Wireless Networks (2020) 26:4657–4675
https://doi.org/10.1007/s11276-020-02368-2

Prediction-based secured handover authentication for mobile cloud computing

Walid I. Khedr[1] · Khalid M. Hosny[1] · Marwa M. Khashaba[1] · Fathy A. Amer[2]

Published online: 19 May 2020

Abstract

Mobile cloud computing (MCC) is a new technology that brings cloud computing and mobile networks together. It enhances the quality of service delivered to mobile clients, network operators, and cloud providers. Security in MCC technology, particularly authentication during the handover process, is a big challenge. Current vertical handover authentication protocols encounter different problems such as undesirable delays in real-time applications, the man in the middle attack, and replay attack. In this paper, a new authentication protocol for heterogeneous IEEE 802.11/LTE-A mobile cloud networks are proposed. The proposed protocol is mainly based on the view of the 3GPP access network discovery and selection function, which uses the capacities given by the IEEE 802.11 and the 3GPP long term evolution-advanced (LTE-A) standards interconnection. A prediction scheme, with no additional load over the network, or the user is utilized to handle cloud computing issues arising during authentication in the handover process. The proposed handover authentication protocol outperformed existing protocols in terms of key confidentiality, powerful security, and efficiency which was used to reduce bandwidth consumption.

Keywords Mobile cloud computing · Handover authenticating · Prediction scheme · ANDSF

1 Introduction

The number of mobile phone users over the world exceeds six billion. Mobile Cloud Computing (MCC) is attracting a large number of users in different communities such as academia, industry, and governments where MCC serves as a method which aim to improve and deploy basic mobile phone applications. Gmail and Google Maps are examples of existing mobile applications [1–3]. Customers using cloud applications can connect to their applications using a cloud-based site through their receiver browser, which supports better capabilities with lower consumption of mobile's provider.

As users communicate through different networks, security policies differ significantly, which necessitates the development of a new vertical handover authentication mechanism. Supporting smooth roaming and confident handover in MCC is a motivated mission, due to different mobility, security needs, and Quality-of-Service (QoS) for each access network [4]. Cloud applications designed for real-time, such as media streaming and video conferencing [5] suffer from strict performance needs, such as packet loss, and end-to-end delay. These performance limitations need to be avoided in order to provide unbroken secure facilities for mobile users. Therefore, handover protocol needs to be well-designed, which means that authentication is an essential component in designing handover protocols.

The handover authentication protocol is a crucial part of communication in Mobile Wireless Networks (MWNs), where cell phones need regular safe and perfect roaming between different access points [6]. Mobile clients in wireless networks need to be re-authenticated when they are roaming a new station (Wireless Local Area Network WLAN or 4G Long Term Evolution LTE) after the handover. Once a mobile user moves from mobile networks to

✉ Khalid M. Hosny
k_hosny@yahoo.com

[1] Department of Information Technology, Faculty of Computers and Informatics, Zagazig University, Zagazig 44519, Egypt

[2] Department of Information Technology, Faculty of Computers and Informatics, Cairo University, Giza 12511, Egypt

the wireless network and vice versa, many security risks arise. This is due to the infrastructure of mobile and wireless networks such as the opening of mobile and wireless channels, the complications of both cases and the restriction of supply to radio stations. Thus, to overcome these performance restrictions and to give unbroken secure services for mobile users, a secure and well-organized handover authentication protocol represents a high need.

1.1 Background

1.1.1 Mobile cloud computing

Cloud computing is a vital paradigm designed for conveying on-demand sharing resources such as infrastructure, platform, software, etc., to client's devices like PC or cell phones, over the Internet [7]. Users can access cloud applications using an internet browser on their PC or on their cell phones or any other mobile device. Cloud applications are used to get an improved level of performance and service.

The software and data are stored on servers at unidentified distant locations, as shown in Fig. 1. MCC which is a combination of cloud and mobile networks, adds extra benefits to mobile users using all cloud computing' features and benefits in the mobile environment.

