is protected against a passing attack on the gateway node. Authentication cannot begin until the user, U_i, communicates with the sensor, S, and not the gateway, GWN. The sensor then establishes a connection and transmits the authentication data to the gateway, GW. Both the user, U, and the sensor, S, are verified by the gateway.

4.3. Denial of Service Attack

The presented method is DoS threat resistant. Because both the user and the sensor get an acceptance or disapproval message from the gateway. Additionally, the use of a time stamp mitigates any urgent request. As a result, this protocol is resistant to DoS attacks.

4.4. Replay Attack

If the intruders can access the message $<BIO_i, TSM_1, n_i>$ during the authentication phase and start a new session with the message $<BIO_i^*, TSM_1^*, n_i^*>$ to connect with the sensor. Because this protocol verifies the timestamp in every transfer, this conversation will be terminated.

4.5. Man in the Middle Attack

Assume an intruder eavesdrops on the $<BIO_i, TSM_1, n_i>$ authentication phase. He changes it to $<BIO_i^*, TSM_1^*, n_i^*>$. However, the attacker may only transfer this information to the sensors if he can compute the user's master key, MKU_{gwn} and $MBIO_i$. MKU_{gwn} is only known to the user, and to compute BIO_i, he needs biometric information n_i and r_i, which the attacker cannot manufacture. That is why this approach is impervious to man-in-the-middle attacks.

4.6. Stolen Smart Device Attack

A smart device might be stolen or lost. The intruder may use a memory attack to recover the stored information if lost. Assume that the attacker has the following information: $<BIO_i, r_i, y_i, z_i, f_i>$. The user's ID, U_i, is not recorded in a

clear way here. It is encrypted and kept masked. If the attacker intends to connect with Sensor S, it must compute BIO_i, something the attacker cannot do. Because the attacker requires knowledge of the User's, Ui's, and r_i's biometric information. Additionally, r_i is created using ID_i and X_{gwn}. However, the attacker cannot determine the user's ID, ID_i, since it is saved in masked form rather than plain text. As a result, this strategy is resilient to stolen smart device attacks.

5. Results and Discussions

The proposed task is organized in MATLAB, and the data network is completed in MSACCESS. It runs Windows 10 on an Intel i5 2.60 GHz processor with 16 GB of RAM. The MATLAB GUI part is utilized to structure the designing of the frameworks whose square measure is needed for utilization.

5.1. Implementation of the Proposed Work

The re-enactment of the essential work of the desk and the planned task is completed by constructing the GUI. The MATLAB GUI component enables us to create screens by drag-and-dropping controls onto the workspace. The registration form seen in Figure 1 will serve as the beginning point for our research. The node needs to be enrolled to carry on with the mutual authentication simulation. During the registration process, we require the following details: a fingerprint, a MAC address, an email address, and a user name. Next, the SHA 512 techniques are used to build a hash that matches the fingerprint and MAC addresses, which is then used to construct the TOTP.

