International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Fast Authentication and Secure Handover for Wireless Mesh Network

Vanlalhruaia[1], Ajoy Kumar Khan[2], Amit Kumar Roy[3]

Submitted: 27/01/2024 **Revised**: 05/03/2024 **Accepted**: 13/03/2024

Abstract: Wireless Mesh Networks (WMNs) have become the preferred choice for service providers due to their cost-effectiveness and ability to provide extensive network coverage. However, ensuring secure and seamless handoffs in such networks poses a significant challenge due to client mobility and the inherently open nature of the medium. Additionally, the resource constraints of client devices necessitate lightweight computation and communication during both handoff authentication and login authentication phases, which are the focal points of this study. To address these challenges, this work proposes a authentication scheme tailored for WMNs. The scheme revolves around the use of dynamically generated tickets and encrypted session data to facilitate secure communication within the network. These tickets ensure that only authorized nodes can initiate connections, the proposed scheme is the integration of cryptographic techniques, including symmetric and asymmetric encryption. These techniques bolster the security of the authentication process, providing resilience against various security threats . By leveraging these cryptographic mechanisms, the scheme ensures the authenticity of network entities. The proposed authentication scheme addresses the challenges of secure handoffs and lightweight authentication in WMNs. Through the use of dynamically generated tickets and cryptographic techniques, it provides a secure and efficient solution for authentication. Our proposal is effective in terms of the overhead associated with authentication, according to the performance and security analyses.

Keywords: *Wireless Mesh networks, authentication, handover, ticket*

1. Introduction

In order to offer improved network access services, an increasing number of wireless network topologies have been developed. This is a result of the rapid development of mobile technology and the pervasiveness of its use in daily life. A fundamental wireless mesh network (WMN) technology has recently emerged as various wireless networks upgrade to the next generation to offer improved services. WMNs are made up of a gateway router (GR), a number of mesh routers (MRs), and a number of mesh clients (MCs). MRs have powerful resources, while MCs have constrained resources but excellent mobility [23].WMNs are designed to give mobile users wireless connectivity and have a number of unique characteristics that set them apart from traditional wireless networks[1]

•Multi-hop wireless network: One objective of the development of WMNs is to increase the wireless network coverage without reducing channel bandwidth. Another goal is to give customers who lack direct line-of-sight (LOS) links non-line-of-sight (NLOS) connectivity. To accomplish these objectives, mesh-style multi-hopping is essential [8], which achieves higher throughput without sacrificing effective radio range via shorter link distances, less interference between the nodes, and more efficient frequency re-use.

•Multiple types of network access: Peer-to-peer (P2P) communications and backhaul Internet access are both enabled by WMNs [6]. Moreover, WMNs can be used to integrate other wireless networks that offer services to these networks' end users with WMNs.

• Support for ad hoc networking and self-forming, self-healing, and self-organizing properties. WMNs enhance network performance because to their adaptable network architecture, straightforward deployment and configuration, fault tolerance, and mesh connectivity (multipoint-to-multipoint communications). Mobility is influenced by the mesh component type. While mesh clients can be either stationary or mobile nodes, mesh routers typically have limited mobility.

• Constraints on power usage depend on the kind of mesh nodes. Mesh routers typically do not have stringent power consumption restrictions. However, power-efficient methods might be needed for mesh clients. For instance, a sensor with mesh capabilities needs its transmission protocols to be power-efficient [12][13].

• Interoperability and compatibility with current cellular networks. For instance, WMNs built based on IEEE 802.11 technologies must be compatible with IEEE 802.11 standards in the sense of supporting both mesh capable and conventional Wi-Fi clients. Additionally, such WMNs must be able to communicate with other wireless networks

[1] *Department Of Computer Engineering, Mizoram University,Mizoram India*
ORCID ID : 0009-0001-7871-7832
[2] *Department Of Computer Engineering, Mizoram University,Mizoram India*
ORCID ID : 0000-0002-0493-6020
[3] *Indian Institute of Information Technology Kottayam, Kerala,India*
ORCID ID : 0000-0003-1568-7872
**Corresponding Author Email : hruai_a56@yahoo.com*

like WiMAX, Zig-Bee, and cellphone networks.

The self-organization, self-healing, self-configuration, quick deployment, simple maintenance, and cost effectiveness of WMNs are all appealing benefits. Nearly all of the traits of more generic wireless ad hoc networks are inherited by WMNs (e.g., decentralized design, distributed communications). Mesh routers, however, are typically fixed, in contrast to the movement of ad hoc nodes. Ad hoc networks frequently have energy constraints, so energy economy is a key design goal. Mesh routers, on the other hand, have no restrictions on how much electricity they can use[11].

1.1. Wireless Mesh Network Architecture

Mesh clients (MCs), mesh routers (MRs), mesh gateways (MGs), and a collection of wireless links are the main components of a WMN. An MC can be thought of as a user device and is typically the endpoint of a network data flow. The MRs create a wireless backbone that the MCs are linked to. The MGs serve as the points of connection between a WMN and a wired network, usually the Internet. As a result, a network request coming from an MC would be sent to the wireless backbone through the MR it is connected to, where there are one or more steps before MG is reached and then the Internet (and vice versa) [7].

