IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier

SAP: A Secure Low-latency Protocol for Mitigating High Computation Overhead in WI-FI Networks

VINEETA JAIN[1], (Member, IEEE), ULF WETZKER[1], VIJAY LAXMI[2], MANOJ SINGH GAUR[2], (Member, IEEE), MOHAMED MOSBAH[3], and DOMINIQUE MERY[4]
[1]Fraunhofer Institute for Integrated Circuits, Division Engineering of Adaptive Systems EAS Dresden, Germany (e-mail: vineeta.jain@eas.iis.fraunhofer.de, ulf.wetzker@eas.iis.fraunhofer.de)
[2]Malaviya National Institute of Technology Jaipur, India (e-mail: vlaxmi@mnit.ac.in, gaurms@mnit.ac.in)
[3]LaBRI, CNRS, Bordeaux INP, University of Bordeaux, Talence, France (e-mail: mohamed.mosbah@labri.fr)
[4]LORIA & University of Lorraine, France (e-mail: dominique.mery@loria.fr)

Corresponding author: Vineeta Jain (e-mail: vineeta.jain@eas.iis.fraunhofer.de).

ABSTRACT The increase in popularity of wireless networks in industrial, embedded, medical and public sectors has made them an appealing attack surface for attackers who exploit the vulnerabilities in network protocols to launch attacks such as Evil Twin, Man-in-the-middle, sniffing, etc., which may result in economic and non-economic losses. To protect wireless networks against such attacks, IEEE 802.11 keep updating the protocol standards with new and more secure versions. There has always been a direct correlation between attacks and the improvement of protocol standards. As the sophistication of attacks increases, protocol standards tend to move towards higher security, resulting in a significant rise in both latency and computational overhead, and severe degradation in the performance of low-latency applications such as Industrial Internet of Things (IIoT), automotive, robotics, etc. In this paper, we make the first attempt to highlight the importance of both latency and security in wireless networks from implementation and performance perspective. We make a review of existing IEEE 802.11 protocols in terms of security offered and overhead incurred to substantiate the fact that there is a need of a protocol which in addition to providing optimum security against attacks also maintains the latency and overhead. We also propose a secure and low-latency protocol known as Secure Authentication Protocol (SAP) which operates in two phases - registration and authentication, where the first phase is a one time process implemented using asymmetric cryptography and the second phase is implemented using symmetric cryptography. The protocol is structured in a way that it maintains the original structure of IEEE 802.11 protocols and performs both phases using fewer messages than existing protocols. By simulating the protocol using well-established OMNeT++ simulator, we proved that the proposed protocol incurs a low computation overhead, making it ideal for low-latency applications. We extensively verified the security properties of the proposed protocol using formal verification through widely-accepted Scyther tool. Finally, we perform a comparative analysis of SAP with existing IEEE 802.11 wireless network protocols to highlight the improvement.

INDEX TERMS wireless network, security, low-latency, computation overhead, authentication, reauthentication

I. INTRODUCTION

Nowadays, wireless networks have become one of the ubiquitous and fastest means of accessing the Internet across the globe. According to the Cisco Visual Networking Index for $2017-2022$ [1], 51% of the global Internet Protocol (IP) traffic was predicted to be received from wireless networks by the end of 2022. This is mainly due to the ubiquity of wireless communication systems in the automotive, medical, military, IIoT and public sectors owing to the mobility and flexibility offered by the wireless networks. In medical technology, wireless networked devices, such as electronic medical records, physiological monitoring devices (wearables) or diagnostic equipment, are already being used in large numbers. In vehicles, the use of wireless communication is not limited to infotainment systems. Vehicular communication supports the driver via computer-assisted safety warnings and traffic information from external sources and inside the vehicle sensor information is transmitted wirelessly for condition monitoring. With the digitalization of the automation industry, the number of wirelessly networked devices has increased significantly. Rigid structures such as conveyor belts and overhead cranes are increasingly being replaced by intelligent, automated guided vehicle (AGVs). Augmented reality (AR) supports the worker in carrying out individual work steps by providing work and safety instructions via wirelessly connected data glasses. With the increase in data volume-dependent costs and international roaming charges on 4G networks, the popularity of public free Wi-Fi networks has increased for the use of data, voice and video services, resulting in deployment of Access Points (APs) in public places such as airports, railway stations, cafes/restaurants, etc. As per the Cisco Annual Report for 2018-2023 [2], IIoT devices will witness a 2.4 fold growth from 6.1 billion in 2018 to 14.7 billion in 2023 [2]. Most of the above applications have very high security and availability requirements [3] that must be met by the communication system.

With the increasing popularity of wireless networks, it is also becoming a prime target of attackers, posing a dangerous threat to the safety of users. Some of the contemporary attacks include eavesdropping where an attacker actively or passively sniffs the information transmitted between clients and AP and then uses brute forcing and cryptanalysis techniques to decrypt the encrypted information, Evil Twin (ET) attack where an attacker deploys a rogue AP mimicking the genuine characteristics (such as SSID, BSSID, passphrases, etc.) of legitimate AP in the network to fool clients to connect to the ET allowing him to hijack sessions, intercept network traffic, push malicious payloads etc., Man-in-the-middle (MITM) attack where an attacker authenticates itself to both client and AP as AP and client, respectively by sniffing and redirecting authentication messages to maliciously locate itself between AP and client so that all the traffic can flow through the attacker which can lead to information loss, malware installation, financial loss, remote control, etc., and replay attack where an attacker maliciously uses the previously transmitted authentication messages to gain unauthorized access to the network. Launching these attacks in medical, military or industrial environments for sniffing or tampering the transmitted information could have serious consequences, including economic espionage, operational failure, physical damage, environmental harm, and injury or loss of life.

To protect wireless networks from such attacks, IEEE 802.11 has launched several protocols. Wired Equivalent Privacy (WEP) is the first protocol launched by IEEE 802.11 in 1997, which uses password-based authentication where the password is a 40-bit static key already known to all the clients. Further, WEP applies Rivest Cipher 4 (RC4) stream cipher for encryption using 24-bit Initialization Vector (IV). Due to the unencrypted transmission of authentication messages, smaller key size and reuse of IVs [4], WEP is found vulnerable to MITM, ET and replay attacks [5].

To overcome the shortcomings of WEP, IEEE 802.11 launched WI-FI Protected Access (WPA) protocol in 2003. The aim was to fix the limitations of WEP without upgrading the hardware. WPA uses password-based authentication, where the password is a passphrase also known as pre-shared key (PSK). WPA applies Temporal Key Integrity Protocol (TKIP) for encryption which uses the RC4 algorithm and introduces the concept of 4-way handshake after the authentication and association phases. In the 4-way handshake, all types of keys used for encryption and transmission are generated using the PSK. Due to the use of RC4 for encryption and similar passphrase for all the clients, it is found vulnerable to offline dictionary attacks [6]. Once the attacker cracks the passphrase, launching MITM and ET attacks is a cakewalk.

Further in 2004, IEEE 802.11 introduced WPA2 protocol which is an improved version of WPA protocol. WPA2 uses Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) which utilizes Advanced Encryption Standard (AES) for encryption. In WPA2, both client and AP share a passphrase known as Pairwise Master Key (PMK), which is used to generate Pairwise Transient Key (PTK) for encrypting the user sessions. The usage of high-level encryption reduces the chance of cryptanalysis, but still the offline dictionary attack and ET attacks are possible [7].

In 2018, IEEE 802.11 has introduced WPA3 protocol. For public networks, WPA3 uses opportunistic wireless encryption (OWE) mode also known as enhanced open WI-FI network [8]. In this mode, there is no pre-shared information between AP and client. Both the entities exchange their pubic keys to generate a shared secret key, i.e., PMK using the Elliptic Curve Diffie-Hellman (ECDH) algorithm. The derived PMK is then utilized in the four-way handshake mechanism to generate session keys, i.e., PTK. For personal networks, WPA3 provides an extra layer of security (in addition to WPA2) in the form of simultaneous-authentication-of-equals (SAE) handshake (a variant of the dragonfly handshake mechanism) and this standard is called as WPA3-personal. During SAE handshake, the passphrase shared between client and AP is converted into a high entropy key (PMK). Further, this key is used to produce PTK during four-way handshake mechanism. The computational overhead of WPA3-personal is relatively very high given the complexity of the SAE handshake [9].

802.1X protocol is an IEEE Standard for Port-Based Network Access Control (PNAC) which uses unique certificates or credentials for every user to authenticate eliminating the reliability on single password for authentication. In addition to client and AP, 802.1X also requires a RADIUS[1] server and identity provider for authentication. The RADIUS server verifies the identity of a client by communicating with the identity provider (a directory containing user credentials/certificates information). Although 802.1X is the most secure protocol, the number of messages exchanged for authentication are way too high for use in wireless networks. The typically fluctuating transmission conditions of a WiFi network occasionally lead to situations in which a new connection setup is required. Under such conditions, long connection setup procedures inevitably lead to greatly increased latency in the network.

