International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 15, No.1 (Apr. 2024)

http://dx.doi.org/10.12785/ijcds/1501112

Towards Robust and Low Latency Security Framework for IEEE 802.11 Wireless Networks

Inam Ul Haq[1], Amna Nadeem[2], Saba Ramzan[3], Nazir Ahmad[1] and Yasir Ahmad[1]

[1]*Faculty of Computing, University of Okara, Okara, Pakistan*
[2]*Lahore Garrison University Lahore, Pakistan*
[3]*Superior University, Lahore, Pakistan*

Received 13 May. 2023, Revised 01 Feb. 2024, Accepted 03 Apr. 2024, Published 06 Apr. 2024

Abstract: Due to inherent vulnerability, wireless networks require additional security, integrity, and authentication. The purpose of this study is to highlight the outdated ”Counter Mode Cipher Block Chaining Message Authentication Code Protocol” (CCMP) that has lately taken the place of the flawed ”Wired Equivalent Privacy” (WEP) protocol for authenticating IEEE 802.11 (WLANs). The IEEE 802.11s, a draught widespread for wireless networks in a mesh topology, also recommended using CCMP (WMNs). Due to CCMP’s two-pass operation, multi-hop wireless networks like WMN have a considerable latency problem. An increase in latency results in a decrease in service quality for multimedia applications as it is sensitive to delays. In addition to highlighting the CCMP’s vulnerability to pre-computation time-memory trade-off (TMTO) attacks, this paper recommends improving WLAN packet security by implementing a packet-by-packet security mechanism. Furthermore, we propose a fresh, dependable, low-latency foundation for WMN. Our security framework architecture employs a piggyback challenge-response mechanism to ensure data secrecy and data integrity. The use of a secret nonce, a new encryption key for each packet, and packet-level authentication are all features of the Piggyback challenge-response protocol. By authenticating every packet, unauthorized access can be swiftly prevented.

Keywords: Social Networks, Information Security, Decentralization, Individual Servers, Decentralized Framework

1. INTRODUCTION

Even when not physically connected to the network, devices with wireless capabilities can access computing resources through wireless networks. The device must be close enough to a wireless network infrastructure to be within a set range. A group of wireless network nodes with radio communication capabilities gathered in a confined space is renowned as a WLAN. The WLAN is typically an extension of existing wired LANs to enable user mobility and regularly used devices a relatively in short range. Wi-Fi is just one of the many standards and technologies created since wireless networks started to take off. The IEEE is one of the most active groups developing standards for wireless networks (IEEE). This guidebook section primarily discusses the WLAN IEEE 802.11 group of standards that provides a broad overview of wireless networks. The center components of an IEEE 802.11 WLAN are described in Segment 2.2, together with the architectural models that shape the idea for the remainder of the manual.

The objectives of this study are to identify (1) Vulnerabilities of IEEE 802.11WLAN (2) Beacon Frames and Service Set Identifiers (SSID) Problems (3) MAC ACL Problems (ACL) (4) Weaknesses in Authentication Schemes and provide effective security mechanism to tackle these issues. The major contribution is to propose a Per-Packet Authentication Mechanism. In this mechanism, the pair-wise key hierarchy uses pseudo-random functions (PRFs) to extract session-specific keys from the pairwise master key (PMK) [1]. The PMK is accessible through a successful IEEE 802.1X exchange, a pre-shared key (PSK), or a cached PMK obtained in another way. PMK has a bit size of 256. The pair-wise key hierarchy uses the PMK to produce a pairwise transitional key (PTK). The PTK also produces a Temporary Key (TK). This key is thus the shared encryption key utilized in AES counter mode to encode the MIC and the data. To obtain the counter’s initial value from the time key, we advise using PRF-128 as described as a pseudorandom function that outputs 128 bits.

A. *Short History of Wireless Networking Standards*

WLAN technology initially became widely available in the late 1990s with manufacturers’ introduction of products that functioned in the 900 MHz bands. These technologies used proprietary, non-standard architectures with data rates of roughly 1 megabit per second (Mbps). It’s mile far slower than the average wired local area network (LAN) speed of 10 Mbps. In 1992, manufacturers began selling WLAN hardware that used 2.4 gigahertz (GHz), Even though some products used exclusive recommendations and had faster data speeds than those in the 900 MHz bands. Due to the requirement for compatibility between diverse WLAN device makers, numerous organizations have developed wireless network standards. Many wireless technologies are in use including IEEE 802.11 and WPA. Such standards are not related to IEEE 802.11, but they are included in this section to set the scene and show how certain criteria are met by IEEE 802.11 and other standards. Examples of key existing and developing wireless network standards as well as descriptions of the basic varieties of wireless architecture are included in the list below. Wireless personal area networks are compact wireless networks with minimal infrastructure requirements (WPANs). Instead, WPANs usually use several wired devices arranged in a single location. For instance, WPANs can provide wireless keyboard and mouse interfaces with computers or offer printing services. IEEE 802.15.1, Bluetooth (Bluetooth) With wireless networks connecting tiny portable devices in mind, the WPAN standard was created. Bluetooth 2.0 can transmit data at a speed of 3 Mbps as opposed to Bluetooth's predecessor, which operated at a frequency of 2.4 GHz and had a maximum transmission rate of about 720 Kbps. The eighth standard is IEEE 802.15.3 (High-Speed Ultra-Wide Band; Wireless USB) (High-Speed Ultra-Wide Band; WI Media, Wireless USB). By utilizing a wide range of GHz frequencies, this low-cost, low-power WPAN standard prevents interference with other wireless signals. It supports various WPAN applications and can carry up to 480 Mbps across short distances.

B. *Wireless Metropolitan Area Networks (WMANs)*

Many devices, often positioned kilometers away from one another, let users connect to networks. Many WMAN installations enable wireless broadband for customers in metropolitan areas. For instance, data is transferred using the WiMAX protocol, part of the IEEE 802.16e WMAN standard. The IEEE 802.16a version permits extensive data flows with minimum disturbance. For landline connections, WiMAX provides a speed of up to 75 Mbps in a range of 30 miles. Because 75 Mbps is feasible at half a mile, significantly lower than 30 miles, there is frequently a trade-off. WWANs (Wireless Wide Area Networks) link people and things over vast, frequently global geographic regions. Satellite communication, mobile phone, and data connectivity are common uses. for WWANs. 2.2 The network and architectural elements of IEEE 802.11.