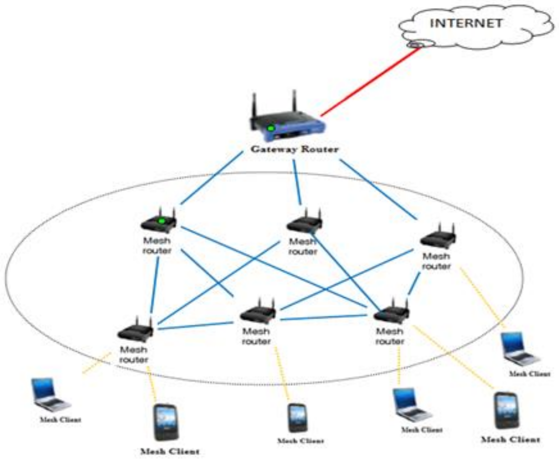

Fig 1: Architecture of Wireless Mesh Network

1.2. Application of Wireless Mesh Network

A safe wireless campus network based on the WMN in coordination with Wi-Fi cameras, sensors, and other security devices. In less time and at lower cost, it enables schools to install security cameras anywhere within the school district. They can even achieve full campus coverage for fast response to a variety of emergencies. Online course materials that teachers submit allow for live teaching and online course storage. Students can select a teacher's lesson based on their preferences and replay it at different times. With increased development, the wireless mesh network is now a more flexible and practical choice for network applications on campuses [27].

1.3. Security Requirements

When deploying and managing WMNs, security is always an important stage. Over wireless LANs, virtual private networking (VPN) is feasible. To provide secure virtual paths along shared networks, it is typically done with common key encryption tunneling algorithms like IPSec [25]. The target MR and the roaming MC are each persuaded of the other's legitimacy, i.e., they are all approved by the authentication server (AS) by direct message exchange or via ticket. The process that does not require AS would decrease latency as the AS may be several hop away. Based on the aforementioned authentication, the AS grants the MC permission to join to the network. The secret is shared by the MC, the designated MR, and the AS. Data sent over the network cannot be altered, replayed, or intentionally delayed. It is impossible to obtain the substance of communications by listening in[24] Wireless network authentication protocol designs must take into account the following factors[26]

Privacy and security: A strong authentication protocol should be able to withstand various security intrusions. The majority of users hope that their service provider will safeguard their privacy in addition to providing access to the internet (such as their identities and locations).if the MC authenticates with many MRs in the network using the same identity, anyone can track its travel paths. As a result, it's crucial to offer a strong handover authentication mechanism with user anonymity and intractability (to stop authenticated users' privacy from being compromised).

Efficiency: Either MCs or MRs typically have limited power and processing capabilities, it is crucial to focus on authentication protocol's efficiency. Hence, an effective authentication scheme should be efficient (in terms of communication and computation complexity).

2. Related Work

Numerous methods have been put forth in the literature to ensure the security of ticket base authentication in WMN. Here, we only briefly discuss those that are most important to our work.

Davoli and Ferrari [3] discussed in the book, the choosing of the low-layer communication protocol that forms the WMN's foundation is critical. IEEE 802.11 and Bluetooth Low Energy (BLE) appear to be prime candidates to utilize WMNs, yet requiring a careful analysis of the constraints relevant for each network protocol and the definition and adoption of proper routing protocols to be able to forward the data from source to destination. The structure and characteristics of WLAN mesh networks were introduced by Jiang et al. [5] who also examined prevalent security threats and security needs. A novel authentication protocol for WLAN mesh networks is introduced after a study of the security authentication protocol used by router nodes in WLAN mesh networks. To show the effectiveness of design, which enables secure access to WLAN mesh networks and safeguards data privacy, they built a scalable (redesigned to allow quick transactions) and lightweight blockchain in comparison to the traditional block chain network. Reddy et al. [16] investigated on network layer assault simulation in wireless mesh networks. They researched different network layer assaults, and determined how these attacks interacted with one another as a result. To leverage these attacks, they employ the AODV protocol. The outcomes of simulations demonstrate that each attack's intensity in relation to good put and packet delivery ratio (PDR). Based on malevolent node behavior, their interdependencies were discovered. In order to gauge the severity of the attacks, they also included these attacks in the AODV routing algorithm. This models show that wormhole attacks are the most harmful of all attacks, while grayhole attacks are the least harmful. Rathee and Saini [14] proposed Elliptic Curve Cryptography (ECC) technique for authentication in WMN. Over WMN, a Diffie-Hellman elliptic curve method is used to cut down on delay and computational overhead problems. The performance of the suggested work is evaluated theoretically and experimentally over the (Network Simulator 2) NS2 simulator in order to further demonstrate its validity. A safe authentication verification method using an elliptic curve cryptographic algorithm is built over WMN, accelerating the authentication process and reducing key management overheads.. Assegie and Nair [2] studied the Gauss-Markov's mobility model's effectiveness in a simulated software-defined wireless mesh network. The outcome of the experiment demonstrated that the network efficiency is significantly influenced by the Gauss-Makov's mobility model. The mobility model developed by Gauss Makov was also used to investigate how nodes move in virtual simulation environments.