1.1.2 Handover in mobile networks

Mobile networks and WLANs are IP-based systems. The architectures of these networks are not the same, where protocol stacks; access schemes, mobility mechanisms, and service quality are different. Thus, the interconnection between these two types of networks is not simple. The Evolved Packet Core (EPC) is introduced in Release 15 [8], which characterized the interconnecting functionality between 3GPP and non-3GPP access systems. It is conceivable that you have new options for mobility using technology transfer over multiple access network systems. In addition, a trusted WLAN is provided in the EPC, facilitating a smooth transition between 3GPP and 3GPP networks, as shown in Fig. 2. Seamless handover is vital in designing progressive wireless broadband systems such as 3G and 4G. Although efforts have been performed to enhance handover latency, handover remains the most essential mobile network issue. When an MS enters into a cell boundary or suffers from dropping in signal quality in the serving station, the handover process is started. Therefore, the handover must be well designed. Otherwise, it will reduce QoS [9] dramatically. In the MCC environment, the data transfer rate changes dynamically, unlike wired networks that use a physical connection. Continuous service in mobile communications can be achieved when handover is supported from station to another seamlessly.

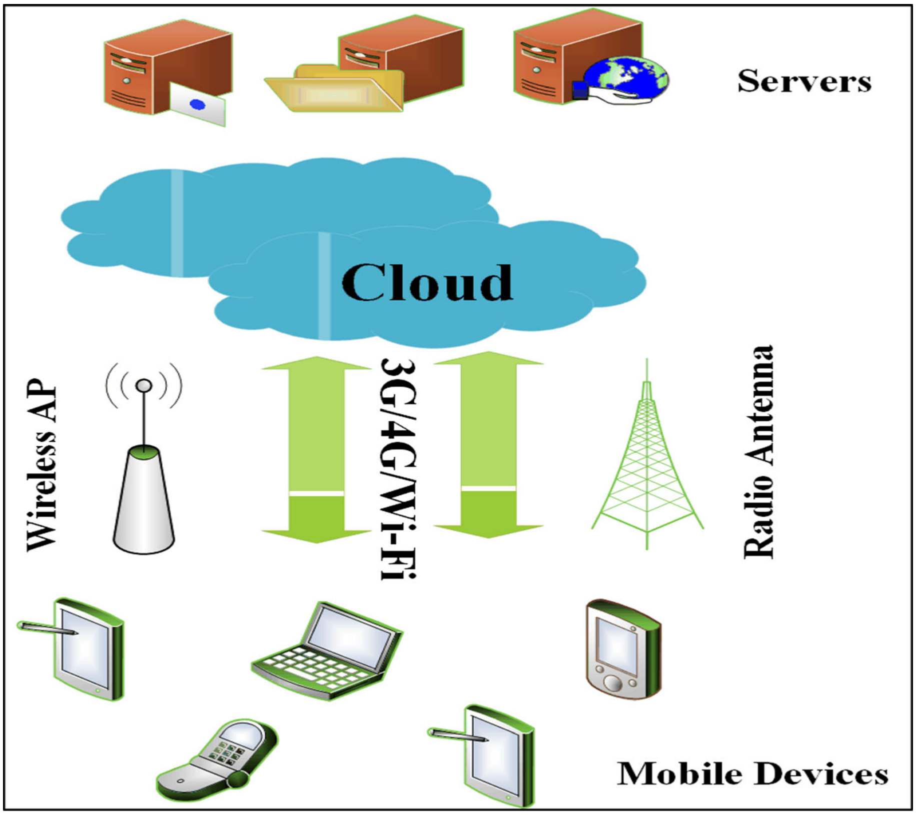


Fig. 1 An illustration for internet cloud computing

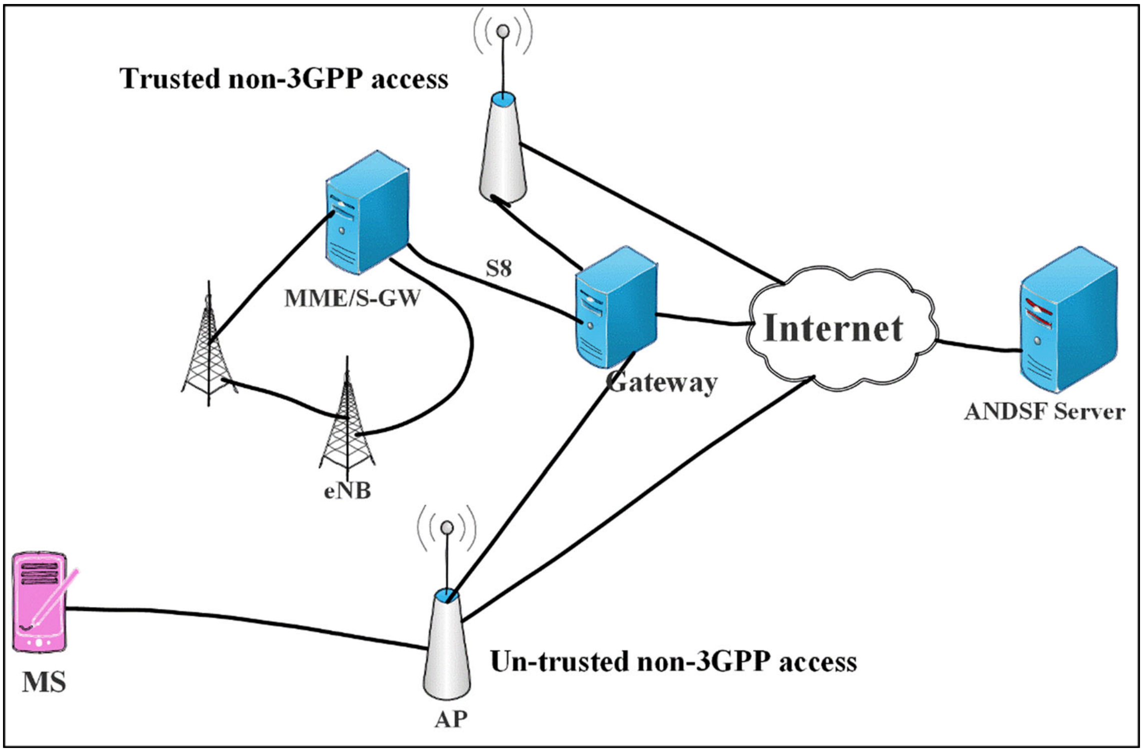


Fig. 2 LTE-WLAN interconnection

1.1.3 ANDSF overview

Evolved Packet System (EPS) [10] is designed to support many non-3GPP accesses to possess various features such as security, bandwidth, and so on. ANDSF is presented in EPS, its main function is to give information about non-3GPP networks, for example, WLAN. ANDSF provide information based on the operator's structure such as:

1. MS Location: the current location can be sent by MS to the ANDSF server, using geographical position or macro cell-ID (SSID).