1) *Certification of Wi-Fi Alliance*

Once IEEE started looking into the security flaws with IEEE 802.11 and worked on the 802.11 amendment, the Wi-Fi Alliance created an interoperability certificate scheme for the WLAN category of products. While the IEEE worked to complete the 802.11i amendment, the 5Wi-Fi Alliance thought it was critical to develop an optimum solution that could be used with the existing IEEE 802.11 equipment. As a result, this Alliance created another Wi-Fi Protected Access called WPA, which became accessible in October 2002. The IEEE 802.11i specifications that were being proposed at the time were simply a subset of this specification. As IEEE 802.11 compatible hardware could not execute intensive encryption methods without additional hardware components, WPA does not require compatibility with AES. It is regarded as the fundamental distinction between WPA and IEEE 802.11i proposal [2].

C. *WLAN Security Issues*

Like other wireless technologies, WLANs often must satisfy several security goals. A mix of security mechanisms in the wireless Network Standard is meant to do this. The following are the most typical security objectives for WLANs: Make sure unauthorized individuals can't view communications to maintain confidentiality. Integrity is the identity of any planned or unintended interchanges to facts that arise in communication. The term Availability is ensuring people and objects can use the technology resources whenever needed. Limiting Access control refers to limiting a device or person's access to a network or its resources. The primary high-level dangers that wired and wireless LANs must face have similar security goals. The primary LAN danger categories are listed in the Table. In most WLAN attacks, the offender obtains access either between two STA's or a radio link between the STA and the AP. For some of the threats listed in the Table, the attacker must be able to intercept and inject network communication. The relative ease with which network communication can be intercepted and changed with new data from sources that can only be presumed reliable while using wireless and wired LANs. Unlike a cable LAN, where an attacker would need to physically enter the Network or remotely infiltrate its systems, a wireless LAN only requires an attacker within the WLAN infrastructure's range. The attacker may also benefit from deploying susceptible directional antennas, that may significantly increase the usable range of wireless LAN outside the designated range.

1) *History of pre-RSN IEEE 802.11 security*

Before the invention of the RSN framework and the IEEE 802.11i, the IEEE 802.11 had several significant security faults. 15 Many suppliers have incorporated proprietary features to solve security weaknesses in the standard. However, these features often need to be more compatible. As a beginning point for comprehending the rationale for RSN, this section lists the security features and flaws present before RSN. Some of these flaws include Data Integrity, Access control, authentication, encryption, replay protection, and availability for IEEE 802.11 pre-RSNs 3.2.1.

2) *Authentication and access control*

Open system and shared key authentication are the techniques described in the original IEEE 802.11 specs for verifying the identity of wireless devices attempting to enter WLAN; these procedures need to be more secure. Open system authentications are required in IEEE 802.11 implementations, but shared solid authentication is optional. In reality, open system authentication is an ineffective kind of identification verification. Indeed, STA authentication to the AP can be completed by simply providing the information below

3) The AP Service Set Identifier (SSID)

SSID serves for WLAN and it allows STA to differentiate one WLAN from another. As SSID broadcasts in the air in simple text, a listener can quickly ascertain the WLAN's SSID. Originally the SSID was not introduced as an access control feature; hence doing so is not permitted.

D. The STA's Media Access Control (MAC) address

Recognizable MAC addresses are required. A 48-bit identification number that is always connected to a particular wireless network port. Administrators can identify a list of authorized MAC addresses in various IEEE 802.11 implementations, and the AP will only permit devices with these MAC addresses to utilize WLAN. It is known as ”MAC address filtering” to do this. Despite this, it is trivial to interrupt traffic and recognize MAC addresses that are permitted behind the MAC filter because the MAC address is not encrypted. Because practically all WLAN adapters allow the MAC address to be modified, it is unfortunate that attackers can quickly get unwanted access by easily faking a MAC address. Some of these issues are also discussed in [3].

E. Area of Research

Organizations rely increasingly on data networks to link their workers, partners, and global marketplaces. The ensuing connectivity offers untold advantages, but it has also raised the possibility of being a target of cyberattacks, which may seriously disrupt business. The US has spent over $100 million in the last six months to repair damage and preserve digital assets from cyber threats and other computer network difficulties. Cyber-attacks are one of the potential vulnerabilities to national security that the US faces [4]. Many wireless network technologies are used to give digital connectivity. WLANs based on IEEE 802.11 [**?**] are the most widely used among them. Laptops, PDAs, smartphones, security cameras, parking meters, home entertainment systems, printers, and peripherals are some prominent platforms that utilize WLAN devices.

2. Related Work

A. Vulnerabilities of IEEE 802.11WLAN

The scientific community is actively attempting to increase the security of wireless networks. For diverse wireless network types, numerous cryptographic frameworks and approaches have been proposed [5], [6], [7], [8], [9], [10]. A suggested standard for wireless LAN (WLAN) MAC layer security is IEEE 802.11i [1]. The proposed IEEE 802.11s standards also recommended IEEE 802.11i for WMN security [11]. Better cryptographic services were added to IEEE 802.11i. IEEE 802.1X over Extensible Authentication Protocol (EAP) is used for AA when using a centralized authentication server such as RADIUS [12], [13], [14]. A fixed network is the normal setting for a centralized authentication server. AES uses CCMP to provide data secrecy and integrity [15]. Two passes are required for CCMP. In CCMP, the message is encrypted in counter mode with the AES algorithm.

B. Privacy Issue with Wired (WEP)

The first security feature included in the IEEE 802.11 standard to reduce the danger of unrestricted data exchange across a broadcast channel is WEP. Self-synchronization may result in individual data frame loss without requiring re-initialization [16]. According to Jesse Walker, a Network Security Architect for Intel Platform Networking Group [17], the primary issue with WEP is that it recycles a 24-bit initialization vector (IV), which is used to generate a secret key by combining it with a pseudorandom number. It is simple to decrypt the remaining portion of the cipher because the IV is comparatively short and transmitted in its purest form as part of the MAC layer protocol of each data frame [30]. Groups of similar frames are gathered so that an adequate amount of connected data (e.g., TCP exchanges with identical format fields for each frame) may be analyzed to solve the puzzle. This method is used by the majority of WEP cracking tools, most notably Air Snort (available at www.snort.org).