The resource allocation of heterogeneous networks and the satisfaction of user networks were solved by Shang et al. [20] using the admission control approach. Completely distribute the diverse network resources in a sensible manner. A WMN admission control algorithm based on matching game theory was suggested for the issue of user and network admission control. Based on both user and network satisfaction, the algorithm uses a compromised network admission scheme. In order to provide secure communication, the multi-party key exchange protocol protects the confidentiality of the information transmitted during the handover authentication process (HAP) and login authentication process (LAP). Roy et al. [19]introduced multi-party key exchange protocol for WMN. The experimental findings demonstrate that, in terms of computation cost and communication cost, the suggested protocol achieves the shortest authentication delay when compared to existing protocols. According to security analysis, the proposed protocol provides a greater level of security during the login authentication process (LAP) and handover authentication process (HAP), where no outsiders can tamper with the shared information. For intra- and inter-domain handoff, Sharma and Surender [21] suggested an ID-based signcryption authentication algorithm. A proxy-based hierarchical network has been taken into account in this approach. A caching-list-based pre-fetching method has been used to decrease the handoff latency. The identity-based proxy group signature [4] and ticket-based handoff authentication protocol by Xu et al. [24] have been contrasted with the suggested ID-based signcryption authentication algorithm (ISAA). By creating tickets for the mesh clients that are divided into various zones of mesh routers based on their communication range, Rathee and Saini [15] suggested a secure handoff process. In order for mesh clients to authenticate themselves with the new mesh router by verifying their generated tickets, an authentication server is in charge of creating and updating the associated tickets for each mesh client. The security risks presented by client mobility in mesh environments as well as storage overhead have been substantially addressed by the suggested technique. Based on the extensible authentication protocol (EAP) mechanism, Rekik et al. [17] suggested authentication and re-authentication schemes are optimized and secure. A security evaluation using the AVISPA tool and a QoS evaluation using the OPENSSL utility are both used for validation. The results of AVISPA show that the proposed protocol is safe and the solution greatly reduces authentication and re-authentication latency, according to the performance evaluation.

The resource allocation of heterogeneous networks and the satisfaction of user networks were solved by Shang et al. [20] using the admission control approach. Completely distribute the diverse network resources in a sensible manner. A WMN admission control algorithm based on matching game theory was suggested for the issue of user and network admission control. Based on both user and network satisfaction, the algorithm uses a compromised network admission scheme. In order to provide secure communication, the multi-party key exchange protocol protects the confidentiality of the information transmitted during the handover authentication process (HAP) and login authentication process (LAP). Roy et al. [19]introduced multi-party key exchange protocol for WMN. The experimental findings demonstrate that, in terms of computation cost and communication cost, the suggested protocol achieves the shortest authentication delay when compared to existing protocols. According to security analysis, the proposed protocol provides a greater level of security during the login authentication process

(LAP) and handover authentication process (HAP), where no outsiders can tamper with the shared information. For intra- and inter-domain handoff, Sharma and Surender [21] suggested an ID-based signcryption authentication algorithm. A proxy-based hierarchical network has been taken into account in this approach. A caching-list-based pre-fetching method has been used to decrease the handoff latency. The identity-based proxy group signature [4] and ticket-based handoff authentication protocol by Xu et al. [24] have been contrasted with the suggested ID-based signcryption authentication algorithm (ISAA). By creating tickets for the mesh clients that are divided into various zones of mesh routers based on their communication range, Rathee and Saini [15] suggested a secure handoff process. In order for mesh clients to authenticate themselves with the new mesh router by verifying their generated tickets, an authentication server is in charge of creating and updating the associated tickets for each mesh client. The security risks presented by client mobility in mesh environments as well as storage overhead have been substantially addressed by the suggested technique. Based on the extensible authentication protocol (EAP) mechanism, Rekik et al. [17] suggested authentication and re-authentication schemes are optimized and secure. A security evaluation using the AVISPA tool and a QoS evaluation using the OPENSSL utility are both used for validation. The results of AVISPA show that the proposed protocol is safe and the solution greatly reduces authentication and re-authentication latency, according to the performance evaluation.

To reliably identify and stop wormhole attacks, Vo et al. [22] suggested a novel multi-level authentication model and protocol (MLAMAN). All intermediate nodes are given the ability by MLAMAN to authenticate control packets hop-by-hop and at three different levels: (1) the packet level, where the integrity of the packet can be checked; (2) the node membership level, where the membership of a public key holder can be confirmed; and (3) the neighbourhood level, where the neighbourhood relationship between nodes can be established. According to the simulation findings, the MLAMAN was extremely resistant to wormhole attacks. It was completely effective in identifying wormhole attacks for a static network topology. With a minimal tunnel length of 1 hop and a maximum node moving speed of 30 m/s for a dynamic and mobile topology, it successfully detects wormholes more than 98.92% of the time in both hidden and participation modes.