2. Information about network discovery: ANDSF server sends discovery information to the MS.
3. Inter-System Mobility Policy (ISMP) and Inter-System Routing Policy (ISRP): These are a set of operators which introduce procedures for the MS.

The MS can access ANDSF using the access technologies in 3GPP or non-3GPP that are connected through the EPC, as shown in Fig. 3. ANDSF is a dynamic database restricted and managed by the operators. Mobile users have the ability to access this server to find out neighboring WLANs. Data flows are exchanged simply only after connection with WAP (Wireless Application Protocol) is set up, while the LTE connection is on all the time for the offloading situation under thought. Therefore, the connection establishment delay can be ignored. The ANDSF server may give an accessible WLANs list to the MS based on its membership, position, day time, and so on. The ANDSF Management Object (MO) provides the MS with information about authority regions, appropriate duration of time, and accessibility of networks owned by various Radio Access Technologies (RATs). TS 24.302 [8] provides additional detailed analysis concerning the ANDSF functionality. Despite the fact that the use of the ANDSF module is optional [11]. Recent studies recognize the ANDSF as a vital empowering agent for productive vertical handover decision making [12, 13].

1.2 Contributions

One of the main factors affecting handover performance in heterogeneous IEEE 802.11/LTE-A mobile cloud network, is the delay introduced by the authentication procedure when a mobile user moves between base stations (BSs). Full mobility while reducing poor QoS, is one of the biggest challenges in mobile wireless networks [14]. The re-authentication delay is the main issue of handover especially in the vertical handover, which is needed to assure secure transmission [15]. Practically, the time required to handle re-authentication is about 46% of the complete handover delay [16]. To decrease the handover latency, the re-authentication procedure must be enhanced. Therefore, many researchers are attracted to this issue. The clear lack