1) Beacon Frames and Service Set Identifiers (SSID) Problems

WLAN Access Points (APs) and Stations (STAs) frequently send stay-alive frames to create and sustain connections inside their Basic Service Set (BSS). It's a frequent misconception that an open system can also offer some degree of security by simply omitting the network's SSID from the AP's beacon frames, discontinuing to broadcast beacon frames, or even ordering the AP to reject all STA probe signals expressly intended to its SSID.

2) MAC ACL Problems (ACL)

Similar to traditional LAN, the WLAN can utilize ACL to identify a set of users who are allowed access to the network. If the STA's MAC address is not included in the ACL of the particular AP it is attempting to connect to, the connection will be declined. When compared to wired LANs, an access point's ACL must take into account both the client's MAC address and the SSID. The two components of WLAN MAC ACLs are particularly prone to MAC-related spoofing because they are passed without visibility. The SSID of the access point may be easily determined, as was already mentioned, and doing so also makes it feasible to know the MAC addresses of permitted users.

3) Weaknesses in Authentication Schemes

To authenticate wired and wireless LAN deployments, IEEE created the 802.1X standard [1]. In Fig.1, the authentication procedure is depicted. The Mobile Unit (MU) uses the AP to send an authentication request in the first phase. The AP synchronizes and answers probe requests, but it postpones connection authentication until server authentication is finished. The second step enables multiple MUs

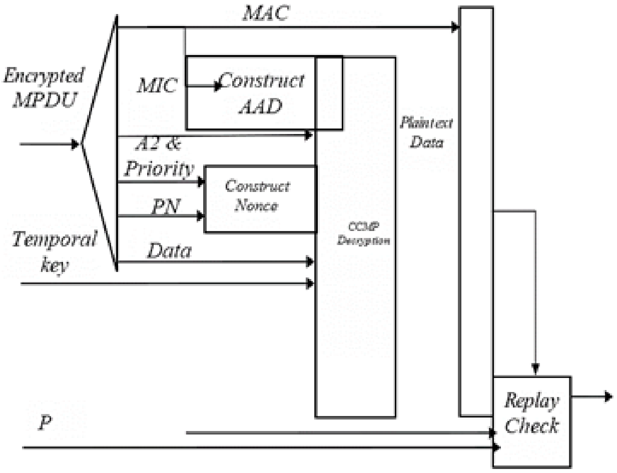


Fig 1. CCMP Decapsulation Block Diagram

Figure 1. CCMP Decapsulation Block Diagram

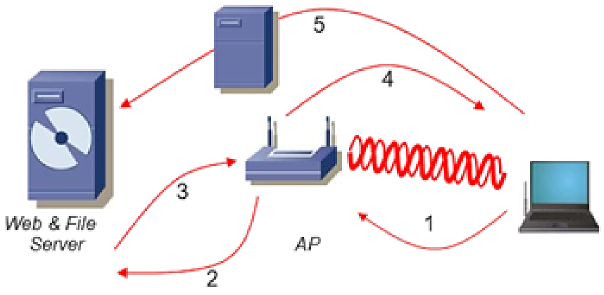


Fig 2. IEEE 802.1X Authentication

Figure 2. IEEE 802.1X Authentication

to share a single authentication database by having the AP pass the MU's encrypted credentials to an Authentication Server (AS) like RADIUS.

4) Authentication Server

In the fourth stage, the AP port is activated, encrypted WEP keys are exchanged, and the connection to the AP is complete. MU is finally given access to the main network and file servers in the final step. The 802.1X specification has two significant flaws. The database of critical authentication is housed in a single location, which makes the WLAN susceptible if it were to be compromised. The second is that it only provides comprehensive network protection by addressing the issue of station authentication [18]. As WEP is used to encrypt the frames being broadcasted and received, an 802.11x WLAN will experience confidentiality problems as a regular WLAN when used alone as shown in Fig 2.

C. CCMP Security Mechanism

To address WEP's security weaknesses, the IEEE developed 802.11i and integrated it into the IEEE 802.11-2007 standard (described in Part 2.3). 802.11i enhances WLAN security by offering authentication, data integrity, and secrecy services. 802.11i employs IEEE 802.1X to authenticate nodes [12]. Data security is guaranteed via WEP, TKIP, or CCMP. CCMP employs the block cipher algorithm of the AES in counter mode [19]. To provide data confidentiality, block ciphers are used in counter mode with steam generators. The beginning counter is first encrypted then XOR with the plaintext in counter mode to generate the ciphertext [20]. Contrarily, CBC-MAC provides message integrity. It is recommended to use a separate temporary key for each CCMP session. It is recommended to employ a different nonce value for each frame and to create a unique nonce value using a 48-bit packet number [1]. MAC layer packet data units contain MAC headers, CCMP headers, FCS fields, encrypted payloads, and encrypted MICs (MPDUs).
While calculating for retransmission, any additional authentication data and packet header fields that can change during the transmission are disguised as 0. A Nonce block is created in the third stage by combining the packet number, source address, and priority field. This priority field value is initialized to 0. In the fourth stage, the 8-octet CCMP header is updated with the new Packet Number and key identifier. Fifth phase: formation of the ciphertext and MIC. An encrypted MPDU is then produced. Following receipt of the encrypted MPDU, CCMP follows the steps in Fig. 2. [1] to complete the task. The AAD and nonce values are first taken out of the encrypted MPDU. The encrypted MPDU is parsed to obtain these values. The MPDU header is where the AAD is found. The nonce is made up of the priority field, A2, and PN. MIC is also gathered to perform integrity checks. The CCMP decryption method recovers MPDU data in plaintext format and checks the accuracy of packet plaintext data and other authentication data using TK, MIC, other authentication data, nonce, and packet encrypted text data. The MPDU plaintext and the received MPDU header are then merged to produce the plaintext as shown in Fig. 3. It is demonstrated in our study [21] that CCMP is susceptible to TMTO attack because of the counter's known beginning value. As a result, the AES algorithm's security level (key length: 128) in counter mode is less robust than what is advised for block ciphers [22]. In Chapter 3 [21], a description of this proof is provided.