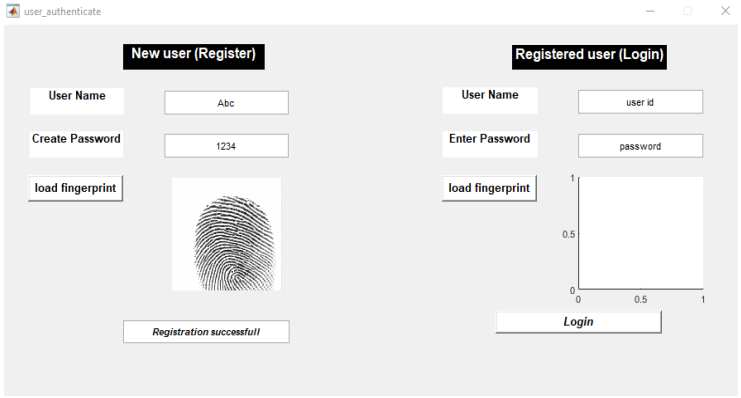

Fig.1. Registration form

Fig.2. Input as fingerprint

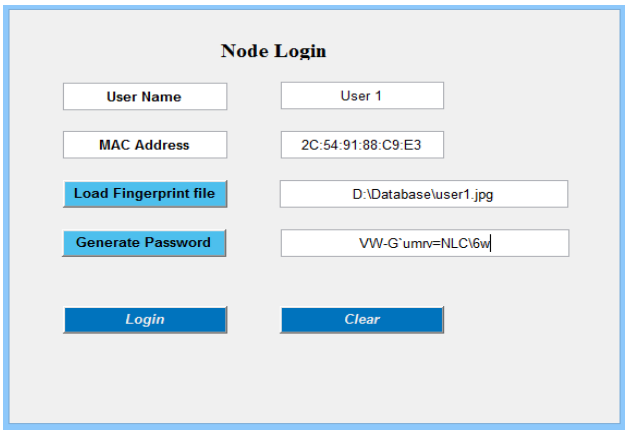

Fig.3. Login form

The Login form, seen in Figure 2, is used to authenticate verified users. The following information about the user is recorded for validation purposes: MAC address, user name and fingerprint. The details are then compared to the node's data, which is stored in the UserData database before the hash is generated once more employing the SHA-512 algorithm. Accessibility to the information system is granted if the user's information is confirmed to be accurate (see Figure 3).

The control panel for the user in Figure 4 displays the two-way channel, "Transfer Data after Validation," employed to transfer information to the destination node. "Receive Data after Integrity Check" receives information from another node.

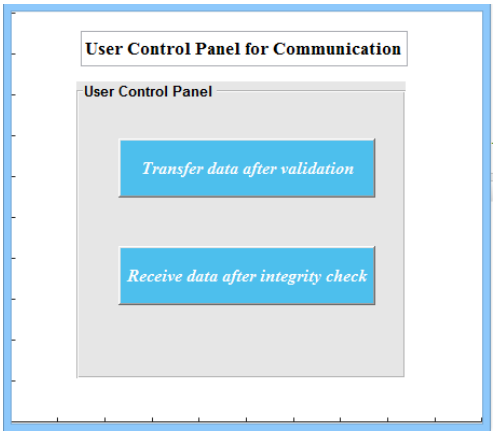

Fig.4. User control panel

For the purpose of sending data to the other node, use the form in Figure 5. Based on the points offered during the login procedure, the user logged in is immediately retrieved. When a form appears, information like the user's name of the person or node submitting the data and the node's MAC address is displayed. The gateway node then generates the smartcard, which includes the user's information, such as fingerprints and MAC address.

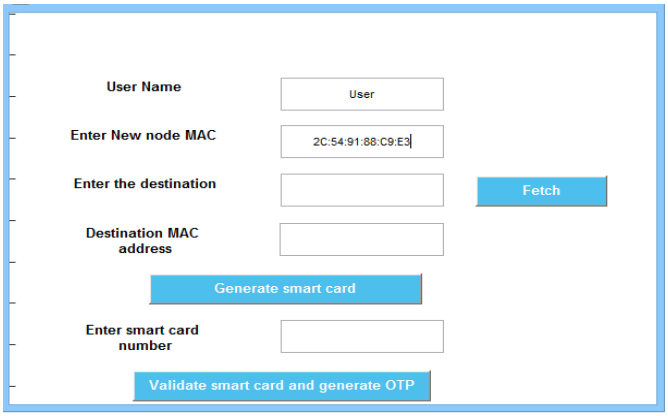

Fig.5. Data sending form

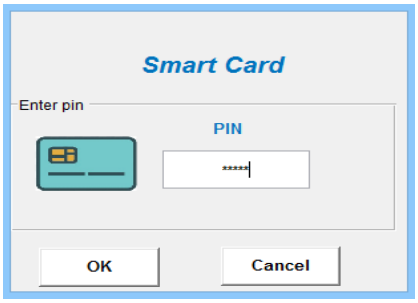

Fig. 6. Authenticated Login using smartcard

The smartcard must be input by the user who wants to send data to another node, and if the smartcard is valid, the network nodes will provide the MAC address if necessary. The field Node No, which contains the network node number, is part of the "Network nodes" table's framework, which is depicted in Table 2. The TOTP is generated once the destination node's MAC address has been determined. The sender's and destination's MAC addresses are hashed utilizing

SHA, and random integers are used to create the TOTP. The architecture of a smartcard with pin generation is seen in Figure 6.