A conditional privacy-preserving authentication and key agreement scheme based on elliptic curves was suggested by Zhou et al. [28] in light of the security requirements of roaming service in vehicular ad hoc networks (VANETs). Using the pre-shared password, the vehicle and the local service agent can mutually authenticate, and after that, the vehicle and the foreign service agent can securely create a session key.

Li et al [10],Lai et.al [9],AK Roy and AK Khan[18] are closely related protocols where li et al [10] is analyzed and improved by [9] and [18], Lai et.al [9] achieve very high level of security with high computational and communication cost whereas AK Roy and AK Khan [18] achieve fast handover with low cost that security flow in terms of forward-backward security and user traceability.

According to the security analysis, our proposed approach satisfies the security requirements of mutual authentication, roaming user anonymity, intractability in terms of security privacy, and the capacity to thwart assaults such forgery attacks and replay attacks.

3. Proposed Protocol

We proposed an authentication methodology based on tickets issued by Ticketing Agents (TA), who would be a trusted third party, in order to strike a healthy balance between security and efficiency.

3.1 Trust Model : In the trust model, the TA is a central authority who issue the ticket for MRs and MCs, but the transfer ticket is issue by the Home Mesh Router(HMR). The trust relationship is as shown in Figure: 2.

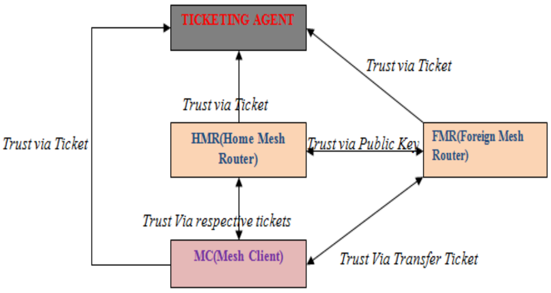

Fig 2: Trust relationship among entities

- TA-HMR: Trust between TA and HMR is via Ticket issued by TA, the ticket is signed by the TA which is verified by HMR.
- TA-MC: Trust between TA and MC is via Client ticket issue by TA that can be verified by the Client.
- HMR-MC: Mutual trust between MC and HMR is via their respective ticket issued by TA
- HMR-FMR(Foreign Mesh Router): The two neighbouring MRs trust each other by public key Crypto system.
- MC-FMR: MC and FRM trust each other by transfer ticket issued by HMR.

3.2 Different Types of Tickets: There are three types of tickets employ in the proposed protocol

Client Ticket*(Tc)***:** The MC ticket is issued by *TA* and the MC submit this ticket to HMR to prove it is a legitimate user of the network

$T_c = \{ I_c, I_A, P_c, \varsigma_{exp}, Sig_A\}$

Where

I_C : Identity of MC who is having the Ticket issued by TA

I_A: Identity of the TA who issued the Ticket.

P_c: Public Key of the Client who is having the Ticket.

ς_{exp}: Expiry time of the ticket.

Sig_A: Signature of the TA who is issuing the ticket.

Mesh Router Ticket*(T_M):* MR ticket issue by TA upon request by any MR

$T_M = \{ I_M, I_A, P_M, \varsigma_{exp}, Sig_A\}$

Where

I_M : Identity of MR who is having the Ticket issued by TA

I_A: Identity of the TA who issued the Ticket.

P_M: Public Key of MR who is having the Ticket.

ς_{exp}: Expiry time of the ticket.

Sig_A: Signature of the TA who is issuing the ticket.

Transfer Ticket *(Θ_c)* : A transfer ticket issue by MR

$\Theta_c = \{I_{CR}, I_M, I_A, \varsigma_{exp}, V_{KMAC}(I_{CR}, I_M, I_A, \varsigma_{exp})\}$

Where

I_{CR} : Anonymous Identity of MC who is having the Ticket issued by HMR.

I_M : Identity of MR who is Issue ticket to MC.

I_A: Identity of the TA.

ς_{exp}: Expiry time of the ticket.

3.3 Login Authentication Protocol: Assuming that the MR had a ticket from TA and the MC also received its ticket from the TA. Each MR periodically broadcast its ID in its coverage area to declare that it is ready to accept an incoming connection.

1. A Mesh Client C moves into the coverage area of HMR received the ID, It submit Its ticket T_C along with a nonce N_C. HMR check the expiry, If not expired it verify the signature Sig_A present in the ticket.

2. Upon successful verification, MR generate a nonce N_M and calculate $K_{MAC}=N_C||N_M$, Encrypt Its own ticket T_M along with nonce N_M and $V_{KMAC}(N_C)$ with the public Key of the client present in the ticket received from the client ticket.

3.Upon receiving the encrypted message C decrypt with its private Key. The expiry time and Sig_A is verified. If the verification is successful, C calculate $K_{MAC}=N_C||N_M$ and verify $V_{KMAC}(N_C)$. If the verification is successful, It send back $V_{KMAC}(N_M)$ to proved that it successfully calculate K_{MAC}.