D. Handover in Networks with low mobility

The Mobile IP protocol is established in Reference [1] to simplify network layer forwarding. A mobile node can have a care-of address in addition to its home address thanks to this protocol. Datagram delivery in various subnets is made possible by tunneling between domestic and foreign agents. A new IPv6 protocol and a choice for IPv6 mobility support are also defined in Reference [12], enabling a mobile node to directly accept packets through its care-of address. Reference [23] studies the handover of a mobile node in

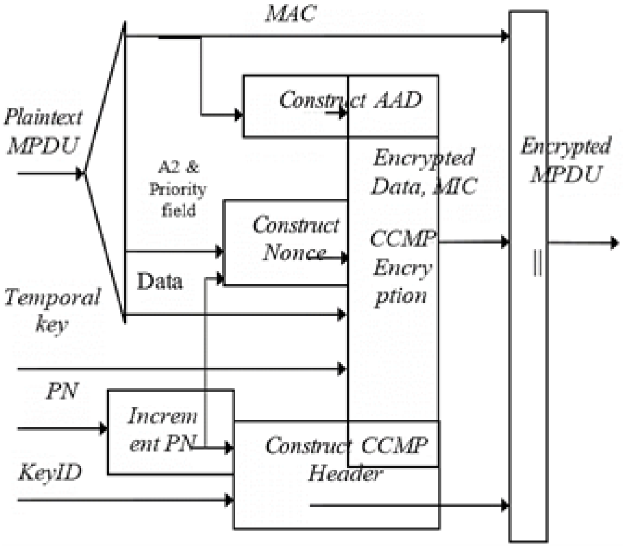


Figure 3. (CCMP) Encapsulation BDiagram

a mixed IPv4/IPv6 environment and presents a handover strategy for various conditions to facilitate handover in hybrid networks

1) Delivery in VANETs

There have been many different methods for seamless transfer. As an illustration, Reference [7] combines NEMO with VANET to ensure seamless handover across various access points. To quickly configure the new access point to the vehicle's requirements and reduce handover delay, the vehicle can aid other cars in obtaining information about the new access point when the changeover is approaching. To encourage scalability and reliability, some studies partition VANETs into various clusters. The addition of a cluster head to each cluster in clustered VANETs optimizes handover not only between various APs but also across various clusters [8]. A change in cluster head between base stations is not handled during the handover. To lessen the impact of TCP connection interruptions on network performance during the changeover process, it enables the vehicle to actively disconnect and reconnect TCP communication when a handover occurs between RSUs. Although this design considers the performance of the transport layer, there are still link breaks during the handover process.

E. Proposed SDN-based VANET architecture

We manage automotive networks using a two-tier SDN controller architecture. Tier 1 consists of a central SDN controller connected to the main network. Tier 1 could only cluster when necessary and with a broad perspective of the network. In Tier 2 base stations, SDN controllers and MEC servers are added, which proactively store data to minimize packet loss during forwarding. Two types of wireless spectrum are used to create a wireless network. It uses the IEEE 802.11p network architecture for car-to-automobile communication to provide extremely high records transmission costs in a mobile setting. Additionally, to provide long-distance wireless connectivity, a mobile network (such as an LTE or 5G network) is necessary for communication between the vehicle and the base station [37]. Using unlicensed airwaves, IEEE 802.11p-based VANETs enable vehicle-to-everything communication. An automobile can connect to the Internet directly using a cellular network or indirectly through another connected vehicle. Through the provision of communication services over the mobile network, vehicles with mobile connections serve as gateways in VANETs.

F. SDN-based handover process

During inter-cluster handovers, the vehicle's network address must be updated to reflect the altered traffic flow [24]. As the connection is recognized by the network address and port in this case, the transport layer service connection is dropped and then picked back up. Therefore, the congestion window constraint may result in a loss in network performance during a switchover. We use SDN to maintain the transport layer connection and conduct a smooth handover to prevent this scenario. SDN is superior to conventional techniques in terms of network scalability and transmission efficiency since it may provide a mechanism for efficiently allocating and managing a network [3]. These benefits may help to handle problems like node mobility, dynamic network features, and big network scale. The newly accessible vehicle will receive a mapping and dampening command from the SDN controller. When it comes to packet address mapping, the CH is in charge of overseeing vehicle access to the cluster.

G. Programming Interface (API)

The experiment was designed to demonstrate how a thorough knowledge of the network, in conjunction with data from the cloud, helps us to better govern network behavior and, ultimately, deliver a service with greater performance. This paper does not consider the implementation of MEC technology, which is the core element of our proposed system. This system's main objectives were network management and application layer flexibility, whereas our suggested structure's main objectives were traffic management and enhancing routing effectiveness by including SDN-managed MEC servers. Research on this topic has also been done by a working group from Nanyang Technological University in Singapore's School of Electrical and Electronic Engineering [18]. This technique utilized the current mobile network architecture in addition to management based on SDN technologies.

3. Methodology

A. Reconstruction of Nonce

In this section, the CCMP a description of the packet header was covered. There are three fields in the CCMP nonce block. These fields are the packet number (PN) field, the address field (MAC field of the A2 header), and the priority field (set to ”0” by default), as illustrated below in Eq. 3-1. Address (A2) — Packet Number (PN) = none

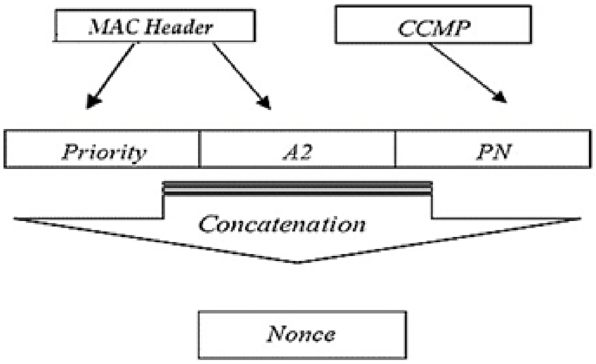


Figure 4. Nonce Reconstruction Scheme

— Priority field (3-1) The opponent might reconstruct the nonce because of how it was built.
The 802.11 MPDUs are easily sniffed in the situation of unbounded wireless communications. The MAC and CCMP headers are passed in plain text and at a fixed point inside the MPDU, so once the MPDU has been sniffed, they may be acquired. The hacker might then extract the A2 addresses and priority data from the MAC header to verify the pre-computed nonces. Now, to rebuild the nonce, only knowledge of the PN field is required. It is already loaded and possible to access the CCMP header in plain text. Therefore, the nonce can be precomputed and confirmed as illustrated in Fig. 4.