Table 2. Network nodes

Field Name	Description
Nodeno	Stores the number of nodes that is automatically incremented
MACadrs	Store the address of the MAC node

In the final stage, a series of random numbers produces TOTP. The messages will be encrypted with TOTP for transmission, and a SHA 512 hash of the data will be generated for verification. The data transmitted between the sender and destination nodes is identified by a unique transaction ID assigned to every transaction. Now that the information has been validated and found to be accurate, the sender submits it. The destination node needs the transaction ID and TOTP for this to happen. Data is then obtained from data logs after validation.

5.2. Performance Comparison

We compare the proposed scheme's performance and security to those of similar schemes in the literature on four aspects 1) Communication cost, 2) Execution time 3) Security strength, 4) Communication overhead and 5) Node trust value.

5.3. Performance Scheme

This work has been conducted to determine the efficacy of our technique.

A. Communication and Smartcard Storage Costs (in Bits) Comparison

In Table 3, shows the cost of smartcard storage for our protocol and other methods, as well as a comparison in Figure 7. In terms of communication and smartcard storage costs, the structure of our protocol is moderate, which means that it is occasionally less expensive and often more expensive than a couple of the protocols under consideration.

Table 3. Smartcard storage costs (in bits) comparison

Schemes	Smart card storage cost
LTQR	768
E-PAC	864
UFAP	832
ESEAP	768
Proposed	670

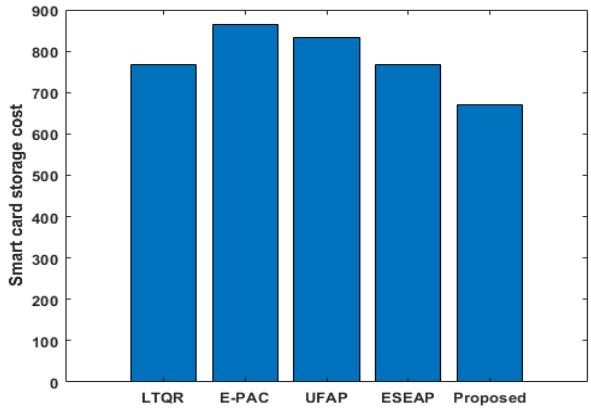

Fig.7. Smartcard storage cost (in bits)

B. Comparative Analysis of Different Protocols for Execution Time (ms)

As seen in Table 4, our protocol executes faster than current protocols. Our protocol protects against known attacks using a verification phase, an efficient login phase, mutual authentication, user anonymity, and session key agreement, and the system's response time is much smaller than previous protocols.

Table 4. Execution time (Ms) comparison of our protocol with other protocols

Schemes	Server	User	Total
LTQR	7.3235 ms	5.4966 ms	12.8200 ms
E-PAC	7.5621 ms	3.6701 ms	11.2322 ms
UFAP	3.6562 ms	3.6566 ms	7.3128 ms
ESEAP	3.7865 ms	3.6562 ms	7.4427 ms
Proposed	5.4837 ms	1.8287 ms	7.3126 ms

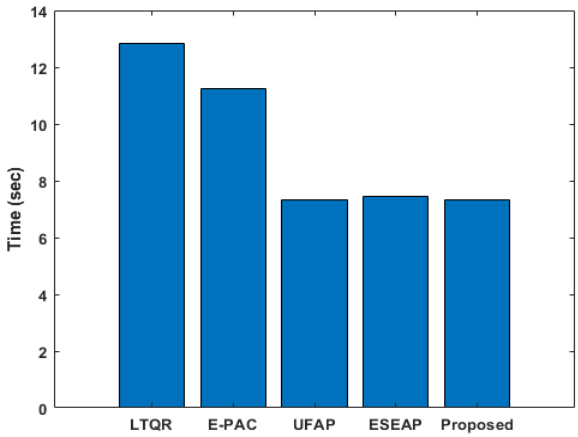

Fig.8. Comparative analysis of different protocols for execution time (ms)

To assist comprehension, we compare the proposed protocol's execution time (ms) to that of existing protocols as shown in Figure 8. The existing schemes like LTQR, E-PAC, UFAP and ESEAP are compared with the proposed approach. While compared with others, the proposed approach yields less protocol execution time. The second protocol's execution time occurs in ESEAP. The LTQR scheme requires much more attention.