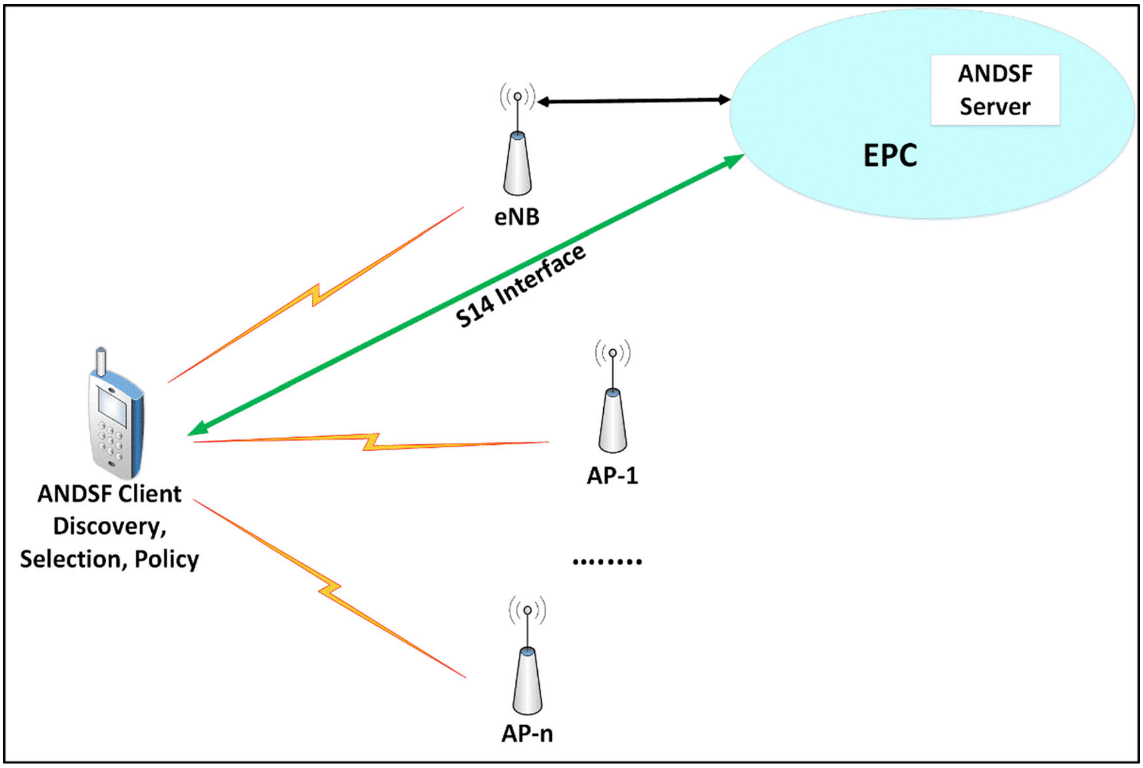


Fig. 3 ANDSF and MS interaction

of fast and secured authentication protocol in MCC motivated the authors to propose a novel predication-based handover authentication protocol for three handovers cases: Wi-Fi-to-LTE, LTE-to-trusted Wi-Fi and LTE-to-untrusted Wi-Fi handover. The handover prediction [17] is the process of determining the next station available for building a network with a Mobile Station (MS). The main contributions of the proposed protocol are:

1. Employing a handover prediction method to help MS to perform authentication for expected target stations before handover occurrence to reduce the degradation in QoS.
2. The proposed authentication protocol is based on symmetric key cryptosystem and Access Network Discovery and Selection Function (ANDSF) that achieves mutual authentication and reduces re-authentication delay, which introduces a high level of security without QoS degradation.
3. The prediction scheme is used to enhance the performance and accuracy of the proposed authentication protocol. It is used to minimize the occurrence of redundant handover and to reduce the elapsed time to establish a secure channel in case of authenticating untrusted station.

1.3 Organization of the paper

The rest of this paper is organized as follows: A brief related work of the authentication handover protocol is presented in Sect. 2. Materials and methods of the proposed protocol are presented in Sect. 3. Evaluation of the proposed scheme, simulation, and performance and security analysis are introduced in Sect. 4. Section 5 concludes the paper.

2 Related work

Many handover security protocols were introduced between 4GPP LTE and WLAN to minimize the re-authentication delays during the handover process. Broadly these protocols can be classified as symmetric encryption-based protocols and asymmetric encryption-based protocols. In most of the existing authentication protocols, there is a gap in mobile equipment as users might need to visit the authentication server and home server more than once [18, 19]. These protocols have the following limitations:

1. They needed redundant several sequences of challenge-response communications between the home subscriber (HSS) server and the MS; as a minimum of 4 messages flows. The visited server frequently

proceeds a great re-authentication delay, as it is remote from the home server.