B. Reconstruction of Initial Counter

AES block cipher in counter mode is used for encrypting the payload and message integrity code (MIC). In the first step, the counter value (Ctr_i) is encrypted to produce output in the form of key-stream blocks (Si) as shown in Table 1.

The field after the counter block is the nonce field. The composition and reconstruction of the nonce field are covered in Section 3.2. Each input string's bit length—both the once and the payload—is a precise multiple of 8-bit [25]. The lengths of the nonce and payload are represented by the integer variables "n" and "p," respectively (in octets). "Q" denotes the length of the payload (measured in octets). The first block of data contains the octet string "Q." "q" denotes the length of "Q" (in octets). "Q" is, therefore, equal to [p] 8q. Only the length of the payload is required to determine the value of the counter block after addressing the reconstruction of the nonce and the status of the flag field as a constant known value. An 802.11 MPDU has a maximum payload length of 2312 bytes.

C. (TMTO) Precumputation Atack

Sections 3.2 and 3.3 described the precomputation of the MAC header's A2 Address field, Priority field, Packet Number field, and Payload field length. The initial counter can be calculated in advance using these values. This obtained counter value allows the hacker to launch a TMTO attack [21]. TMTO attack stands for brute force / exhaustive key search attack [26]. TMTO is a compromise between increased storage requirements and reduced computing power. In a TMTO attack, the hacker creates a large table of pre-calculated data before launching the actual attack on the cipher. Then during the actual phase, using pre-computed data tables, an offensive is launched on many different cryptographic keys. A very important feature of the TMTO attack is that it does not need to have a priori knowledge of the plain text when preparing precomputed data tables. In addition, TMTO also takes a hint from error-correcting code techniques and is effective even when there is uncertainty in the plaintext [27]. The significance of the TMTO attack can be judged by the important role it played in breaking the A5/1 cryptographic algorithm [28]. Sometimes a cryptographic system is considered broken even if partial key information is obtained by a hacker [22]. The importance of pre-calculation attacks is much more pronounced in these cases. The more data available, the greater the chance of a successful precomputation attack. Thus, creating a suitable attack scenario in which sufficient data is available is extremely important. In 802.11, Throughout the same session, the CCMP counter increases monotonically. The fact that there is no maximum for the number of MPDUs that can be used in a single session is also intriguing. Consequently, there is enough information accessible to start an effective TMTO precomputation attack. After the collapse of WEP, the CCMP protocol was used to provide confidentiality, and messages For IEEE WLANs, integrity, and authentication services are provided. Data is generally encrypted via the AES block cipher in counter mode. The Packet Number field, the A2 Address field, the Priority field, and the Payload Length field make up the counter value. This study demonstrates the CCMP protocol's susceptibility to the TMTO pre-calculation attack [21]. Following the completion of this work, a strong security framework is suggested to defend IEEE WLANs from potential attacks made before TMTO computation.

D. Proposed Security Mechanism to Defend TMTO Attack

The Temporal Memory Trade Off (TMTO) attack could be employed against CCMP, according to our earlier research [21]. We continued to work on this problem and made a strong per-packet security recommendation for the next wireless LAN implementations [29] to fix it. The Per-Packet security mechanism's architecture includes Secret Nonce and Per-Packet authentication. The challenge-response procedure used by the packet-based authentication system under development lasts for a whole session. To safeguard the connection from a Denial-of-Service attack, if per-packet authentication fails, the Per-Packet challenge-response method immediately drops the packet. The session key should be used to generate the Nonce, which should be kept secure. Due to its exclusivity and secrecy, the nonce delivers novelty and unpredictability. Freshness defends against replay attacks, and the Nonce's unpredictable character deters pre-computational assaults. The remainder of the chapter talks about the proposed packet authentication

TABLE I. Format of Counter Blocks

Octet Number	0	1. . . .15-q	16-q. . . 15
Contents	Flags	Nonce	$[i]_{8q}$

system's features, benefits, and how it circumvents the MIC requirement.

E. Proposed Per-Packet Authentication Mechanism

The pair-wise key hierarchy uses pseudo-random functions (PRFs) to extract session-specific keys from the pairwise master key (PMK) [1]. The PMK is accessible through a successful IEEE 802.1X exchange, a pre-shared key (PSK), or a cached PMK obtained in another way. PMK has a bit size of 256. The pair-wise key hierarchy uses the PMK to produce a pairwise transitional key (PTK). The PTK also produces a Temporary Key (TK). This key is thus the shared encryption key utilized in AES counter mode to encode the MIC and the data. To obtain the counter's initial value from the time key, we advise using PRF-128 as described as a pseudorandom function that outputs 128 bits in clause 8.5.1.1 [1]. The suggested method for setting the counter's initial value is shown in Fig. 4 [29]. The TK and the start value of the counter will be utilized to encrypt the first packet sent from the authenticator to the supplicant. The authenticator encrypts the data, MIC, and N0 following Eq. 4-1 [29]. (Nonce value). N0 will be produced by PRF as a 48-bit value.

F. Robustness Against Attacks

The suggested per-packet authentication technique is examined in this section for several types of attacks, including MAC spoofing, replay attacks, pre-computation attacks, and denial of service assaults [29]. Under several attack scenarios, the suggested protocol's effectiveness is evaluated.

1) MAC Spoofing

We assume this location has a rogue station. In addition, we assume that the malicious station will be effective in sniffing, decoding, and analyzing the wireless packet to determine the MAC address of the authorized station. We further assume that the malicious packet was created by the rogue station and that its MAC header was present in it. The AP immediately decrypts the packet it just received because the CBC-MAC mechanism is no longer in place. A middle key is used to unlock the packet. The nonce, N0, that the AP sent to the STA is included in the packet. Each nonce and its associated STA MAC address are stored in a table by the AP. If N0, the nonce that the AP earlier provided to the STA with the MAC address in the MPDU, is not received by the STA It tosses the packet after inspecting the decoded packet. The AP immediately ceases the MAC spoofing83 assault as a result.

2) Replay Attack

The decryption on the receiving side of the AP would represent the prior nonce and not the current one in the case of repeated attacks by a rogue station. The AP always anticipates the most recent packet since the nonce in each packet is distinct. If an invalid nonce is received, the packet is dropped. The replay attack is therefore successfully stopped by the continuous challenge-response system. To distinguish between a legitimate, retry packet and an illegal retry packet, we suggested adding a retry bit to the associated data field, which is concatenated with the payload.