C. The Volume of Authentication Messages with the Increased Number of Clients

The number of authentication messages that transit the network affects the network's throughput. When a significant number of users attempt to authenticate, or re-authenticate, to the network, the network might become congested due to the high amount of authentication messages.

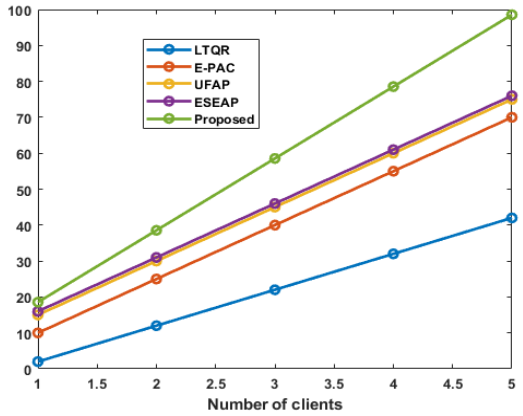

Fig.9. Number of authentication messages for each protocol

The amount of authentication messages increases as the number of users increases in Figure 9. As users or clients visit the system more frequently, the volume of authentication messages typically rises. Due to the requirement to verify and authorize every client/user to guarantee secure access to the system, the number of messages has increased. The proposed scheme has increased the number of clients for the volume of authentication.

D. Security Strength

"Security strength" refers to the resilience and protection that a security method, protocol, or system offers against various threats and vulnerabilities. It assesses how successfully a security solution can fend off attacks and safeguard critical data.

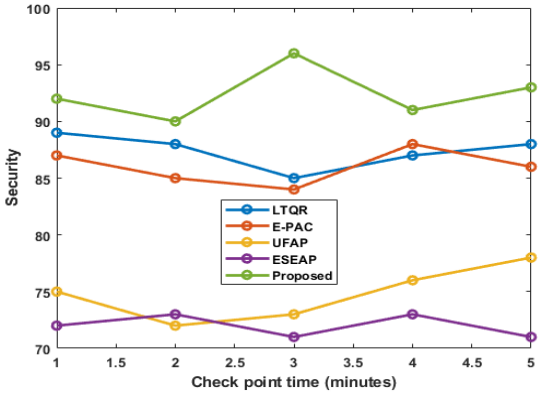

Fig.10. Security strength of proposed and existing methods

Most certainly, the proposed method's security is around 88%, which is superior to the other approaches used in this research. The proposed technique also obtains a stronger security value of 91%, while the closest equivalent method reached 89%. Other approaches have an average security grade of 85%. The security of the proposed approach is shown clearly in Figure 10.

E. Communication Overhead

The memory overheads of node authentication utilizing a hash-based smartcard approach are shown in Table 5 and Figure 11. We discovered that the designed methodology had the least memory overhead compared to alternative mechanisms. As a result, our approach is appropriate for mutual authentication of sensor nodes deployed in MANETs. Existing techniques for minimizing communication overhead aim to reduce the cost of inter-process or inter-node communication, which can negatively impact system performance and scalability. Existing systems might be challenging to retrofit with new methods for reducing communication overhead, mainly if they rely on outdated protocols. While comparing with the existing scheme, the proposed communication overhead was low. The existing E-PAC scheme requires much more attention.