4. When the HMR received $V_{KMAC}(N_M)$, it calculate $V_{KMAC}(N_M)$ from the K_{MAC} that is already generated , it compare $V_{KMAC}(N_M)$ it calculate and the one it received, If they are match it authenticate the MC. Note that from this point K_{MAC} is used as a session key and the session is encrypted with session key. The HMR generate transfer ticket Θ_c and send it to a client. The identity of MC in transfer ticket is as $I_{CR}= H(I_C||N_M)$ to protect client identity while roaming to FMR. Also $\{\Theta_c, K_{MAC}\}$ is send to each one hop neighbor by HMR encrypted with their own public key.

3.4 Handover Authentication Protocol: Proposed Handover Authentication Protocol(HAP) is an enhancement of Lai et.al.[9], It works base on the Elliptic curve Deffiehellman Key Exchange protocol(ECDKE) with precomputation of some information without necessity of the prior knowledge of the next FMR to visit, the precomputation facilitate fast handover authentication with little storage overhead.

In order to employ ECDKE for fast handover, It is assumed that the elliptic curve domain parameters is known to MC and FMR. The domain parameters (a,b,p,G,n) are

a,b : coefficient of the elliptic curve

p : size of the finite field(prime)

G: base point of the elliptic curve

n: order of the elliptic curve

When a MC received handover ticket from HMR it perform the following action:

(1) It generate private Key N_{CH} such that $1< N_{CH}< n$

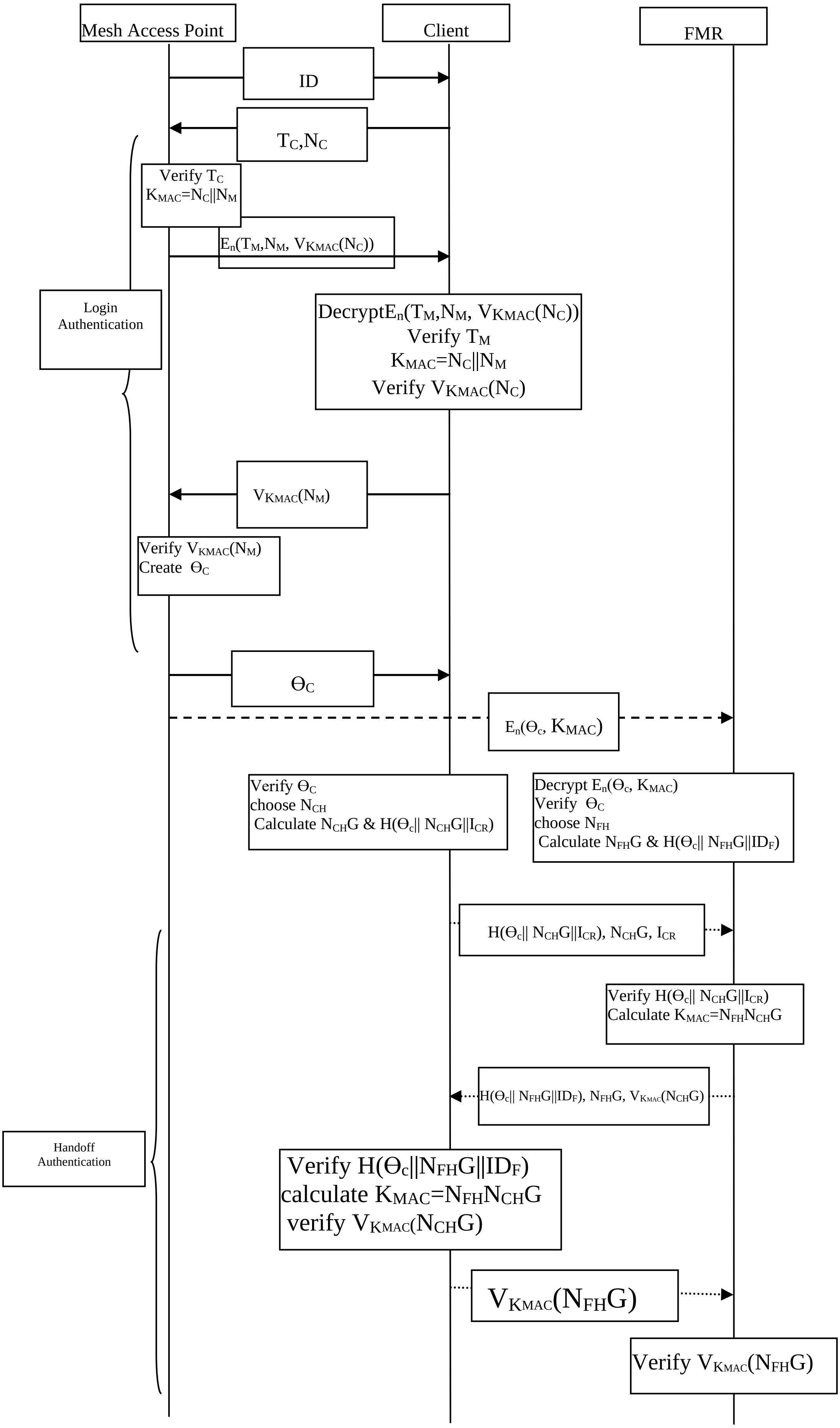
Mesh Access Point
Client
FMR
ID
T_C,N_C
Verify T_C
$K_{MAC}=N_C||N_M$
$E_n(T_M,N_M, V_{KMAC}(N_C))$
Login Authentication
Decrypt$E_n(T_M,N_M, V_{KMAC}(N_C))$
Verify T_M
$K_{MAC}=N_C||N_M$
Verify $V_{KMAC}(N_C)$
$V_{KMAC}(N_M)$
Verify $V_{KMAC}(N_M)$
Create Θ_C
Θ_C
$E_n(\Theta_c, K_{MAC})$
Verify Θ_C
choose N_{CH}
Calculate $N_{CH}G$ & $H(\Theta_c|| N_{CH}G||I_{CR})$
Decrypt $E_n(\Theta_c, K_{MAC})$
Verify Θ_C
choose N_{FH}
Calculate $N_{FH}G$ & $H(\Theta_c|| N_{FH}G||ID_F)$
$H(\Theta_c|| N_{CH}G||I_{CR}), N_{CH}G, I_{CR}$
Verify $H(\Theta_c|| N_{CH}G||I_{CR})$
Calculate $K_{MAC}=N_{FH}N_{CH}G$
$H(\Theta_c|| N_{FH}G||ID_F), N_{FH}G, V_{KMAC}(N_{CH}G)$
Handoff Authentication
Verify $H(\Theta_c||N_{FH}G||ID_F)$
calculate $K_{MAC}=N_{FH}N_{CH}G$
verify $V_{KMAC}(N_{CH}G)$
$V_{KMAC}(N_{FH}G)$
Verify $V_{KMAC}(N_{FH}G)$