3) Denial of Service Attack

Any attempt to degrade resources may be made by sending an excessive number of invalid packets or by attempting to gain unauthorized access to services, to name just two examples. In the case of CBC-MAC processing, the data is gathered first, followed by the generation, verification, and decryption of the MIC and the ciphertext. With our protocol, decryption comes first, and a packet is deleted if it is not up to date. If an attacker supplied packets by altering the packet number to a future packet number, CBC-MAC would proceed with the whole MIC verification process. We save bandwidth since the 48-bit plaintext packet number is not concatenated with each transmission as in the case of CCMP, even though we must decode each packet to check the currency nonce. Therefore, we are not required to figure out the MIC for every packet.

4) Pre-Computation Attack

Precomputation by an imaginary adversary can weaken the CCMP encryption key, as we demonstrated in Chapter 3 via a time-memory trade-off approach [21]. The packet number was transmitted over the air in plaintext, making this precomputation attack possible [21]. Additionally, the adversary may be able to forecast the counter value. The nonce is transmitted in encrypted form using the specified method [29], and no counter value component is visible in clear text to an unauthorized station. This renders the enemy's ability to make plans difficult.

5) Per-Packet Authentication Mechanism –Benefits

The current CCMPs give each packet freshness, but it is predictable. The protocol is susceptible to a precomputation attack because of how predictable the nonce is. The per-packet security method that is being presented offers a secret nonce-based per-packet authentication technique. It is demonstrated that the nonce is created from the session key and kept private. The challenge text from the verifier to the requester also uses the same nonce.

4. Results and Discussion

The use of wireless networks is commonplace worldwide. The ease and speed of installation, affordable equipment, scalable network, lack of significant building alterations and extensions, and appeal of wireless connectivity

all contribute to the widespread use of wireless networks.
WLANs based on IEE 802.11 are widely used, much like all wireless networking protocols. Ones that use WLAN devices frequently include laptops, PDAs, smartphones, security cameras, parking meters, home entertainment systems, printers, and peripherals. Moreover, the IEE 802.11s Working Group is aiming to convert single-hop WLANs to multi-hop WMNs. The WLAN market and application space are expanded by the WMN standard. Wireless campus networks and community networks are examples of WMN applications (hot zones).
Wireless network signals, in contrast to wired network signals, are present in the air in ranges corresponding to their frequencies and power and can be picked up by anyone nearby. The ability to achieve sufficient throughput at the needed ranges is also constrained by wireless frequency. Similar to how interference in the air has a detrimental impact on signal quality. As a result, security and quality of service are difficult issues on which much of the research for wireless networks has been concentrated.

A. SIMULATION RESULTS

This section compares the simulation findings for the latency caused by the security mechanism used in IEEE 802.11i's CCMP and the planned CIPGY back challenge-response protocol. The Quadlet simulator was used to run the simulations (the source code is given in Appendix I of this dissertation). Keep in mind that delay-sensitive applications like network gaming, IP telephony, and video conferencing require attention to latency. We employed a straightforward chain architecture with source and destination nodes situated at the chain's two endpoints to examine how security provisioning affected latency. This WMN architectural model was used for our simulation to examine the outcomes of data traversal over numerous nodes following successful mutual authentication and confidentiality between source and destination nodes. In our approach, source and destination nodes are separate devices that communicate with other nodes in the network utilizing mesh services. In our concept, WMN router nodes serve as access points for clients and forward traffic to nearby nodes. Direct connections to the Internet are made through wire gates (G in Fig. 5.4). Because router nodes are static, topologies are generally stable and only sometimes change as a result of nodes joining or leaving. Client nodes can connect to the mesh network using a few of the routers' additional functions as access points.
In both methods, we noticed how adding more intermediate hops affected the time between endpoints. In the beginning, we looked into the latency caused by a hop distance between two nodes. The latency over a two-hop distance was then measured, and the number of intermediate hops was then increased in both approaches. The results of the simulation are shown in Fig. 5. Note. Figure 5 is a proposed framework (CCMP) in end-to-end delay as a function of the number of nodes in the chai

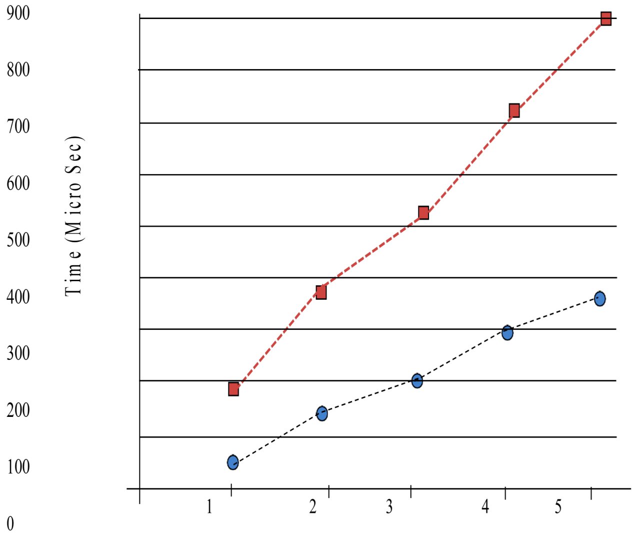


Figure 5. Simulation Results

B. NUMBER OF HOPS

The findings show that in terms of induced delay, the proposed coupled system challenge-response protocol greatly beats CCMP. When compared to CCMP, the proposed protocol's one-hop latency is less than half as great. The reduction in latency is extra noticeable. Increase the wide variety of hops in between. Because counter-mode AES [3] and the proposed per-packet security mechanism can process messages more quickly than the ”counter-mode AES with the Cipher Block Chaining of Messages” (CCM) [15] authentication code used in CCMP, the proposed challenge-response piggyback protocol exhibits improved performance in the presence of robust security.

C. SUMMARY OF RESULTS – PROPOSED SECURITY MECHANISM

The network is successfully shielded from passive traffic analysis by the proposed security framework, and malicious nodes are prevented from initiating several attacks, such as MAC spoofing attacks, replay attacks, pre-computation attacks, and partial matching attacks. In addition to thwarting assaults, the suggested security mechanism decreases the 64-bit CCMP header overhead, the 64-bit MIC field overhead on the MPDU, and the delay-sensitive real-time quality of service. It also saves computational resources used for MIC calculation at the receiving end. apps for multimedia like video on demand and voice over IP. Table 4.1 lists the benefits of the suggested security technique over the current system.