Table 5. Comparison of Communication Overhead

Schemes	Communication overhead
LTQR	3 messages (2880 bits)
E-PAC	4 messages (2240 bits)
UFAP	3 messages (5056 bits)
ESEAP	3 messages (2994 bits)
Proposed	2 messages (2593 bits)

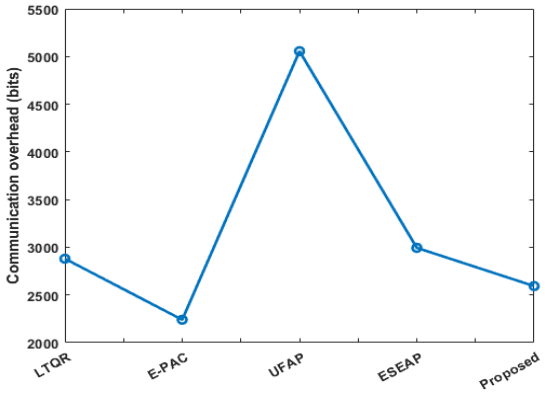

Fig.11. Analysis of communication overhead

F. Nodes Trust Value

As seen in Figure 12, the proposed model efficiently reduces risk by using the trust characteristic 'historical trust recommendations.' The trust value of the node is constant, while the trust values of many other models exhibit more volatility. Additionally, this experiment demonstrates that confidence is rarely built when one loses rapidly. Overall, node trust values are a crucial component of distributed and decentralized systems, enhancing the efficiency, security,

and dependability of communications among network users. They promote confidence and cooperation in contexts lacking in trust while empowering nodes to make informed decisions.

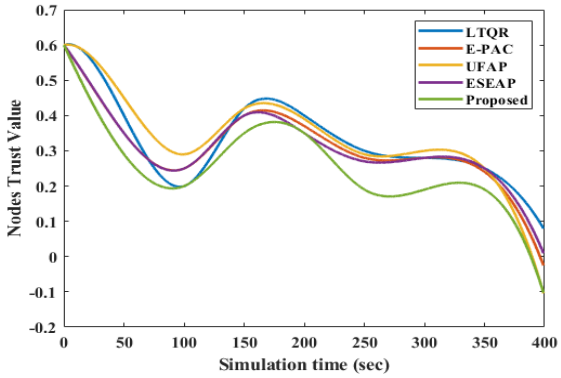

Fig.12. Node's trust value

Currently used methods Biometric information, which is vulnerable and susceptible to false positives and false negatives, is the foundation of fingerprint-based authentication. Failures in authentication or security vulnerabilities might be caused by environmental variables, user fingerprint alterations, or low-quality fingerprint readers. And also Implementing and managing two-factor authentication using MAC address and fingerprint validation can be difficult and may cause usability problems. It could be challenging for users to enroll their fingerprints or solve authentication issues. To overcome the existing approaches drawback, we introduced Mobile Ad hoc Networks (MANETs).

There are many benefits to using Mobile Ad hoc Networks (MANETs) in Two-Factor Mutual Authentication with fingerprint and MAC address validation, particularly in circumstances where traditional wired or centralized network infrastructure is neither practicable nor possible. Due to MANETs' support for dynamic network topologies and their design for mobile devices, the suggested approach has several advantages. This works effectively in situations like military operations, disaster recovery, or outdoor events when people and equipment are continuously on the move. Node failures and network splitting are not fatal to MANETs. The network may frequently self-organize and identify alternate communication pathways if a node goes down, ensuring excellent availability and fault tolerance. Utilizing both MAC address and fingerprint validation lowers the possibility of unwanted network access. Even with a legitimate fingerprint, an attacker would still need to successfully fake the MAC address, which is a more difficult process.

6. Conclusions

In MANETs, successful authentication is critical for assuring the effective and safe execution of the authorized application. New authentication-based strategy created specifically for MANET nodes. The main goal of developing such a framework is to provide a reliable security-based authorization method for adapting the constantly changing topology. This article presents a multi-factor secure smart card-based remote user authentication technique that is both lightweight and secure. In server-less computing, the network protocol techniques are created specifically for the authentication of new members. It included several subsections such as user registration, smart card authentication, sending and receiving messages, all of which were accomplished using various algorithms. MATLAB is used to carry out the execution task. By constructing the GUI, the re-enactment of the basic work and the required design is completed. The SHA-512 is a cryptographic hashing technique employed to determine trustworthiness. A thorough analysis of performance reveals that the proposed scheme provides more security than other existing approaches. While comparing with existing schemes, our proposed scheme obtained above 99% superior performances and it obtains less computational time which is 7.3126 ms.