Figure 3: Login and Handover Authentication

(2)Calculate $N_{CH}G$

(3) Calculate H(Θ_c|| $N_{CH}G$||I_{CR})

keep it ready for fast handover, Similarly each MRs in the neighborhood of HMR perform the following :

(1) It generate private Key N_{FH} such that 1< N_{FH}< n

(2)Calculate $N_{FH}G$

(3) Calculate H(Θ_c|| $N_{FH}G$||ID_F) (ID_F is identity of FMR)

keep it ready for fast handover.

When a MC enter the area of FMR where it find better signal strength with the ID_F broadcast by FMR. Then the handover authentication protocol is carried out as follows:

1. The roaming Mesh client submit {H(Θ_c|| $N_{CH}G$||I_{CR}), $N_{CH}G$, I_{CR}}(note that H(Θ_c|| $N_{CH}G$||I_{CR}) is precalculated) to FMR, Upon receiving {H(Θ_c|| $N_{CH}G$||I_{CR}), $N_{CH}G$, I_{CR}} from Client, FMR identify corresponding ticket from its database using I_{CR} and if not expired, It verify the validity of the received message from Θ_c received from HMR and $N_{CH}G$, I_{CR} received from MC. If valid, It calculate new K_{MAC} value as K_{MAC}=$N_{FH}N_{CH}G$, then it send back {H(Θ_c|| $N_{FH}G$||ID_F), $N_{FH}G$, V_{KMAC}($N_{CH}G$)} to MC.

2.When the MC received {H(Θ_c||$N_{FH}G$||ID_F), $N_{FH}G$, V_{KMAC}($N_{CH}G$)}(note that H(Θ_c||$N_{FH}G$||ID_F) is precalculated), It verify H(Θ_c||$N_{FH}G$||ID_F), if valid it calculate K_{MAC}=$N_{FH}N_{CH}G$ and verify

V_{KMAC}($N_{CH}G$), if the verification is successful the MC authenticate FMR and send back V_{KMAC}($N_{FH}G$).

3. When the FMR received V_{KMAC}($N_{FH}G$) and verified, It authenticate the MC.

4. Security Analysis:

In this section we analyzed common security threats

(1) Mutual authentication: Mutual authentication means both the communicating parties verifies each other for legality to access the network. In the proposed protocol both parties exchange their ticket, the signature of TA present in the ticket provide legality information of both parties. Mesh Access point Encrypt Its ticket with public Key of the client, Only the client can decrypt and extract a nonce N_M. Even though N_C is transfer in the plain text, an attacker do not have the knowledge of N_M it cannot calculate K_{MAC} , if K_{MAC} cannot be calculated the correct

value of $V_{KMAC}(N_M)$ cannot be calculated.

Also K_{MAC} is send to FMR in encrypted form ,only Client and FMR can generate valid V_{KMAC} so that mutual authentication can be achieved in handoff authentication.

(2)Reply Attack: An attacker listening communication channel may reply these messages later to gain access the network or to make the client to believed him/her a valid Mesh Access point. An encryption of random nonce N_M protect reply attack. Without the knowledge of N_M valid K_{MAC} cannot be generated during login authentication.

In handoff authentication K_{MAC} and transfer ticket is encrypted to FMR, It is impossible for adversary to generate valid digest of the ticket.