WPA3 protocol also introduces WPA3-enterprise for high-security Wi-Fi networks such as in government, defense and finance. It includes an additional 192-bit security while still using 802.1X as the base protocol. Further, it adds an additional requirement of certificates for RADIUS servers along with clients. While this has added significantly to the security of the connection, it complicates and lengthens the authentication procedure, makes it computationally more expensive, and is thus not suitable for low-latency wireless networks.

To comprehensively protect Wi-Fi networks against attacks, vulnerabilities in the IEEE 802.11 specification were addressed by new and improved security mechanisms. Although the IEEE protocols provide security against attacks, they result in increased communication and computation overhead, making the authentication process more time-consuming. For a number of low-latency applications, such as heath-care, intelligent transportation system, robotics, AR, etc., this is unacceptable as it would lead to significantly increased downtime during operation leading to unavailability. Due to increasing concerns about the latency and the associated reliability of the IEEE 802.11 standard, many sectors have started to replace their wireless networks with private cellular networks [10]. This leads to an increase in their overall cost as private networks require greater upfront investment. Moreover, for constrained devices such as embedded and IIoT devices, the high computation overhead of security processes further increases these latency issues. Therefore, a lightweight protocol is needed that provides optimal protection against current network attacks (such as ET, MITM, replay and sniffing attacks) while keeping latency and computation overhead as low as possible.

In this paper, we propose a secure low-latency protocol named Secure Authentication Protocol (SAP) which provides security against contemporary network attacks through a secure authentication and reauthentication mechanism. We define authentication as the first attempt of the client to get authenticated to an AP. Any subsequent authentication attempts between a client and an AP are defined as reauthentication. SAP employs Elliptic Curve Cryptography (ECC) for key distribution and authentication, and symmetric encryption for reauthentication and session establishment. Although the usage of ECC and symmetric encryption in security protocols is already established, the novelty lies in how and where they are deployed. SAP ensures that even with the use of cryptographic primitives, the protocol remains lightweight and consumes less number of messages yet provides optimum level of security required. SAP has the following advantages: (i) In the proposed protocol, key generation and distribution between client and AP is performed only once when they get associated for the first time. The process utilizes fewer messages than existing protocols and do not require any additional servers, pre-shared knowledge or large number of message exchanges making it suitable for low-latency applications and embedded systems, (ii) once the key distribution and mutual authentication occurs between client and AP, they securely cache the relevant connection information. For future sessions, the client and AP only undergo reauthentication using the cached information. This makes the process resource-saving, computationally efficient and fast, and (iii) the proposed protocol does not modify the original structure of 802.11 protocol stack. Thus, the deployment is easy on the user side.

In short, the paper makes the following contributions:

- In this paper, we highlight the importance of low-latency for the wireless network protocols and propose a protocol known as SAP, which in addition to providing security against contemporary network attacks also keeps the overhead and delay maintained. To the best of our knowledge, we are the first one to discuss the significance of both latency and security in wireless network context and propose a protocol with the motivation of mitigating high computation overheads in IEEE 802.11 protocols while maintaining the security.
- We propose to use both symmetric and asymmetric cryptography in the protocol in a way that it preserves the original structure of IEEE 802.11 protocols, guarantees mutual authentication and secure key distribution, and exchanges less number of messages incurring low computation overhead in session establishment between client and AP.
- We intensively tested our protocol using formal verification to test the security properties and simulation for network performance parameters. We also

---

[1] It stands for Remote Authentication Dial-In User Service

compared our proposed protocol with the previous IEEE 802.11 standard protocols to highlight the improvement obtained via the proposed protocol.

The organization of the paper is as follows: Section II discusses the various types of keys and network assumptions followed by the proposed protocol, and provides a detailed description of the protocol. Section III theoretically analyzes the proposed protocol in various aspects such as security analysis and mutual authentication between client and AP. Section IV evaluates the security aspects of the proposed protocol by formally verifying SAP using Scyther. Section V explains the practical demonstration of SAP using OMNeT++ simulator. Section VI compares SAP with the existing standard protocols. Section VII concludes the paper.

II. THE PROPOSED PROTOCOL

To address the issues present in the existing standard protocols, we propose Secure Authentication Protocol (SAP). SAP neither uses open nor password-based authentication. SAP employs Elliptic Curve Cryptography (ECC) to generate and exchange keys, and symmetric encryption scheme to encrypt transmitted messages. ECC is chosen because it has outperformed the existing key generation algorithms such as RSA, owing to its shorter key size and small computational overhead [11]. Short key size makes ECC faster and suitable for small and embedded devices. Further, SAP uses AES-CCMP (Advanced Encryption Standard Counter Mode with Cipher Block Chaining Message Authentication Protocol) [4] for symmetric encryption of the messages, as AES-CCMP provides a high level of security for encryption, used by all standard protocols (such as WPA2 and WPA3) and not been proved vulnerable to attacks [4]. By incorporating these cryptographic and encryption schemes, SAP assures mutual authentication, encrypted communication, secrecy against eavesdroppers and resistance to attacks.

A. PRELIMINARIES

In this subsection, we present a concise description of Elliptic Curves and ECC and discuss the various types of keys and network assumptions followed by the proposed protocol.

1) Elliptic Curves

The elliptic curve over a finite field is defined by

$$y^2 = \{x^3 + ax + b\}\text{mod}\{p\} \tag{1}$$

It has domain parameters (p, a, b, G, n, h) where,

- p = prime number specifying the size of finite field,
- a, b = curve parameters,
- G = Generator Point (generates a cyclic subgroup),
- n = ord(G) (size of subgroup),
- h=cofactor=$\frac{|E(Z/pZ)|}{n}$ (ideally 1), where E(Z/pZ) represents elliptic curve defined over Z (integers) modulo p.

Suppose an elliptic curve is defined over integer modulo p as E(Z/pZ) and $Q, P \in E(Z/pZ)$, where P and Q are points on the curve such that

$$P = kQ = Q + Q \ldots k \text{ times} \tag{2}$$

According to Elliptic Curve Discrete Logarithm Problem (ECDLP), the computation of P is simple when k and Q are known. However, given P and Q, the calculation of k is computationally challenging and expensive. This is the basis of ECC.

2) ECC

ECC encodes the message to a point on the curve specified by Eq. 1. The original message can be retrieved by decoding the point. For encoding and decoding the points, entities require key pairs. Suppose A and B have private keys as n_a and n_b respectively. The public keys of A and B are derived as:

$$P_a = n_a G \tag{3}$$

$$P_b = n_b G \tag{4}$$

When A wants to send a message m, he needs to perform two actions - (1) encode the message to a point T (ϕ_T) on the curve, and (2) create any random value u. The process of encoding a message m to a point ϕ_T is known as mapping, and the process of decoding ϕ_T to m is known as reverse mapping [12]. The mapping operations are performed by mapping function F such that

$$F(m) \rightarrow (x, y) \in E_p(a, b) \tag{5}$$

where m is the message and (x, y) are points on the curve $E_p(a, b)$ (as described in Eq. 1). Further, A encrypts the point ϕ_T using P_b and random variable u as:

$$Enc \rightarrow A : \{uG, \phi_T + uP_b\} \tag{6}$$

A sends this message to B. When B receives the message, he can decrypt the message by using uG and B's private key n_b.

$$Dec \rightarrow B : \phi_T + uP_b - n_b(uG) \tag{7}$$

Using Eq. 4, Eq. 7 can be rewritten as:

$$Dec \rightarrow B : \phi_T + u(n_b G) - n_b(uG) \tag{8}$$

By rearranging the term $u(n_b G)$, it can be rewritten as:

$$Dec \rightarrow B : \phi_T + n_b(uG) - n_b(uG) = \phi_T \tag{9}$$

B calculates $n_b(uG)$ to remove uP_b. Hence, no one other than B can decrypt ϕ_T. Further, B decodes ϕ_T using reverse mapping function to obtain the original message m. Thus, the attacker's attempt of obtaining the message m by eavesdropping the communication remains unsuccessful because they don't possess the private keys. The proposed protocol uses the same concept for encryption and decryption using ECC.

3) Keys used in SAP

The keys play a significant role in ensuring the security of the proposed protocol. The following keys are used in authentication and reauthentication phases of SAP:

- Public-Private Key Pair: AP produces a public-private key pair using ECC, and the public key of AP is known to everyone in the network.
- Encryption-Decryption Key Pair: Client produces encryption-decryption key pair using ECC. The functionality of encryption-decryption key pair is similar to public-private key pair in a way that the information encrypted by encryption key can only be decrypted by decryption key. But the difference is that unlike the public key, encryption key of client is not public in the network.
- Master Key (MK): MK is uniquely generated by AP for each client and exchanged only once between the client and AP during their first connection attempt. MK is cached by both the parties as MK is used as a reauthentication parameter for further connection attempts between the client and AP.
- Session Keys: They are freshly produced for each session between client and AP, and used for encrypting the communication between them.