2. A bottleneck may occur in the home server because it must be consistently associated and available.
3. According to [20], the visited server needs to connect to the home server because it can’t authenticate message flows and can’t avoid denial of service (DoS) attack.

2.1 Symmetric encryption-based protocols

He et al. [21] introduced a smart cards handover authentication protocol for wireless communications. The main advantages of the introduced protocol are (1) single registration, (2) no password/verifier table, and (3) high efficiency in password authentication. It is simple to implement for mobile users as it only performs symmetric encryption/decryption operation. However, it suffers from some weaknesses such as lack of user-friendliness, unfairness in key agreement and attacks against the user anonymity. El Bouabidi et al. [22], introduced a secure handover re-authentication protocol between WLAN networks and 3GPP LTE. This protocol achieves mutual authentication between the Universal Mobile Telecommunications System (USIM) and HSS. It can also handle appropriate security keys between MS and appropriate WLAN. The authentication delay is the main drawback of this protocol because of the different interchanging information during the authentication process.

2.2 Asymmetric encryption-based protocols

Choi et al. [23] introduced credentials based handover authentication scheme using chameleon hashing and Diffie–Hellman key exchange. The advantages of this scheme are the offered efficient authentication technique and a robust key. However, it can’t achieve user anonymity since a user always needs to send the same credential to the AP for verification. Yang et al. [24] presented a collective authentication protocol for wireless networks. This protocol depends on the group signature. It needed three message flows between the roaming server and the distant station through the handover process. Although this protocol is able to ensure user anonymity, it neglects user un-traceability. Other drawbacks of this protocol are wasting time and increasing power consumption especially if users’ number is large. He et al. [25] analyzed a roaming protocol based on a group signature with backward unlinkability [26]. Backward unlinkability experiences a high roaming authentication cost for the roaming user. It provided each roaming user with N secret keys, where N is the system parameter. As N increases, the property of backward unlinkability becomes stronger. The introduced protocol uses group signature algorithms to authenticate users anonymously. However, it involves a huge revocation cost and requires four pairing operations and consumes a large amount of communication bandwidth since the revocation values of all revoked users should always be included in the revocation list. Sharma et al. [27, 28] presented a one-pass IP Multimedia Subsystem (IMS) authentication protocol depends on Session Initiation Protocol (SIP) procedures. Although the IMS ensures safety, the proposed protocol remains vulnerable to numerous threats such as replay and man-in-the-middle attacks. He et al. [29] proposed a novel bilinear maps based handover authentication protocol named PairHand. PairHand only requires two handshakes between an MS and an AP and does not need to transmit or verify any certificate as in traditional public-key cryptosystems. The main advantage of PaiHand is its efficiency in computation and communication. However, in mutual authentication and key establishment process, it not only takes into account the possibility that the APs are not trustworthy and may leak users’ privacy-related information. Cao et al. [30] introduced a handover authentication protocol based on integrated ID-based cryptography. This protocol ensures anonymity but is still unprotected from attackers because the user identity of the MS is delivered in a plain text form when an MS needs to authenticate handover to the target station. Another advantage of this scheme is there is no third party between mobile users and the target station in the authentication process in the handover. Although it doesn’t include any pairing procedure for access in heterogeneous networks and doesn’t ensure the user’s un-traceability. Cao et al. [31] presented a straightforward handover authentication protocol based on the enhanced proxy signature. In this protocol, mutual authentication between the MS and the expected next station is straightforwardly achieved by establishing a session key with their long-term secret keys. Sithirasenan et al. [32] presented an authentication mechanism for WLANs beyond wireless technologies such as LTE and WiMAX networks. In this mechanism, a single set of authorizations is used with each network. In some network type, it is hard to implement, because it needs to modify existing network infrastructure and mobile tools considerably. Liu et al. [33] designed a time-bound anonymous protocol to authenticate handover, especially for the nearby networks. This protocol depends on the group signature beside the time information put in the signature. Therefore, normal cancellation is combined with the mandatory cancellation of the user. However, user un-traceability isn’t yet feasible. He et al. [34] introduced a new handover authentication protocol named HashHand. The security analysis and experimental results have demonstrated that HashHand not only eliminates the security vulnerabilities of PairHand without sacrificing its merits but is also more efficient and provides a key update mechanism. However, it is leading to inefficient with regard to computation cost and cannot improve the performance of PairHand and its improved version. Degefa et al. [35] proposed a Security Enhanced Authentication and Key Agreement depends on Wireless Public Key Infrastructure (WPKI). It uses Ellipse Curve Cipher (ECC) encryption to guarantee user identity security and exchanges message with limited energy consumption. Odelu et al. [36] presented an enhanced roaming protocol to address the drawbacks found in Jo et al.'s roaming protocol [37]. It achieves the session key (SK) security along with reduced computation, communication and storage costs.