5. CONCLUSION

This paper suggests a thorough architecture of wireless mesh networks that combines enhanced security and quick response time. The architecture makes use of a cutting-edge hop-by-hop challenge-response mechanism to guarantee data integrity and confidentiality at the MAC layer. Using 802.1X via EAP, the initial trust framework, key distribution, and node authentication are carried out. Moreover, it is discovered that hop-by-hop security is insufficient to thwart a self-centered and corrupted node. The scheme also implements data confidentiality between endpoints and data integrity at the network layer. Our framework is also proven to be robust against a wide variety of security breaches, including passive eavesdropping, MAC spoofing, replay, and pre-computation attacks. Finally, the simulation results showed that the latency induced by security services in our framework is significantly lower than the latency observed in CCM. In short, a continuous challenge-response mechanism is used in the proposed packet-based authentication protocol to safeguard the connection from pre-computational and Denial of Service assaults during the session [30].

6. Future Scope

The proposed security framework needs to be tested on diverse security environments, quantum-safe security measures, and similar. This could involve collaboration with industry partners or conducting field trials to assess the framework's performance, scalability, and effectiveness in diverse environments. There is also a need to continuously update the security framework to align with new revisions of the IEEE 802.11 standard. As wireless networking standards evolve, ensure that the security mechanisms remain relevant and effective, addressing new vulnerabilities and requirements introduced by updated standards.

References

[1] E. K. S. Au, "Ieee 802.11be: Extremely high throughput [standards]," *IEEE Vehicular Technology Magazine*, 2019. [Online]. Available: https://api.semanticscholar.org/CorpusID:202098736

[2] A. K. Yadav, M. K. Misra, P. K. Pandey, K. Kaur, S. Garg, and M. Liyanage, "Lemap: A lightweight eap based mutual authentication protocol for ieee 802.11 wlan," *ICC 2022 - IEEE International Conference on Communications*, pp. 692–697, 2022. [Online]. Available: https://api.semanticscholar.org/CorpusID:251522892

[3] S. K. Memon, K. Nisar, M. H. A. Hijazi, B. S. Chowdhry, A. H. Sodhro, S. Pirbhulal, and J. J. Rodrigues, "A survey on 802.11 mac industrial standards, architecture, security & supporting emergency traffic: Future directions," *J. Ind. Inf. Integr.*, vol. 24, p. 100225, 2021. [Online]. Available: https://api.semanticscholar.org/CorpusID:244842201

[4] K. Shafique, B. A. Khawaja, F. Sabir, S. Qazi, and M. Mustaqim, "Internet of things (iot) for next-generation smart systems: A review of current challenges, future trends and prospects for emerging 5g-iot scenarios," *IEEE Access*, vol. 8, pp. 23 022–23 040, 2020. [Online]. Available: https://api.semanticscholar.org/CorpusID:211058102

[5] K. Kosek-Szott, "A throughput model of ieee 802.11aa intra-access category prioritization," *Wireless Personal Communications*, vol. 71, pp. 1075 – 1083, 2012. [Online]. Available: https://api.semanticscholar.org/CorpusID:6023395

[6] R. Costa, P. Portugal, F. Vasques, C. B. Montez, and R. de Moraes, "Limitations of the ieee 802.11 dcf, pcf, edca and hcca to handle real-time traffic," *2015 IEEE 13th International Conference on Industrial Informatics (INDIN)*, pp. 931–936, 2015. [Online]. Available: https://api.semanticscholar.org/CorpusID:458455

[7] H. Altunbasak and H. Owen, "Alternative pair-wise key exchange protocols for robust security networks (ieee 802.11i) in wireless lans," *IEEE SoutheastCon, 2004. Proceedings.*, pp. 77–83, 2004. [Online]. Available: https://api.semanticscholar.org/CorpusID:14516902

[8] G. Anderson, L. F. Urbano, G. Naik, D. J. Dorsey, A. Mroczkowski, D. Artz, N. Morizio, A. Burnheimer, K. Malfettone, D. Lapadat, E. A. Sultanik, S. Garcia, M. Peysakhov, W. C. Regli, and M. Kam, "A secure wireless agent-based testbed," *Second IEEE International Information Assurance Workshop, 2004. Proceedings.*, pp. 19–32, 2004. [Online]. Available: https://api.semanticscholar.org/CorpusID:952163

[9] "Ieee standard for information technology–telecommunications and information exchange between systems - local and metropolitan area networks–specific requirements - part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications - redline," *IEEE Std 802.11-2020 (Revision of IEEE Std 802.11-2016) - Redline*, pp. 1–7524, 2021. [Online]. Available: https://api.semanticscholar.org/CorpusID:252590949

[10] N. Borisov, I. Goldberg, and D. A. Wagner, "Intercepting mobile communications: the insecurity of 802.11," in *ACM/IEEE International Conference on Mobile Computing and Networking*, 2001.

[11] N. Finn, "Introduction to time-sensitive networking," *IEEE Communications Standards Magazine*, vol. 6, pp. 8–13, 2022. [Online]. Available: https://api.semanticscholar.org/CorpusID:51704314

[12] A. Mildner, "Time sensitive networking for wireless networks-a state of the art analysis," 2019.

[13] "Ieee standard for information technology–telecommunications and information exchange between systems - local and metropolitan area networks–specific requirements - part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications - redline," *IEEE Std 802.11-2020 (Revision of IEEE Std 802.11-2016) - Redline*, pp. 1–7524, 2021. [Online]. Available: https://api.semanticscholar.org/CorpusID:252590949

[14] J. Zheng and Lee, "Top articles," 2005.

[15] X. Wang, "Top articles," 2006.