4) Assumptions

Following are the assumptions in proposed SAP protocol:

- The AP has a valid public key certificate[2] issued by a trusted and verified Certification Authority (CA).
- The client is loaded with a list of trusted CA certificates.
- The key-pairs[3] for network entities are generated only once.
- The client and AP have sufficient storage and mechanism for MK Caching.
- The AP and client possess encoder/decoder to transpose an elliptic curve point into information.
- The protocol is public.
- The AP, attacker and client are in the same network.

The attacker possesses the following characteristics:

- The attacker can conduct active as well as passive attacks.
- The attacker has access to the public key of the AP and ECC domain parameters.
- Any authentic client in the network can be a target of the attacker.

B. PROTOCOL OVERVIEW

SAP operates in two phases - Registration and Authentication. The registration phase is a one-time process borne by AP and client during their first association, whereas the authentication phase is a continuous process between client and AP whenever a new session begins. Table 1 represents the notations used in the proposed protocol.

TABLE 1. Notations with their descriptions used by SAP

S.No.	Notation	Description
1.	C	Client
2.	AP	Access Point
3.	$\mathrm{n_c}$	Decryption key of client
4.	$\mathrm{P_c}$	Encryption key of client
5.	$\mathrm{n_{AP}}$	Private key of AP
6.	$\mathrm{P_{AP}}$	Public key of AP
7.	ϕ_T	Point T on the elliptic curve
8.	m	Message m
9.	$\mathrm{m'}$	Decrypted message m
10.	$\mathrm{P_{MK}}$	Master Key (MK)
11.	$\mathrm{K_{sk}}$	Seed key
12.	$\mathrm{K_{se}}$	Session key
13.	T	Timestamp

1) Registration Phase

The registration phase is a one-time process which occurs when the client tries to connect to an AP for the first time. It consists of the following steps:

1) Beacon Frame: The AP broadcasts beacon frames in the network embedded with its public key certificate issued by a legitimate and verified CA containing the ECC domain parameters and public key of the AP.
2) Probe Request: The client, on receiving the beacon frame, verifies the certificate of the AP. It checks whether it implicitly trusts the certificate or it is trusted and verified by one of various CAs that it also implicitly trusts. If the client detects any problem in the certificate, i.e., either expired or hostname is different or not issued by any verified CA, it rejects the beacon and begin searching for new APs in the network. Else, it extracts the ECC domain parameters from the certificate and using them, the client chooses a decryption key $\mathrm{n_c}$ and produces an encryption key $\mathrm{P_c}$ as:

$$\mathrm{P_c} = \mathrm{n_c G} \tag{10}$$

---

[2] Public key certificate, also known as a identity certificate or digital certificate, is an electronic document issued by a Certification Authority (CA) to prove the ownership of a public key. It contains name of the certificate holder, public key of the holder and the digital signature of a CA for authentication.

[3] Public-private key pair for AP and encryption-decryption key pair for clients

Further, the client sends a probe request to the AP consisting of P_c and current timestamp value T_c by encoding it to a point T (ϕ_T) and encrypts ϕ_T using P_{AP} (as explained in Section II-A2) extracted from the certificate, such that $\phi_T = P_c || T_c$. The timestamp is included to prevent replay attacks. The message also includes the hash of the message to maintain integrity.

$$C \rightarrow AP : m_0 = \{kG, \phi_T + kP_{AP}\}, h(m_0) \qquad (11)$$

3) Probe Response: The AP possess a public-private key pair as $\langle P_{AP}\text{-}n_{AP} \rangle$, where:

$$P_{AP} = n_{AP}G \qquad (12)$$

On receiving the message, AP decrypts it using n_{AP}. Let the decrypted message be represented as m'_0. AP matches T_c with the current timestamp. If T_c is verified, then it computes the hash of m'_0, and matches against $h(m_0)$. If $h(m'_0) = h(m_0)$, then it selects a point on the curve ϕ_J. Using ϕ_J and P_c, it produces a master key (MK) as:

$$MK = \text{SHA-256}(\phi_J || P_c) \qquad (13)$$

AP encrypts the MK using P_c and sends it to the client by encrypting it to the point S such that $\phi_S = P_{MK} || T_{MK}$, where T_{MK} represents the current timestamp.

$$AP \rightarrow C : m_1 = \{uG, \phi_S + uP_c\}, h(m_1) \qquad (14)$$

This method of key exchange is known as Elliptic Curve Diffie-Hellman (ECDH) algorithm.

4) On receiving the message, the client decrypts it using n_c. Initially, it verifies T_{MK} and $h(m_1)$ to detect the legitimacy of the message. Further, it computes MKID (Master Key Identifier) as:

$$MKID = \text{trucate}_{64}\{h(P_c || P_{AP})\} \qquad (15)$$

The client caches MK and MKID. Similarly, the AP also calculates MKID and caches MK and MKID. IEEE 802.11 implements“Pairwise Master Key (PMK) caching" for WPA where a client and AP can cache a PMK for a certain period and reuse it during the 4-way handshake occurring at the time of reassociation to bypass potentially expensive authentication. We have implemented the concept of caching to bypass the process of registration during reauthentication. For further connections, the client directly sends the authentication request encrypted with MK to the AP. Figure 1 shows the steps involved in registration phase.

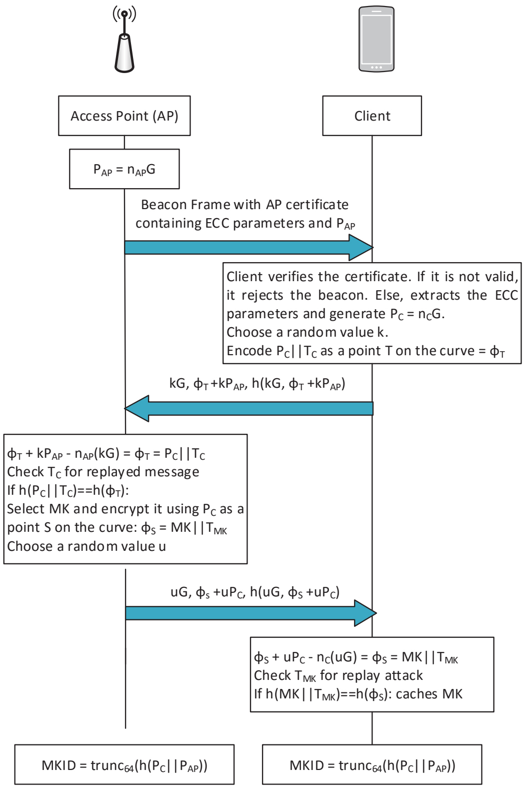

Access Point (AP)
Client
$P_{AP} = n_{AP}G$
Beacon Frame with AP certificate containing ECC parameters and P_{AP}
Client verifies the certificate. If it is not valid, it rejects the beacon. Else, extracts the ECC parameters and generate $P_C = n_C G$.
Choose a random value k.
Encode $P_C || T_C$ as a point T on the curve = ϕ_T
kG, $\phi_T + kP_{AP}$, h(kG, $\phi_T + kP_{AP}$)
$\phi_T + kP_{AP} - n_{AP}(kG) = \phi_T = P_C || T_C$
Check T_C for replayed message
If $h(P_C || T_C) == h(\phi_T)$:
Select MK and encrypt it using P_C as a point S on the curve: $\phi_S = MK || T_{MK}$
Choose a random value u
uG, $\phi_s + uP_C$, h(uG, $\phi_S + uP_C$)
$\phi_S + uP_C - n_C(uG) = \phi_S = MK || T_{MK}$
Check T_{MK} for replay attack
If $h(MK || T_{MK}) == h(\phi_S)$: caches MK
MKID = $\text{trunc}_{64}(h(P_C || P_{AP}))$
MKID = $\text{trunc}_{64}(h(P_C || P_{AP}))$

FIGURE 1. Registration phase.