The proposed authentication protocol is based on symmetric key cryptosystem and Access Network Discovery and Selection Function (ANDSF) that achieves mutual authentication and reduces re-authentication delay, which introduces a high level of security without QoS degradation caused by public-key encryption.

3 The proposed vertical handover authentication protocol

The standard handover process is based on the transition from higher coverage, and a small bandwidth station to a larger bandwidth station with less coverage. Vertical delivery depends on switching from one network to another with a different type, such as LTE and WLAN. A well-structured handover is required to integrate different wireless access networks with each other. The re-authentication process is considered a critical issue in designing the handover protocol. It might cause an undesirable delay in real-time applications. Therefore, the re-authentication delay should be kept to its minimum.

The non-3GPP trust relationship is defined by the MS to determine which non-3GPP station will be used to initiate handover. The trust relationship may be trusted non-3GPP or un-trusted non-3GPP. It is recognized using any of the next possibilities:

1. The MS determines the trust relationship through the 3GPP-based access authentication if the non-3GPP required access authentication from the MS (password is required).
2. The MS uses information from its memory if the non-3GPP depends on a pre-defined policy with the MS.

A new MCC handover authentication protocol is proposed, considering the different architecture in handover between LTE and Wi-Fi networks. The flowchart of the proposed protocol is illustrated in Fig. 4.

The assumptions of the proposed protocol are:

I. The channel between the base station and the MC is assumed to be secure. Also, the channel between the MC and the trusted AP is secure.
II. Before the handover operation takes place:

A pre-shared symmetric key(s) is established between each of the following using the secure channel e.g. SSL:

1. MC and a trusted AP which is termed as ($K_{MC,AP}$)
2. MC and ANDSF which is termed as ($K_{MC,ANDSF}$).
3. ANDSF and LTE BS which is termed as ($K_{BS,ANDSF}$).
4. MC and BS which is termed as ($K_{MC,BS}$).

Each AP has a unique ID and each LTE provider has a unique ID, so MC can easily identify and connect to Wi-Fi AP and ANDSF. Table 1 shows the notations used in the proposed protocol.

The proposed protocol consists of three phases: initial entry, handover decision, and handover authentication phases. Each one of these phases will be explained in the next sections. It is assumed that the *MC* can visit the same BS/AP more than once, so in the proposed protocol, a table called Key Tracking Table (KTT) is provided with information about MC login history including the identity of the mobile cloud, current AP_{ID}/BS_{ID}, visited AP_{ID}/BS_{ID}, and time to live for key expiration time T. The KTT will be stored in both MC and ANDSF. The information in that table is used to reduce the time for re-calculating the symmetric key ($K_{MC'}$) used for authenticating previous visited AP_i/BS_i.

3.1 Case I: Handover from Wi-Fi to LTE

If the MS moves away from the serving station (here WLAN AP), the radio signal strength is reduced beyond the threshold and the data flow might cut off. In order to continue data transfer, the MS initiates a handoff request to the neighboring station (here LTE eNode). The proposed Wi-Fi to LTE authentication protocol is explained in the next sub-sections.

3.1.1 Initial entry phase

During the initial entry phase, MC generates a shared symmetric key K_{MC} and sends it along with MC_{ID} to both Wi-Fi AP (encrypted by $K_{MC,AP}$), and to ANDSF (encrypted by $K_{MC,ANDSF}$).