(3) Forgery Attack: In login Authentication the ticket and signature of TA ensure that the tickets are not modified. In handover authentication any modification will be easily detected by either parties because they have exactly same transfer ticket and K_{MAC}.

(4) Privacy: Privacy of the client is protected while

Table 1: Performance Comparison

		Ours		Lai et al[9].		Roy et al[18].	
operation	Time(ms)	Login	Handover	Login	Handover	Login	Handover
T_E(RSA-1024)	1.420	1	0	2	0	2	0
T_D(RSA-1024)	33.30	1	0	2	0	2	0
T_{Sig}(RSA-1024)	33.30	0	0	0	0	0	0
T_{Ver}(RSA-1024)	1.420	2	0	2	0	2	0
T_{MAC}(HMAC)	0.015	5	4	0	5	6	4
T_H(SHA-1)	0.009	1	2	6	3	0	0
T_{PMUL}(ECC-128)	~0.376	0	2	0	2	0	0
Number of Transmission		4	3	6	3	6	2
Authentication latency		37.644+4d	0.83+3d	72.334+6d	0.854+3d	72.37+6d	0.06+2d

roaming. The real identity is used only in the initial login authentication subsequent Mess Access Points do not have the knowledge of the real identity of the client.

(5) Forward backward security: The proposed protocol achieved forward backward security by creating new session key each time handover take place, the Mesh Client and FMR generate new Nonce, these new Nonces are combine with the base point in an elliptic curve before exchanging between them. It is protected by elliptic curve discrete logarithm problem.

5. Performance Analysis:

The performance is analyzed based on the number of cryptographic operation involved and message exchange during login and handover authentication, for this we refer the comparison table from [9] and [18] even though they applied different algorithms for some operation like Signature verification(RSA-1024 and ECDSA respectively), Hash(SHA-1 and SHA-2 respectively) etc. Both of them have same amount of computational time for same algorithm(RSA encryption and decryption)Table 1. shows the comparison of proposed protocol with the similar existing protocol, the proposed protocol perform better in login authentication latency this is because the number of message exchange and cryptographic operation is reduced without lowering security threat. In handover authentication, proposed protocol it is slightly better than [9] due to the pre computation of point multiplication on Elliptic curve, [18] protocol have low latency during handover but it suffer from security threat like forgery attack on transfer ticket, absence of forward backward security.

6. Conclusion

The rapid login authentication algorithm for wireless mesh networks we offer in this study reduces the computational and communication overhead, making it more practical for a device with constrained resources. The proposed protocol conforms with the required authentication security criteria. The proposed handover authentication mechanism has somewhat lower computational latency than [9] and has higher security than [18] Analysis and performance comparison show that the proposed protocol perform better compare to the similar existing protocol. Further Research could focus on developing advanced ticket management protocols that minimize latency and overhead while ensuring robust security. These protocols could incorporate techniques such as efficient ticket distribution, dynamic ticket lifetimes, and optimized ticket revocation mechanisms. The integration of ticket-based authentication with emerging technologies such as blockchain and distributed ledger technology (DLT) could offer tamper-resistant ticket issuance and validation mechanisms, enhancing the overall security and transparency of the authentication process. By exploring these future research directions, scholars and practitioners can advance the state-of-the-art in ticket-based authentication for wireless mesh networks, paving the way for more secure, efficient, and resilient network infrastructures in the future.

References

[1] I.F. Akyildiz, X. Wang and W. Wang “Wireless mesh networks: a survey" *Computer networks*,Vol.47,No.4,pp.445-487, March, 2005.

[2] Assegie, T. Admassu, and Pr. Sekharan Nair. "The performance of Gauss Markov’s mobility model in emulated software defined wireless mesh network." *Indonesian Journal of Electrical Engineering and Computer Science*, Vol. 18, No. 1, pp. 428-433, April 2020.

[3] L. Davoli and G.Ferrari. “Wireless Mesh Networks for IoT and Smart Cities: Technologies and Applications”. *The Institution of Engineering and Technology, pp. 1-289,2022.*

[4] T. Gao, F. Peng and N Guo "Anonymous authentication scheme based on identity-based proxy group signature for wireless mesh network." *EURASIP journal on wireless communications and networking*,Vol.2016,No.193,pp.1-10,August,2016.

[5] X. Jiang, M. Liu1, C. Yang , Y. Liu and R. Wang “A Blockchain-Based Authentication Protocol for WLAN Mesh Security Access" *Computers, Materials & Continua*, Vol.58, no.1, pp.45-59, 2019.

[6] J. Jun and M.L .Sichitiu ”The nominal capacity of wireless mesh networks” *IEEE wireless communications*, Vol.10,No.5,pp.8-14, Oct,2003.

[7] S. Karunaratne and H. Gacanin, "An Overview of Machine Learning Approaches in Wireless Mesh Networks" *IEEE Communications Magazine*, Vol. 57, no. 4, pp. 102-108, April 2019, doi: 10.1109/MCOM.2019.1800434.