2) Authentication Phase

This phase authenticates a client to the network. Whenever the client gets disconnected from the network, the reassociation begins with this phase, known as reauthentication. The session keys are produced during this phase, which are utilized for encrypting further communication. All the message exchanges in this phase are encrypted. The phase contains the following steps:

1) Auth Request: The client generates a nonce value N_A and sends it to AP with the current timestamp value T_A by encrypting them with MK.

$$C \rightarrow AP : m_2 = (N_A, T_A)_{MK} \qquad (16)$$

2) Auth Response: On receiving Auth request, AP verifies T_A to check whether the message is genuine or any replayed message. Further, the AP generates a seed key K_{sk} and sends $\{N_A, K_{sk}, T_{sk}\}$ to the client encrypted with MK, where T_{sk} represents the timestamp value. The AP sends N_A again in the response to prove that the AP has successfully received the Auth request message and not any replayed message.

$$AP \rightarrow C : m_3 = \{N_A, K_{sk}, T_{sk}\}_{MK} \qquad (17)$$

3) Next, the client and AP produce session key using PBKDF2 (Password-Based Key Derivation

Function 2) [13], which uses K_{sk} as the key and $N_A||MKID$ as the salt. It undergoes 4096 rounds of encryption to produce a key of 128 bytes in length. We use PBKDF2 because the cryptanalysis attack is highly expensive for this function [13].

$$K_{se} = PBKDF2(HMAC - SHA256, K_{sk}, N_A||MKID, 4096, 128) \quad (18)$$

4) Auth Completion Request: Client further generates a nonce value N_B, timestamp value T_{AB}, and sends $\{N_A, N_B, T_{AB}\}$ to the AP by encrypting it with new session key K_{se}.

$$C \rightarrow AP : m_4 = \{N_A, N_B, T_{AB}\}_{K_{se}} \quad (19)$$

5) Auth Completion Response: The AP verifies T_{AB} and N_A, and acknowledges the correctness of the received message by sending N_B and T_B encrypted with K_{se}. This message proves that both the parties have correctly generated the session key. The purpose of nonces and timestamps in the entire communication is to determine the continuity of messages and prevent replayed messages.

Figure 2 shows the steps involved in authentication phase. Further, the client and AP proceed towards the association phase. Notably, all the subsequent transmitted messages are encrypted with the session key, which gets changed with every session as during reauthentication new session keys are produced by the client and AP.

The registration phase of the proposed protocol is similar to HTTPS in a way that both AP and client verify the identity of other parties using certificates. But the difference is that for every session in HTTPS, the server send its certificate to the client for verification followed by the generation of session keys. Whereas in our protocol, the client verifies the certificate of AP only once, which reduces the computation time. Moreover, with the use of the proposed protocol, the encrypted communication will become a normal scenario which will enhance the security of the network.

Similar to WPA3-OWE, the proposed protocol also uses ECC during the initial handshake for generating master key. But the approach used is different. In WPA3-OWE, both the parties exchange public keys and further ECDH algorithm is utilized for deriving PMK. The unencrypted exchange of public keys and not validating them before proceeding towards PMK generation, make WPA3-OWE vulnerable to MITM and ET attacks. This proves that mere adoption of ECC does not guarantee the resistance of a protocol against network attacks.

The proposed protocol only exchanges the public key of the AP unencrypted, which is also validated by the client using certificate and hostname validation. After successful validation, the client generates it's encryption-decryption key pair and sends it's encryption key to the AP by encrypting it with public key of AP, so that only AP can decode the message. AP generates master key (MK) and sends it to client by encrypting it with encryption key of client, so that only client can decode it. Thus, every client possesses a unique MK used in authentication via four-way handshake. The secure exchange of MK between client and AP without any pre-shared knowledge, unique MKs for every client, encryption of nonces in four-way handshake and preserving the original structure of 802.11 protocol stack are some of the advantages of the proposed protocol. The major advantage of SAP over existing protocols is that it performs key exchange and authentication by utilizing less number of messages. The proposed protocol tries to address the security issues present in the existing protocols while maintaining the latency and computation overhead, making it suitable for low-latency wireless systems.

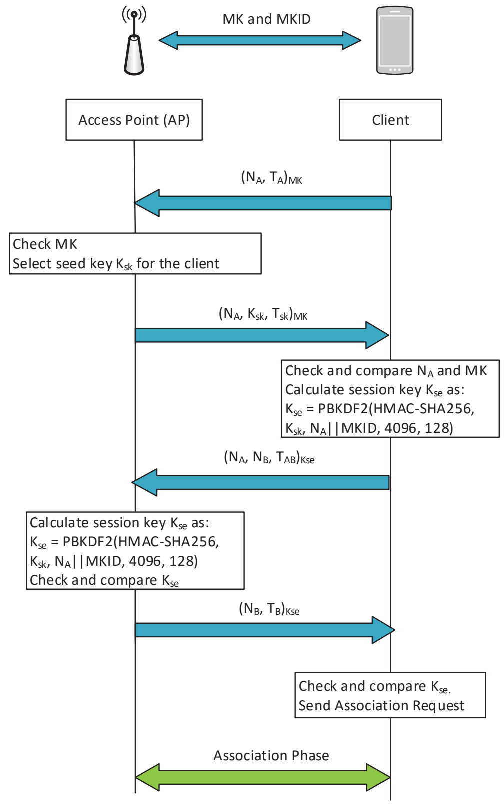

MK and MKID
Access Point (AP)
Client
(N_A, T_A)_MK
Check MK
Select seed key K_sk for the client
(N_A, K_sk, T_sk)_MK
Check and compare N_A and MK
Calculate session key K_se as:
K_se = PBKDF2(HMAC-SHA256,
K_sk, N_A||MKID, 4096, 128)
(N_A, N_B, T_AB)Kse
Calculate session key K_se as:
K_se = PBKDF2(HMAC-SHA256,
K_sk, N_A||MKID, 4096, 128)
Check and compare K_se
(N_B, T_B)Kse
Check and compare K_se.
Send Association Request
Association Phase

FIGURE 2. Authentication phase.

III. ANALYSIS OF SAP

This section theoretically analyzes SAP in various aspects such as mutual authentication and security analysis.

A. MUTUAL AUTHENTICATION BETWEEN CLIENT AND AP

For authenticating client in the network, the AP verifies the MK received by the client in Auth request message. If the MK matches with the one generated and transmitted by the AP to the client in the registration phase (encrypted with the encryption key of the client), the AP authenticates the client in the network.

Suppose an attacker A sends an Auth-request message to AP encrypted with MK':

$$\mathrm{A} \rightarrow \mathrm{AP} : (\mathrm{N}'_{\mathrm{A}}, \mathrm{T}_{\mathrm{A}})_{\mathrm{MK}'} \tag{20}$$

On receiving the message, the AP tries to decrypt the message with the MK cached for the respective client. Since the message is encrypted with MK' and not MK, the AP drops the message and does not send any Auth-response message further.

Similarly, the client also uses MK as a parameter for verifying the authenticity of the AP. The client sends Auth request message encrypted with the MK received from AP in the registration phase. If the AP can decrypt the message and send correct Auth response message, the client believes the legitimacy of the AP.

Suppose the attacker A captures the Auth request message sent by client to AP:

$$\mathrm{C} \rightarrow \mathrm{AP} : (\mathrm{N}_{\mathrm{A}}, \mathrm{T}_{\mathrm{A}})_{\mathrm{MK}} \tag{21}$$

Since the attacker does not possess MK, he is unable to decrypt the message. The attacker can try implementing the partial known-plaintext attack to crack MK as partial message (T_{A}) is already known to the attacker. However, due to the use of randomized nonces and AES-CCMP for encryption, the cryptanalysis is highly expensive [4]. Suppose, the attacker sends an Auth response message encrypted with MK':

$$\mathrm{A} \rightarrow \mathrm{C} : \{\mathrm{N}'_{\mathrm{A}}, \mathrm{K}'_{\mathrm{sk}}, \mathrm{T}_{\mathrm{sk}}\}_{\mathrm{MK}'} \tag{22}$$

On receiving the message, the client tries to decrypt the message with the cached MK. When the client fails to decrypt, it drops the message and does not send any messages further.

Suppose, the MK shared between client and AP gets compromised. Consequently, the attacker successfully exchanges the Auth request and response messages with the client. But, when the attacker receives Auth completion request message from the client encrypted with the session key, he fails to decrypt the message because he is unable to produce correct session key. The reason being, the attacker does not have access to MKID generated in the registration phase. Thus, both client and AP can mutually authenticate each other in SAP and no third party can do this.

B. SECURITY ANALYSIS

In this subsection, we prove that the proposed protocol is able to prevent the exchanged messages from various types of network attacks, which we have formally proved in Section IV. We assume that capturing private key of the AP and decryption key of the client is not possible by the attacker as nowhere in the communication they are being exchanged. Figure 3 shows the network model of SAP. In this model, three entities exist - client, AP and attacker. The figure shows the system setup of the network in the presence of the proposed protocol, the attacker's objectives and information possessed by the entities. In the figure, green-colored text represents publicly available information, black-colored text denotes the knowledge of the entities, and blue-colored text implies information being targeted by the attacker.

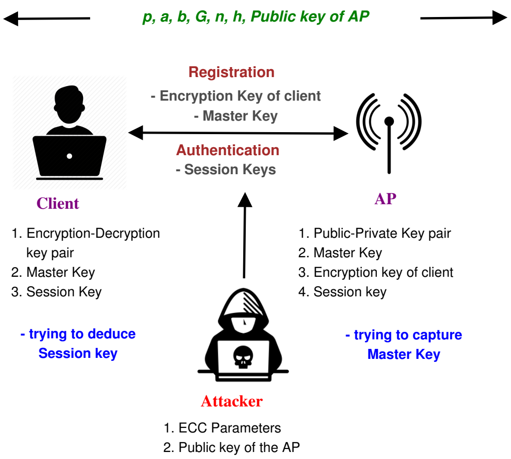

p, a, b, G, n, h, Public key of AP
Registration
- Encryption Key of client
- Master Key
Authentication
- Session Keys
Client
AP
1. Encryption-Decryption key pair
2. Master Key
3. Session Key
1. Public-Private Key pair
2. Master Key
3. Encryption key of client
4. Session key
- trying to deduce Session key
- trying to capture Master Key
Attacker
1. ECC Parameters
2. Public key of the AP

FIGURE 3. Network model showing Network entities, their capabilities, attacker's objective and system setup used in SAP.