Acknowledgements

We declare that this manuscript is original, has not been published before and is not currently being considered for publication elsewhere.

Conflicts of interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Funding

The author's received no financial support for the research, authorship, and/or publication of this article.

References

[1] M. Adil, R. Khan, M. A. Almaiah, M. Al-Zahrani, M. Zakarya, M.S. Amjad, and R. Ahmed, "MAC-AODV based mutual authentication scheme for constraint-oriented networks," *IEEE Access*, vol. 8, pp.44459-44469, 2020.

[2] U. Jain, M. Hussain and J. Kakarla, "Simple, secure, and lightweight mechanism for mutual authentication of nodes in tiny wireless sensor networks," *International Journal of Communication Systems*, vol. 33, no. 9, pp. e4384, 2020.

[3] M. Alshahrani and I. Traore, "Secure mutual authentication and automated access control for IoT smart home using cumulative keyed-hash chain," *Journal of information security and applications*, vol. 45, pp. 156-175, 2019.

[4] S. Singh and V. K. Chaurasiya, "Mutual authentication scheme of IoT devices in fog computing environment," *Cluster Computing*, vol. 24, no. 3, pp. 1643-1657, 2021.

[5] J. Xu, X. Meng, W. Liang, H. Zhou and K. C. Li, "A secure mutual authentication scheme of blockchain-based in WBANs," *China Communications*, vol. 17, no. 9, pp. 34-49, 2020.

[6] M. Adil, M. A. Jan, S. Mastorakis, H. Song, M. M. Jadoon, S. Abbas and A. Farouk, "Hash-MAC-DSDV: mutual authentication for intelligent IoT-based cyber-physical systems," *IEEE Internet of Things Journal*, vol.12, pp. 1-12, 2021.

[7] M. Barbareschi, A. De Benedictis, E. La Montagna, A. Mazzeo and N. Mazzocca, "A PUF-based mutual authentication scheme for cloud-edges IoT systems," *Future Generation Computer Systems*, vol. 101, no.2, pp. 246-261, 2019.

[8] M. Sidorov, M. T. Ong, R. V. Sridharan, J. Nakamura, R. Ohmura and J. H. Khor, "Ultralightweight mutual authentication RFID protocol for blockchain enabled supply chains," *IEEE Access*, vol. 7, pp. 7273-7285, 2019.

[9] Z. Xu, C. Xu, W. Liang, J. Xu and H. Chen, "A lightweight mutual authentication and key agreement scheme for medical Internet of Things," *IEEE Access*, vol. 7, pp. 53922-53931, 2019.

[10] Y. Zhang, K. Cheng, F. Khan, R. Alturki, R. Khan and A. U. Rehman, "A mutual authentication scheme for establishing secure device-to-device communication sessions in the edge-enabled smart cities," *Journal of Information Security and Applications*, vol. 58, pp. 102683, 2021.

[11] A. Kumari, S. Jangirala, M. Y. Abbasi, V. Kumar and M. Alam, "ESEAP: ECC based secure and efficient mutual authentication protocol using smart card," *Journal of Information Security and Applications*, vol. 51, pp. 102443, 2020.

[12] S. F. Chiou, H. T. Pan, E. F. Cahyadi and M. S. Hwang, "Cryptanalysis of the Mutual Authentication and Key Agreement Protocol with Smart Cards for Wireless Communications," *Int. J. Netw. Secur*., vol. 21, no. 1, pp. 100-104, 2019.

[13] A. K. Singh, A. Solanki, A. Nayyar and B. Qureshi, "Elliptic curve signcryption-based mutual authentication protocol for smart cards," *Applied Sciences*, vol. 10, no. 22, pp. 8291, 2020.

[14] L. Chen and K. Zhang, "Privacy-aware smart card based biometric authentication scheme for e-health," *Peer-to-Peer Networking and Applications*, vol. 14, no. 3, pp. 1353-1365, 2021.

[15] M. Karuppiah, A. K. Das, X. Li, S. Kumari, F. Wu, S. A. Chaudhry and R. Niranchana, "Secure remote user mutual authentication scheme with key agreement for cloud environment," *Mobile Networks and Applications*, vol. 24, no. 3, pp. 1046-1062, 2019.