[8] L. Krishnamurthy, S. Conner, M. Yarvis and J. Chhabra "Meeting the Demands of the Digital Home with High-Speed Multi-Hop Wireless Networks" *Intel Technology Journal*, Vol. 6, No. 4, November,2002.

[9] Y.M. Lai, P.J. Cheng, C.C. Lee and C.Y. Ku "A new ticket-based authentication mechanism for fast handover in mesh network" *PloS one* Vol.11,No.5,May, 2016.

[10] C. Li, U.T. Nguyen, H.L. Nguyen and N Huda “Efficient authentication for fast handover in wireless

mesh networks" *computers & security* Vol.37,pp.124-142,September,2013.

[11] F. Liu and Y. Bai "An overview of topology control mechanisms in multi-radio multi-channel wireless mesh networks" *EURASIP Journal on Wireless Communications and Networking*, Vol 2012, No.324,pp.1-12,October,2012.

[12] R.Poor "Wireless Mesh Networks: Providing industrial-strength connectivity, this technology delivers self-configuring, scalable, and self-healing networks. And it's aimed right at distributed data acquisition and control" *SENSORS-PETERBOROUGH*, Vol.20,No.2,pp.38-42,2003.

[13] R.Poor "Wireless mesh links everyday devices" *Electronic Engineering Times,* No.5, 2004.

[14] G.Rathee and H. Saini "Authentication Through Elliptic Curve Cryptography (ECC) Technique in WMN" *International Journal of Information Security and Privacy (IJISP),*Vol.12, No.1,pp. 42-52,January-March, 2018.

[15] G.Rathee and H. Saini "Secure handoff technique with reduced authentication delay in wireless mesh network" *International Journal of Advanced Intelligence Paradigms*, Vol.13,No.1-2,pp.130-150, May,2019.

[16] K.G. Reddy, M.S. Sudheer, P.K. Sree and VP Raju "Simulation analysis on network layer attacks in wireless mesh networks" *International Journal of Engineering & Technology*, Vol.7(3.29):pp.301–303, 2018.

[17] M. Rekik, A. Meddeb-Makhlouf, F. Zarai and P. Nicopolitidis " Oap-wmn: Optimised and secure authentication protocol for wireless mesh networks" *International Journal of Security and Networks*, Vol.14,No.4,pp.205–220, October,2019.

[18] A.K. Roy and A.K. Khan "Authentication protocol with privacy preservation for handover in wireless mesh networks." *In First International Conference on Sustainable Technologies for Computational Intelligence: Proceedings of ICTSCI 2019*, pp. 383-395. Springer Singapore, 2020.

[19] A.K. Roy, K. Nath, G. Srivastava, T.R. Gadekallu and J.C.W. Lin "Privacy preserving multi-party key exchange protocol for wireless mesh networks" *Sensors*. 2022 March 2;22(5):1958 https://doi.org/10.3390/s22051958.

[20] algorithm based on matching game and differentiated service in wireless mesh networks" *Neural Computing and Applications*, Vol.32, pp.2945-2962,2020.

[21] P.K. Sharma, R. Mahajan and Surender "Id-based signcryption authentication algorithm for intra-and interdomain handoff in wireless mesh networks" *Iranian Journal of Science and Technology, Transactions of Electrical Engineering*, Vol. 44, pp. 659–667, June,2020.

[22] T.T. Vo, N.T. Luong and D. Hoang "MLAMAN: a novel multi-level authentication model and protocol for preventing wormhole attack in mobile ad hoc network" *Wireless Networks* Vol.25 No. pp.4115-4132, May,2019.

[23] D. Wang, L. Xu, F. Wang and Q Xu "An anonymous batch handover authentication protocol for big flow wireless mesh networks" *EURASIP Journal on Wireless Communications and Networking*, Vol.2018,No.200,pp.1-8,December,2018.

[24] L. Xu, Y. He, X. Chen and X. Huang "Ticket-based handoff authentication for wireless mesh networks" *Computer networks* Vol.73, pp.185-194, November, 2014.

[25] H. Yang, H. Luo, F. Ye, S. Lu and L. Zhang, "Security in mobile ad hoc networks: challenges and solutions," in *IEEE Wireless Communications*, Vol.11, no.1, pp.38-47, February, 2004.

[26] X. Yang, Y. Zhang, J. K. Liu and Y. Zeng, "A Trust and Privacy Preserving Handover Authentication Protocol for Wireless Networks," *2016 IEEE Trustcom/BigDataSE/ISPA*, Tianjin,China,2016,pp.138-143,doi: 0.1109/TrustCom.2016.0056.

[27] Z. Yu, X. Xu and X. Wu, "Application of Wireless Mesh Network in campus network," *2010 Second International Conference on Communication Systems, Networks and Applications*, Hong Kong, 2010, pp.245-247, doi: 10.1109/ICCSNA.2010.5588704.

[28] Y. Zhou, X. Long, L. Chen and Z. Yang "Conditional privacy-preserving authentication and key agreement scheme for roaming services in VANETs." *Journal of Information Security and Applications*, Vol. 47, pp. 295-301,August. 2019.