1) Eavesdropping

In SAP, all the exchanged messages are either encrypted using ECC or symmetric encryption to maintain end-to-end confidentiality of exchanged messages in the network. If the attacker eavesdrops the communication, he gets the encrypted frames which cannot be decrypted without the knowledge of private and decryption key (ECC), and MK and session keys (symmetric encryption). As already discussed, the attacker cannot obtain private and decryption keys because they are never transmitted. Thus, the attacker cannot generate MK and session keys as they are exchanged through messages encrypted with ECC keys. Hence, the transmitted messages in the network are secure from eavesdropping in the presence of the proposed protocol.

2) Replay Attack

SAP is resistant to replay attack as it sends timestamp values ($\mathrm{T}_{\mathrm{c}}, \mathrm{T}_{\mathrm{MK}}, \mathrm{T}_{\mathrm{A}}, \mathrm{T}_{\mathrm{sk}}, \mathrm{T}_{\mathrm{AB}}, \mathrm{T}_{\mathrm{B}}$) with every message in the registration and authentication phase. Further, SAP also uses nonces in the authentication phase to prove the continuity of messages.

3) ET Attack

The objective of the attacker in ET attack is to force clients to get disconnected from the genuine AP and get connected to the ET so that the attacker can control the network traffic of the client. Suppose, in a network equipped with SAP; an ET disconnects a client from a genuine AP by sending deauthentication frames. The client tries to reauthenticate by sending Auth request frame. Although, the Auth request sent by the client is received by the ET, the ET is unable to read the contents of the message as it is encrypted with MK. Therefore, ET is unable to send correct Auth response message. An ET attack cannot be successful in the presence of SAP as an attacker needs private and public key of the AP and encryption key of the client to capture MK for successfully launching an ET attack.

4) MITM Attack

In this attack, the attacker tries to locate itself between client and AP, such that all the communication between them is through the attacker. Thus, the attacker can either intercept, replay or inject messages in the ongoing communication between the two parties. In our context, an attacker can perform MITM attack in two ways - (1) by launching ET attack and (2) by performing registration phase with the client. We have already proved that the ET attack cannot be launched in a network implementing SAP. Suppose, the client sends the probe request message to the AP. Attacker eavesdrops the communication and tries to forge the message to make the client connect to itself. However, the attacker cannot decrypt the probe request encrypted by the public key of AP as it does not have access to the private key of the AP. Nowhere in the exchanged messages, the private keys are shared. Moreover, we provide a public key certificate to the AP which makes the protocol resistant to MITM attack.

IV. FORMAL VERIFICATION OF SAP

The formal verification of security protocols can be performed using model checking approach to automatically verify the security properties of a protocol. It is based on evaluating the protocol by exploring all possible states and behaviors of the protocol. It runs multiple instances of the protocol simultaneously and analyzes whether the protocol satisfies security properties in all the instances or not.

To verify and analyze the security properties of the proposed protocol, we use Scyther. The reasons being manifold - (1) Scyther utilizes the unbounded model checking approach with confirmed termination which allows it to verify all possible states and behaviors of the protocol [14], (2) Scyther uses backward symbolic state search technique which empowers it to explore all type flaws and infinite state spaces [14] and (3) According to a study conducted in [15], Scyther is the fastest tool among the existing state-of-the-art tools. In case of an attack, it gives an attack scenario which provides a better understanding of the flaws in the protocol.

In the subsequent subsections, we explain the adversary model and security claims used in Scyther, and further, we discuss the modeling and verification of SAP using Scyther. Scyther uses spdl (Security Protocol Definition Language) format for describing the semantics of a protocol, which is explicitly invented for Scyther.

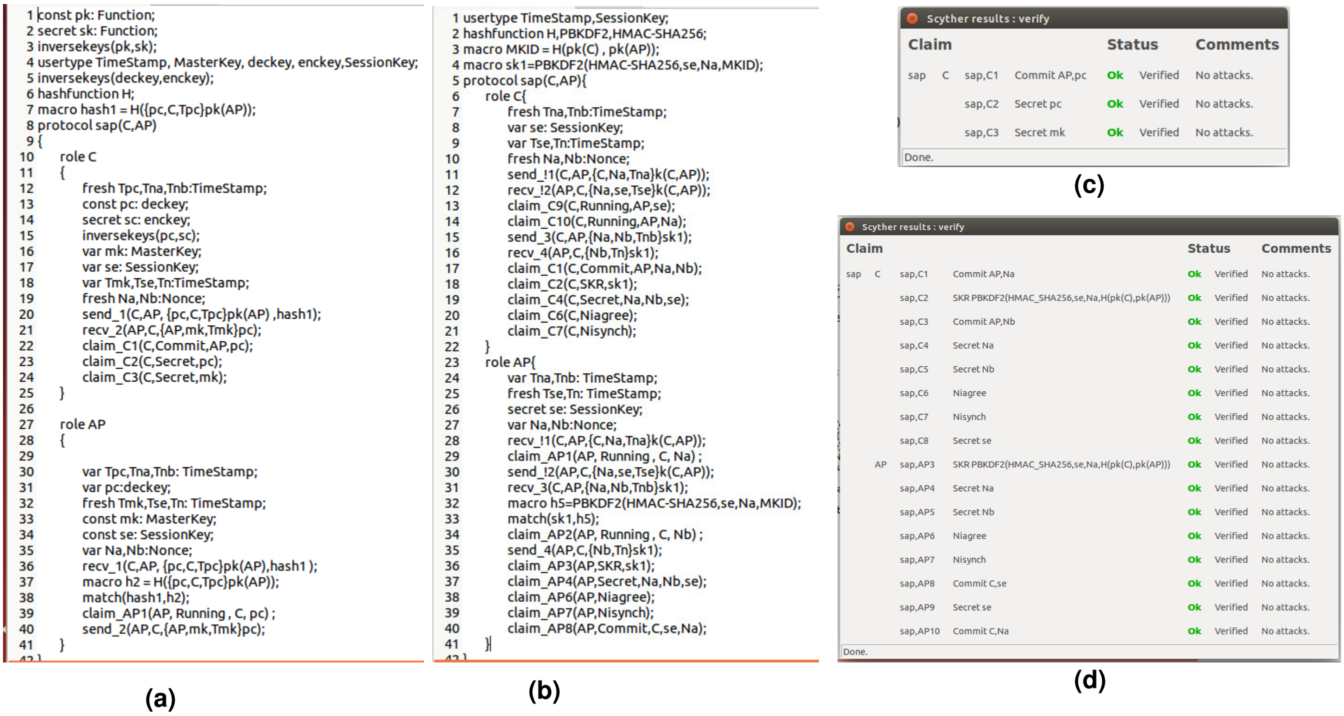
A. ADVERSARY MODEL

Scyther uses Dolev-Yao model as an adversary model which allows the adversary to replay, delete, breach, reroute, eavesdrop and process the content of the messages exchanged through the network. This model is predefined in the semantics of Scyther and thus, there is no need to define capabilities of an adversary for analyzing protocols in Scyther.