[16] M. Junaid, M. Akbar, and M. Mufti, "Per packet authentication for ieee 802.11 wireless lan," *2008 IEEE International Multitopic Conference*, pp. 207–212, 2008. [Online]. Available: https://api.semanticscholar.org/CorpusID:24813826

[17] M. S. Ibrahim, A. M. M. Hussain, and N. Sidiropoulos, "A novel linear precoder design for reliable ul/dl detection in tdd cellular networks," *IEEE Transactions on Communications*, vol. 70, pp. 8167–8180, 2022. [Online]. Available: https://api.semanticscholar.org/CorpusID:253347600

[18] M. U. Ilyas, M. Mufti, R. Iqbal, M. J. Hussain, and S. S. Kanhere, "Indict: Intruder detection, identification, containment and termination," *2006 International Conference on Computing*

& *Informatics*, pp. 1–8, 2006. [Online]. Available: https://api.semanticscholar.org/CorpusID:14849554

[19] S. L. Keoh and E. C. Lupu, "Towards flexible credential verification in mobile ad-hoc networks," in *Principles of Mobile Computing*, 2002.

[20] X. Cheng, W. Li, T. Znati, and systems Wireless algorithms, "Wireless algorithms, systems, and applications, first international conference, wasa 2006, xi'an, china, august 15-17, 2006, proceedings," in *Wireless Algorithms, Systems, and Applications*, 2006.

[21] X. Wei, X. W. LITH-ISY-EX, and G. C. Liu, "Analysis of quality of service of wireless lan for ieee 802 . 11 e information networks," 2004.

[22] C. Chigan, L. Li, and Y. Ye, "Resource-aware self-adaptive security provisioning in mobile ad hoc networks," *IEEE Wireless Communications and Networking Conference, 2005*, vol. 4, pp. 2118–2124 Vol. 4, 2005. [Online]. Available: https://api.semanticscholar.org/CorpusID:3167521

[23] A. de la Oliva, P. Serrano, P. Salvador, and A. Banchs, "Performance evaluation of the ieee 802.11aa multicast mechanisms for video streaming," *2013 IEEE 14th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM)*, pp. 1–9, 2013. [Online]. Available: https://api.semanticscholar.org/CorpusID:3007543

[24] B. Aboba, L. J. Blunk, J. R. Vollbrecht, J. Carlson, and H. Levkowetz, "Extensible authentication protocol (eap)," *RFC*, vol. 3748, pp. 1–67, 2004. [Online]. Available: https://api.semanticscholar.org/CorpusID:26413732

[25] T. S. Messerges, J. Cukier, T. A. M. Kevenaar, L. Puhl, R. Struik, and E. Callaway, "A security design for a general purpose, self-organizing, multihop ad hoc wireless network," in *ACM Workshop on Security of ad hoc and Sensor Networks*, 2003.

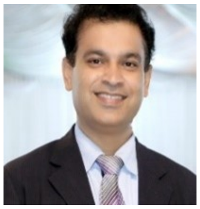
[26] J. Allen and J. Wilson, "Securing a wireless network," in *Conference on User Services*, 2002.

[27] K. Ren, W. Lou, and Y. Zhang, "Leds: Providing location-aware end-to-end data security in wireless sensor networks," *Proceedings IEEE INFOCOM 2006. 25TH IEEE International Conference on Computer Communications*, pp. 1–12, 2006. [Online]. Available: https://api.semanticscholar.org/CorpusID:5890157

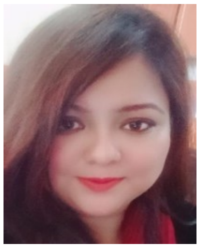
[28] F. Ullah, T. Mehmood, M. Habib, M. Ibrahim, S. Zulfikar, and A. Bhutto, "Spins: Security protocols for sensor networks," 2011.

[29] B. Bellalta, L. Bononi, R. Bruno, and A. Kassler, "Next generation ieee 802.11 wireless local area networks: Current status, future directions and open challenges," *Comput. Commun.*, vol. 75, pp. 1–25, 2016. [Online]. Available: https://api.semanticscholar.org/CorpusID:13140229

[30] A. Sujanani and S. Pai, "802.11 frame-level network ids for public wireless networks," *Advances in Intelligent Systems and Computing*, 2020. [Online]. Available: https://api.semanticscholar.org/CorpusID:230561622



Inam ul Haq (M'1979) was born in Okara Pakistan. The author received an MS Computer Science degree from Blekinge Institute of Technology Sweden in 2013 and is now a PhD Scholar from Superior University Lahore. He is currently working as an Assistant Professor at the University of Okara from 2005 to date. His research interests include Artificial Intelligence, Machine Learning, Image Processing, Healthcare and Wellness. He has published 08 research papers as a Principal Author in international journals/conferences. Inam is a member of IEEE, ACM, Parkinson's Disease Foundation, Movement Disorder Society, IEEE Sensors Council, IEEE Electronic Design Automation Council, IEEE Nanotechnology Council, IEEE Biometric Council, IEEE Education Society & IEEE Young Professionals, IEEE Collabratec, and many others.



Amna Nadeem (F'1989) is born in Okara Pakistan. The author received an MSc in IT from Punjab University College of Information and Technology Lahore in 2013 and an MS Computer Science degree from Lahore Leads University in 2016. Now she has enrolled as a PhD Student at Superior University Lahore. She is currently working as a Lecturer at Lahore Garrison University from 2022 to date. Her research interests include Artificial Intelligence, Machine Learning, Image Processing, and Cloud Computing. She has published 03 research papers as a Co-author Author in international journals and conferences.

Saba Ramzan (F,1993) is a highly accomplished computer scientist and researcher, with a MS degree in Computer Science and currently pursuing a Doctor of Philosophy (PhD) in the same field. Her research interests lie in the areas of artificial intelligence, machine learning, and computer vision. Saba completed her MS in Computer Science from a top university, where she worked on various research projects related to Machine learning and artificial intelligence. Her research was well-received and recognized by the academic community, leading to several publications in high-impact peer-reviewed journals and presentations at top conferences.

Nazir Ahmad (M'1995) was born in OKARA Pakistan. The author has received MS COMPUTER SCIENCE degree from University of OKARA, and now a MS Scholar from University OF Okara. He is currently working as IT MANAGER IN POLICE Department GOVT of Punjab. His research interests include Artificial Intelligence, Image Processing, Machine Learning and Networking.

Yasir Ahmed (M'1994) was born in Pattoki Pakistan. The author has received MSC Information Technology degree from University of Central Punjab Lahore in 2020, and now a MS Scholar from University OF Okara. He is currently working as a FWA in Population Welfare Department GOVT of Punjab from 2015 to till date. His research interests include Artificial Intelligence, Machine Learning, Image Processing and Networking. Now he has interest to publish a research paper in the Area of Networking.