[16] H. T. Pan, H. W. Yang and M. S. Hwang, "An enhanced secure smart card-based password authentication scheme," *Int. J. Netw. Secur*., vol. 22, no. 2, pp. 358-363, 2020.

[17] S. S. Sahoo, S. Mohanty and B. Majhi, "Improved biometric-based mutual authentication and key agreement scheme using ECC," *Wireless Personal Communications*, vol. 111, no. 2, pp. 991-1017, 2020.

[18] B. D. Deebak and F. Al-Turjman, "Smart mutual authentication protocol for cloud based medical healthcare systems using internet of medical things," *IEEE Journal on Selected Areas in Communications*, vol. 39, no. 2, pp. 346-360, 2020.

[19] M. K. Sharma and M. J. Nene, "Dual factor third-party biometric-based authentication scheme using quantum one-time passwords," *Security and Privacy*, vol. 3, no. 6, pp. e129, 2020.

[20] V. Sureshkumar, R. Amin, M. S. Obaidat and I. Karthikeyan, "An enhanced mutual authentication and key establishment protocol for TMIS using chaotic map," *Journal of Information Security and Applications*, vol. 53, pp. 102539, 2020.

[21] A. Kumari, S. Jangirala, M. Y. Abbasi, V. Kumar and M. Alam, "ESEAP: ECC based secure and efficient mutual authentication protocol using smart card," *Journal of Information Security and Applications*, vol. 51, pp. 102443, 2020.

[22] W. Bian, P. Gope, Y. Cheng and Q. Li, "Bio-AKA: An efficient fingerprint based two factor user authentication and key agreement scheme," *Future Generation Computer Systems*, vol. 109, pp. 45-55, 2020.

[23] A. K. Singh, A. Solanki, A. Nayyar and B. Qureshi, "Elliptic curve signcryption-based mutual authentication protocol for smart cards," *Applied Sciences*, vol. 10, no. 22, pp. 8291, 2020.

[24] M. J. Hossain, C. Xu, C. Li, S. H. Mahmud, X. Zhang and W. Li, "ICAS: Two-factor identity-concealed authentication scheme for remote-servers," *Journal of Systems Architecture*, vol. 117, pp. 102077, 2021.

[25] T. Sudhakar, V. Natarajan, M. Gopinath and J. Saranyadevi, "An enhanced authentication protocol for multi-server environment using password and smart card," *Wireless Personal Communications*, vol. 115, no. 4, pp. 2779-2803, 2020.

[26] K. Wu, R. Cheng, W. Cui and W. Li, "A lightweight SM2-based security authentication scheme for smart grids," *Alexandria Engineering Journal*, vol. 60, no. 1, pp. 435-446, 2021.

[27] P. G. Chilveri and M. S. Nagmode, "A novel node authentication protocol connected with ECC for heterogeneous network," *Wireless Networks*, vol. 26, no. 7, pp. 4999-5012, 2020.

Authors' Profiles

Jolin J.S. is a student in Computer Science and Engineering at Karunya Institute of Technology and Sciences, Coimbatore, Tamil Nadu. His research interests include Data Management also on Mobile Networking, Green Mobile Communication, Mobile-Social Networks.

A. Theophilus is a student in Computer Science and Engineering at Karunya Institute of Technology and Sciences, Coimbatore, Tamil Nadu. His research interest includes Soft Computing, Software Engineering, Mobile Network Modeling and also Evaluation, Mobile-Edge Computing.

Dr. A. Kathirvel is an Assistant professor, Computer Science and Engineering, Karunya Institute of Technology and Sciences, Coimbatore, Tamil Nadu. His research interests are in the field of Information Security, Big Data Analytics, Machine Learning Algorithms.

How to cite this paper: J.S. Jolin, A. Theophilus, A. Kathirvel, "Two-factor Mutual Authentication with Fingerprint and MAC Address Validation", International Journal of Computer Network and Information Security(IJCNIS), Vol.16, No.6, pp.56-68, 2024. DOI:10.5815/ijcnis.2024.06.05