B. SECURITY CLAIMS

In Scyther, security properties are represented in the form of claims known as security claims. The adherence of a claim is checked by verifying whether the claim state is reachable or not during the protocol execution. Security claims in Scyther include:

- Secrecy: According to this claim, the messages exchanged over the network are not exposed to the attacker, even when the network is under full control of the attacker. The secrecy claim is expressed as $\mathrm{claim_L(R, secret, rt)}$ which denotes, for the role R, rt should not be known to the adversary [14]. If rt is a session key, Scyther uses $\mathrm{claim_L(R, SKR, rt)}$ to represent the secrecy of rt, where SKR stands for Session Key Reveal.
- Mutual Authentication: According to this claim, the communication must happen with the intended communication partner and not with the adversary. For verifying the authenticity of the communicating party, Scyther introduces the notion of Synchronization. This property states that the communication should occur between the expected, intended and genuine partners, and the protocol events should execute in the same way as described in the protocol specification. The synchronization claim is expressed as $\mathrm{Nisynch(R, Nisynch)}$, where Nisynch stands for Non-injective Synchronization.
- Agreement over exchanged messages: Mutual authentication is not sufficient to judge whether the sent message is exactly same as the received message or not. It is also crucial to verify the integrity of the exchanged messages by checking the agreement of both the parties on the contents of exchanged messages. Scyther uses commit signal to verify the integrity of exchanged messages during protocol execution.



```
const pk: Function;
secret sk: Function;
inversekeys(pk,sk);
usertype TimeStamp, MasterKey, deckey, enckey,SessionKey;
inversekeys(deckey,enckey);
hashfunction H;
macro hash1 = H({pc,C,Tpc}pk(AP));
protocol sap(C,AP)
{
    role C
    {
        fresh Tpc,Tna,Tnb:TimeStamp;
        const pc: deckey;
        secret sc: enckey;
        inversekeys(pc,sc);
        var mk: MasterKey;
        var se: SessionKey;
        var Tmk,Tse,Tn:TimeStamp;
        fresh Na,Nb:Nonce;
        send_1(C,AP, {pc,C,Tpc}pk(AP) ,hash1);
        recv_2(AP,C,{AP,mk,Tmk}pc);
        claim_C1(C,Commit,AP,pc);
        claim_C2(C,Secret,pc);
        claim_C3(C,Secret,mk);
    }

    role AP
    {

        var Tpc,Tna,Tnb: TimeStamp;
        var pc:deckey;
        fresh Tmk,Tse,Tn: TimeStamp;
        const mk: MasterKey;
        const se: SessionKey;
        var Na,Nb:Nonce;
        recv_1(C,AP, {pc,C,Tpc}pk(AP),hash1 );
        macro h2 = H({pc,C,Tpc}pk(AP));
        match(hash1,h2);
        claim_AP1(AP, Running , C, pc) ;
        send_2(AP,C,{AP,mk,Tmk}pc);
    }
}
```

(a)

```
usertype TimeStamp,SessionKey;
hashfunction H,PBKDF2,HMAC-SHA256;
macro MKID = H(pk(C) , pk(AP));
macro sk1=PBKDF2(HMAC-SHA256,se,Na,MKID);
protocol sap(C,AP){
    role C{
        fresh Tna,Tnb:TimeStamp;
        var se: SessionKey;
        var Tse,Tn:TimeStamp;
        fresh Na,Nb:Nonce;
        send_!1(C,AP,{C,Na,Tna}k(C,AP));
        recv_!2(AP,C,{Na,se,Tse}k(C,AP));
        claim_C9(C,Running,AP,se);
        claim_C10(C,Running,AP,Na);
        send_3(C,AP,{Na,Nb,Tnb}sk1);
        recv_4(AP,C,{Nb,Tn}sk1);
        claim_C1(C,Commit,AP,Na,Nb);
        claim_C2(C,SKR,sk1);
        claim_C4(C,Secret,Na,Nb,se);
        claim_C6(C,Niagree);
        claim_C7(C,Nisynch);
    }
    role AP{
        var Tna,Tnb: TimeStamp;
        fresh Tse,Tn: TimeStamp;
        secret se: SessionKey;
        var Na,Nb:Nonce;
        recv_!1(C,AP,{C,Na,Tna}k(C,AP));
        claim_AP1(AP, Running , C, Na) ;
        send_!2(AP,C,{Na,se,Tse}k(C,AP));
        recv_3(C,AP,{Na,Nb,Tnb}sk1);
        macro h5=PBKDF2(HMAC-SHA256,se,Na,MKID);
        match(sk1,h5);
        claim_AP2(AP, Running , C, Nb) ;
        send_4(AP,C,{Nb,Tn}sk1);
        claim_AP3(AP,SKR,sk1);
        claim_AP4(AP,Secret,Na,Nb,se);
        claim_AP6(AP,Niagree);
        claim_AP7(AP,Nisynch);
        claim_AP8(AP,Commit,C,se,Na);
    }
}
```

(b)

```
Claim                                  Status          Comments
sap   C    sap,C1   Commit AP,pc       Ok   Verified   No attacks.
           sap,C2   Secret pc          Ok   Verified   No attacks.
           sap,C3   Secret mk          Ok   Verified   No attacks.
Done.
```

(c)

```
Claim                                                                    Status          Comments
sap   C    sap,C1    Commit AP,Na                                        Ok   Verified   No attacks.
           sap,C2    SKR PBKDF2(HMAC_SHA256,se,Na,H(pk(C),pk(AP)))       Ok   Verified   No attacks.
           sap,C3    Commit AP,Nb                                        Ok   Verified   No attacks.
           sap,C4    Secret Na                                           Ok   Verified   No attacks.
           sap,C5    Secret Nb                                           Ok   Verified   No attacks.
           sap,C6    Niagree                                             Ok   Verified   No attacks.
           sap,C7    Nisynch                                             Ok   Verified   No attacks.
           sap,C8    Secret se                                           Ok   Verified   No attacks.
      AP   sap,AP3   SKR PBKDF2(HMAC_SHA256,se,Na,H(pk(C),pk(AP)))       Ok   Verified   No attacks.
           sap,AP4   Secret Na                                           Ok   Verified   No attacks.
           sap,AP5   Secret Nb                                           Ok   Verified   No attacks.
           sap,AP6   Niagree                                             Ok   Verified   No attacks.
           sap,AP7   Nisynch                                             Ok   Verified   No attacks.
           sap,AP8   Commit C,se                                         Ok   Verified   No attacks.
           sap,AP9   Secret se                                           Ok   Verified   No attacks.
           sap,AP10  Commit C,Na                                         Ok   Verified   No attacks.
Done.
```

(d)

FIGURE 4. **(a) spdl script for registration phase, (b) spdl script for reauthentication phase, (c) Scyther execution results for registration phase, and (d) Scyther execution results for reauthentication phase.**

C. VERIFICATION OF THE PROPOSED PROTOCOL

The proposed protocol involves two parties - AP = Access point and C = Client. Table 2 represents the notations with their descriptions used in the verification of the proposed protocol using Scyther. The messages exchanged during the execution of the proposed protocol are represented according to the notations described in Table 2.

TABLE 2. **Notations with their descriptions used in the verification of the proposed protocol using Scyther**

S.No.	Notation	Description
1.	sc	Decryption key of client
2.	pc	Encryption key of client
3.	sk(AP)	Private key of AP
4.	pk(AP)	Public key of AP
5.	Na, Nb	Nonces
6.	se	Seed key
7.	sk1	Session key
8.	mk	Master key
9.	T	Timestamp

Registration

- $\mathrm{C} \rightarrow \mathrm{AP} : \mathrm{m}_0 = \{\mathrm{pc},\ \mathrm{Tpc}\}\mathrm{pk}(\mathrm{AP}),\ \mathrm{hash}(\mathrm{m}_0)$
- $\mathrm{AP} \rightarrow \mathrm{C} : \mathrm{m}_1 = \{\mathrm{mk},\ \mathrm{Tmk}\}\mathrm{pc},\ \mathrm{hash}(\mathrm{m}_1)$

Authentication

- $\mathrm{C} \rightarrow \mathrm{AP} : \mathrm{m}_2 = \{\mathrm{Na},\ \mathrm{Tna}\}\mathrm{mk}$
- $\mathrm{AP} \rightarrow \mathrm{C} : \mathrm{m}_3 = \{\mathrm{Na},\ \mathrm{se},\ \mathrm{Tse}\}\mathrm{mk}$
- $\mathrm{C} \rightarrow \mathrm{AP} : \mathrm{m}_4 = \{\mathrm{Na},\ \mathrm{Nb},\ \mathrm{Tnb}\}\mathrm{sk1}$
- $\mathrm{AP} \rightarrow \mathrm{C} : \mathrm{m}_5 = \{\mathrm{Nb},\ \mathrm{Tn}\}\mathrm{sk1}$

We assume that revelation of sk(AP) and sc to the attacker is not possible, as nowhere in the protocol specification, private and decryption keys are exchanged. Figure 4(a) and 4(b) represent the spdl scripts of registration and authentication phase of the proposed protocol, respectively. In Figure 4(b), the authentication phase represents the script used in reauthentication, where mk is replaced with k(C, AP) as in reauthentication phase mk acts as a symmetric key shared between client and AP.

The following security claims are made in spdl scripts of registration and authentication phases of SAP:

- claim(C, Secret, pc/mk): The encryption key of the client and master key generated by AP should not be revealed to the attacker for preventing MITM and ET attacks.
- claim(C, Commit, AP, pc): Client C and AP should agree on the value of pc to proceed towards the authentication phase.
- claim(AP/C, Secret, se/Na/Nb): The seed key and nonces used as an input to generate session key should not be leaked to the adversary to forbid attacker from generating the session key.
- claim(AP/C, SKR, sk1): The generated session key sk1 should not be revealed to the attacker to avoid

eavesdropping, MITM and message tampering attacks.

- claim(C/AP, Commit, AP/C, Na/Nb/se): The AP and client should agree on the values of nonces Na and Nb, and seed key se, to ensure prevention from tampering attack.
- claim(C/AP, Nisynch): For both the roles, the claim of synchronization should hold to ensure prevention from replay, ET and MITM attacks.

Figure 4(c) and 4(d) represent the Scyther execution results of the proposed protocol, which shows that no attack has been found in the protocol. Hence, the proposed protocol is secure from the network attacks.

V. PRACTICAL PERSPECTIVE: SIMULATION OF PROPOSED PROTOCOL

The proposed protocol is simulated using the INET Framework extension of broadly accepted OMNeT++ simulator [16] on Windows 10 platform. The INET framework of OMNeT++ represents network devices such as hosts, switches, routers, APs, etc., as modules written in C++. It also contains devices configured with IEEE 802.11 network interfaces and represents several layers of the IP suite such as UDP, TCP, ARP and IPv4 protocols. We embed OpenSSL APIs (Application Program Interface) in INET framework to model the cryptographic operations (ECC, AES-CCMP and PBKDF2) of the proposed protocol.

A. SIMULATION SETUP

The setup for simulation consists of a network containing an AP modeled using AccessPoint compound module of INET, client modeled using WirelessHost compound module of INET, configurator module to assign IP address to the network entities, radioMedium module to send and receive packets for wireless nodes, visualizer module to visualize the packet transmission in the network, and pcapRecorder module to record the packets and further analyze them using packet analyzer tools such as Wireshark. Figure 5 shows the network setup used for simulation.

We modified the management layer frames of AccessPoint and WirelessHost modules to include the ECC encryption and decryption operations in beacon, probe request and probe response frames; AES encryption and decryption functions in authentication frames; and PBKDF2 function for session key generation. The UDP protocol is used for exchanging messages between the modules.

B. SIMULATION RESULTS AND DISCUSSION

The INET framework of OMNeT++ already contains a default implementation of the scanning and authentication process performed in IEEE 802.11 open networks. Since we modified the packet contents of the default implementation of IEEE 802.11 network protocol, we compared the performance of proposed protocol with the default open network protocol. The comparison is performed on various parameters such as computation overhead analysis (in ms) and packet size (in bytes).

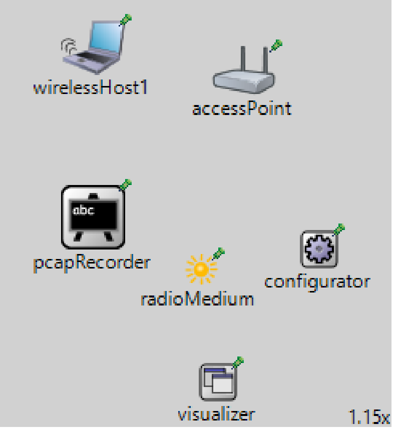


FIGURE 5. Simulation setup for the proposed protocol.

TABLE 3. Timing Analysis

Algorithm.	Action	Approximate Time Taken (in μs)
ECC	Encryption	200
	Decryption	300
	Key Generation	50
AES-CCMP	Encryption	400
	Decryption	500
PBKDF2	Key Generation	100

1) Computation Overhead Analysis

Since the proposed protocol performs key generation and encryption-decryption functions in registration and authentication phases, it incurs an additional computation time. In the simulation of the proposed protocol, the approximate computation time spent on key generation and encryption-decryption operations by using various cryptographic algorithms is shown in Table 3. For ECC operations, we use the standard NIST curve Secp384r1 owing to the reason that for a highly secure system, a minimum of 384-bit key size is required [17].

Let the time taken to generate a key, encrypt and decrypt a message using ECC be represented as α, β and γ, respectively; time taken to encrypt and decrypt a message using AES-CCMP be denoted as δ and ϵ, respectively; and time taken to generate a key using PBKDF2 be represented as η.

During the registration phase in SAP, the client generates keys using ECC and all the message transmissions are encrypted and decrypted through ECC. Let the computation time spent during the registration phase be denoted as T_{reg}. It is calculated as:

$$T_{reg} = \alpha + 2 \times \{\beta + \gamma\} \tag{23}$$

Using the values in Table 3, T_{reg} is evaluated as approximately 1050 μs. During the authentication phase, SAP encrypts and decrypts the messages using AES-CCMP and produces session key using PBKDF2 algorithm. Let the computation time consumed during the authentication phase be represented as T_{auth}. It is computed as:

$$T_{auth} = 2 \times \eta + 4 \times \{\delta + \epsilon\} \tag{24}$$

The approximate value of T_{auth} is obtained as 3800μs. Thus, the total overhead incurred while connecting to SAP is 4850μs (T_{reg} + T_{auth}). So, overhead approximates to 4.85ms. However, the registration phase is a one-time process, so the overhead for reauthentication process of the proposed protocol is 3.8ms only. For many applications, low-latency is of utmost importance, such as factory automation applications require latency between $0.25-10$ms, Intelligent Transport System (ITS) applications between $10-100$ms, heathcare applications between $1-10$ms and education applications require less than 10ms [18]. Since the proposed protocol incurs a very low computational overhead, it can be a suitable choice for such applications.

2) Packet Size

Since the packets transmitted during registration and authentication phases in SAP implementation carries additional encrypted information for safely exchanging master and session keys, a comparison between the packet sizes of various frames under SAP and default open network implementation is required. Figure 6 shows the packet size comparison. The difference in packet sizes of frames under SAP and default open network INET implementation during registration and authentication phases is approximately 71B and 35B. We agree that the difference is not negligible, but if the trade-off between security offered by SAP in open networks and the packet sizes is considered, the difference can be ignored.

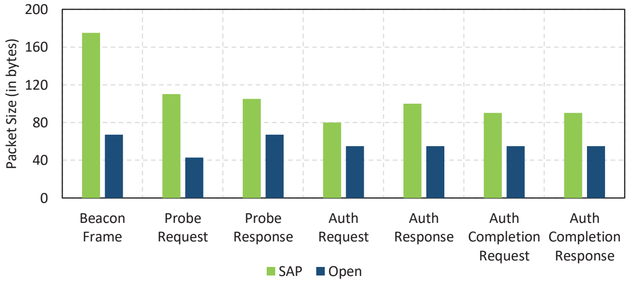


FIGURE 6. **Packet Size.**

VI. COMPARISON OF THE PROPOSED PROTOCOL WITH EXISTING STANDARD PROTOCOLS

We compared SAP with the most widely used protocols WEP, WPA, WPA2, WPA3, and 802.1x based on the following characteristics in Table 4 - Attack methods successfully used against the protocols, number of parties involved in the connection establishment and the total number of messages exchanged during the process. According to Table 4, the open authentication protocol is vulnerable to all the attacks as it does not incorporate any type of authentication and encryption. WPA is susceptible to ET, MITM and message tampering attacks due to the use of weaker encryption standards such as RC4. WPA2 is vulnerable to ET and MITM attacks due to the unencrypted transfer of nonces making it a prey to offline dictionary attack. WPA3-OWE is considered as the most secure protocol for public networks at the time of writing this paper. It is found secure against all attacks except message tampering and ET attacks because of unencrypted transmission of authentication messages and the use TOFU (Trust-on-first-use) model for authentication. The computational overhead of WPA3-personal is very high given the complexity of the SAE handshake [9]. Moreover, it undergoes two rounds of four-way handshakes before authentication leading to a high connection establishment time and thus, a high latency protocol. The credential-based 802.1X protocol is vulnerable to sniffing attack due to unencrypted over-the-air transfer of credentials. Most of the organizations including small-scale industries and tertiary educational institutes (TEIs) still use credential-based 802.1X protocol without enforcing the optional RADIUS server identity verification making them vulnerable to ET and sniffing attacks. As per the study conducted in [19], out of 7045 TEIs across 56 contries, 86% are vulnerable to credential theft and ET attacks. To overcome this problem, 802.1X introduced certificate-based protocol which uses unique client certificates for authentication. RADIUS server authentication by clients is not implemented in many networks due to the increased overhead caused by the certificate management, which makes it vulnerable to ET attacks. In addition, 802.1X exchanges a higher number of messages for authentication compared to SAP. The costs of implementing and operating an 802.1X based network are significant, as additional servers are required and the complexity of administration and certificate management is high.

From the Table 4, it can be seen that SAP exchanges the least number of messages compared to the presented protocols (except for open), which for directly results in reduced authentication and re-authentication time. In addition to this property, which is especially required in the area of low-latency applications, SAP offers very good protection against all evaluated threats. It assures end-to-end encrypted message transmission without any high-level expertise requirement for deployment. Al-

TABLE 4. Comparative analysis of SAP with existing standard protocols.

Protocol	Eavesdropping	Replay attack	ET attack	MITM attack	Message Tampering attack	No. of parties involved	Total messages exchanged
Open	✗	✗	✗	✗	✗	2	7
SAP	✓	✓	✓	✓	✓	2	9
WPA	✓	✓	✗	✗	✗	2	11
WPA2	✓	✓	✗	✗	✓	2	11
WPA3-OWE	✓	✓	✗	✓	✗	2	13
WPA3-personal	✓	✓	✗	✓	✓	2	15
Credential-based 802.1X	✗	✓	†	✓	✓	4	22
Certificate-based 802.1X	✓	✓	†	✓	✓	4	15

✗= The protocol is vulnerable to the attack, ✓= The protocol is resistant to the attack, †= The protocol may or may not be vulnerable to the attack

though the protocol introduces the use of certificates for AP authentication which adds additional cost to AP setup, low-latency, small computation overhead and security from network attacks makes it a reliable choice for sectors requiring both security and availability as their key parameters. The use of ECC makes SAP suitable for embedded and IIoT devices as ECC incurs low computational overhead owing to its small key size.

VII. CONCLUSIONS

In this paper, we tried to emphasize the prominence of low-latency along with security in wireless networks for delay sensitive applications and studied the existing protocols in terms of computation overhead with respect to number of packets required for the authentication and reauthentication, and in terms of security with respect to traditional network attacks. We proposed a protocol comprising of two phases, where in the first phase cryptographic credentials are generated and securely exchanged and in the second phase, mutual authentication occurs. With simulation experiments, it is shown that the proposed protocol incurs low computation overhead and a lower authentication time. The protocol utilizes lightweight cryptographic primitives making it suitable for embedded and low-power devices. By using formal verification, we have justified resistance of SAP against network attacks and by performing comparative analysis, we demonstrate its advantages over the existing protocols. In future, the authors intend to imbibe trust management in the protocol with a strong focus on the deployment of certificates on embedded and IIoT devices so that client side attacks can be contained without additional expense.

Although 5G networks are already available and will be a performant alternative for many delay-sensitive applications, the initial investment and implementation costs for 5G networks are too high in many cases. They are not economically feasible for many small and start-up businesses as well as in the hobbyist/consumer sector. In addition, the 5G standard is still under development and does not yet include all of the targeted features, so this technology is no replacement for widely used Wi-Fi based embedded platforms. In addition to the initial and ongoing operating costs, the flexibility of a communication standard will also play an important role regarding the acceptance. The use of the license-free industrial, scientific, and medical (ISM) frequency bands provides a high degree of freedom during development, which has led to products that are strongly tailored towards one specific application. It is likely that a large number of different wireless communication standards will continue to co-exist in the future, especially in certain specialized areas. For this reason, wireless network protocols need to be developed that place their emphasis on both security as well as low-latency and computational overhead. With the increasing use of IIoT and embedded devices, we would like to raise awareness among the research community about the importance of the interaction between security, latency, and computational overhead in the context of wireless network applications. The development of dedicated protocols would be an important step towards enhancing the use of wireless networks in industrial applications and would enable a variety of new applications.

REFERENCES

[1] Cisco visual networking index: Global mobile data traffic forecast update, 2017–2022. http://media.mediapost.com/uploads/CiscoForecast.pdf. [Online; accessed 03-June-2022].
[2] Cisco annual internet report (2018–2023) white paper. https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html. [Online; accessed 25-November-2022].
[3] Andreas Frotzscher, Ulf Wetzker, Matthias Bauer, Markus Rentschler, Matthias Beyer, Stefan Elspass, and Henrik Klessig. Requirements and current solutions of wireless communication in industrial automation. In 2014 IEEE international conference on communications workshops (ICC), pages 67–72, 2014.
[4] Christopher Kohlios and Thaier Hayajneh. A comprehensive attack flow model and security analysis for wi-fi and wpa3. Electronics, 7(11):284, 2018.
[5] Joon S Park and Derrick Dicoi. Wlan security: current and future. Internet Computing, 7(5):60–65, 2003.

[6] Md Waliullah and Diane Gan. Wireless lan security threats & vulnerabilities. International Journal of Advanced Computer Science and Applications, 5(1), 2014.
[7] Omar Nakhila, Afraa Attiah, Yier Jin, and Cliff Zou. Parallel active dictionary attack on wpa2-psk wi-fi networks. In MILCOM 2015-2015 IEEE Military Communications Conference, pages 665–670. IEEE, 2015.
[8] Songhui Kwon and Hyoung-Kee Choi. Evolution of wi-fi protected access: security challenges. IEEE Consumer Electronics Magazine, 10(1):74–81, 2020.
[9] Mathy Vanhoef and Eyal Ronen. Dragonblood: Analyzing the dragonfly handshake of wpa3 and eap-pwd. In 2020 IEEE Symposium on Security and Privacy (SP), pages 517–533. IEEE, 2020.
[10] Industrial wireless: choosing between wi-fi & cellular. https://www.automate.org/industry-insights/industrial-wireless-part-3-choosing-between-wi-fi-and-cellular. [Online; accessed 14-October-2021].
[11] Nissa Mehibel and M'Hamed Hamadouche. A new approach of elliptic curve diffie-hellman key exchange. In 2017 5th International Conference on Electrical Engineering-Boumerdes (ICEE-B), pages 1–6, Boumerdes, Algeria, 2017.
[12] Aritro Sengupta and Utpal Kumar Ray. Message mapping and reverse mapping in elliptic curve cryptosystem. Security and communication networks, 9(18):5363–5375, 2016.
[13] PBKDF2. https://en.wikipedia.org/wiki/PBKDF2. [Online; accessed 15-March-2018].
[14] Casimier Joseph Franciscus Cremers. Scyther: Semantics and verification of security protocols. Ph.D. dissertation, Inst. Program. Res. Algorithmics, Eindhoven University of Technology, Eindhoven, The Netherlands, 2006.
[15] Cas Cremers and Pascal Lafourcade. Comparing state spaces in automatic security protocol verification. Proceedings 7th International Workshop on Automated Verification of Critical Systems (AVoCS'07), 558, Electronic Notes Theoreotical Compututer Science, Elsevier Science Publishers B. V. 2007.
[16] Omnet++ discrete event simulator. https://omnetpp.org/. [Online; accessed 14-March-2020].
[17] Elliptic curve cryptography. https://www.linuxjournal.com/content/elliptic-curve-cryptography. [Online; accessed 15-April-2018].
[18] Imtiaz Parvez, Ali Rahmati, Ismail Guvenc, Arif I Sarwat, and Huaiyu Dai. A survey on low latency towards 5g: Ran, core network and caching solutions. IEEE Communications Surveys & Tutorials, 20(4):3098–3130, 2018.
[19] Man Hong Hue, Joyanta Debnath, Kin Man Leung, Li Li, Mohsen Minaei, M Hammad Mazhar, Kailiang Xian, Endadul Hoque, Omar Chowdhury, and Sze Yiu Chau. All your credentials are belong to us: On insecure wpa2-enterprise configurations. In Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security, pages 1100–1117, 2021.

DR. VINEETA JAIN is currently pursuing her postdoctoral study at Fraunhofer Institute of Integrated Circuits IIS Division Engineering of Adaptive Systems EAS, Germany. Her research interests include the area of security and privacy with a special emphasis on wireless networks and mobile security. She received her Ph.D. in computer science from Malaviya National Institute of Technology Jaipur, India. She is a member of IEEE. Contact her at vineeta.jain@eas.iis.fraunhofer.de.

ULF WETZKER is a Research Scientist with the Division Engineering of Adaptive Systems (EAS), Fraunhofer Institute for Integrated Circuits IIS, Germany. His research interests are in the areas of wireless communication systems, data analytics, and machine learning, with a special focus on anomaly detection in wireless networks. He received the Diploma degree in computer science and systems engineering from the Ilmenau University of Technology, Ilmenau, Germany. Contact him at ulf.wetzker@eas.iis.fraunhofer.de

PROF. VIJAY LAXMI is a faculty in Department of Computer Science and Engg., Malaviya National Institute of Technology Jaipur, India. Her research interests include Information security, Malware analysis, Security and QoS provisioning in wireless Networks. She received her PhD from University of Southampton, UK. Contact her at vlaxmi@mnit.ac.in.

PROF. MANOJ SINGH GAUR has been a faculty in Department of Computer Engg., Malaviya National Institute of Technology Jaipur, India and currently Director, IIT Jammu, India. His research areas include Networks-on-Chip, Computer and network security and wireless networks. He received PhD from University of Southampton, UK. He is a member of IEEE. Contact him at gaurms@mnit.ac.in.

PROF. MOHAMED MOSBAH is a full Professor in computer science at the Polytechnic Institute of Bordeaux, France. His research interests include distributed algorithms and systems, formal models, security, and ad hoc and sensor networks. He obtained his Ph.D. from the University of Bordeaux, in 1993. Contact him at mohamed.mosbah@labri.fr

PROF. DOMINIQUE MERY is a full professor of computing science at University of Lorraine since September 1993. His research interests include proof-oriented system development for computer-based systems with higher levels of reliability and correctness, proof- based development of distributed algorithms and the proof-based modelling of medical devices. He is a member of IEEE. Contact him at dominique.mery@loria.fr.