3.1.2 Handover decision

The ANDSF is responsible for the process of discovery and selection of the LTE network, so it always scans the area for an available network(s). After receiving K_{MC} and MC_{ID} from MC; the ANDSF will:

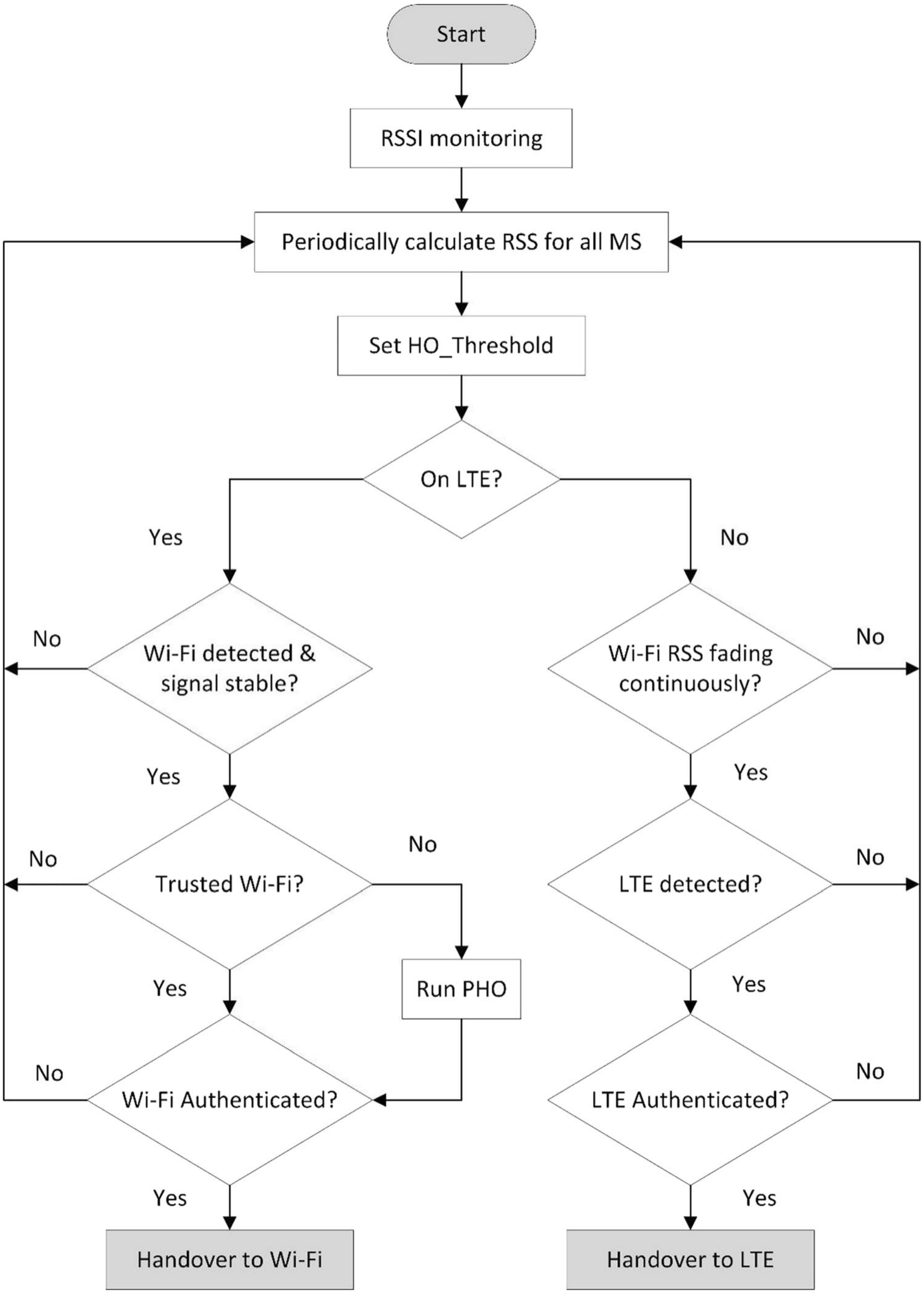


Fig. 4 A flowchart of the proposed protocol

- Generate a random number r_1.
- Compute $K_{MC'}$, which is a symmetric key that will be used to authenticate the target BS_i, using Eq. 1

$$K_{MC'} = H(K_{MC}, r_1, MC_{ID}) \tag{1}$$

.

- ANDSF sends the term ($K_{MC'}$, r_1, MC_{ID}) encrypted by $K_{ANDSF,BS}$

3.1.3 Vertical handover authentication phase

After HO decision is made and ANDSF selects the appropriate BS_i, the selected base station, BS_i, sends the random value r_1, to MC. The mutual authentication between MC and BS_i is as follows:

1. MC Compute $sK_{MC'}$ using Eq. (1).
2. MC Encrypt the random number r_1, using $K_{MC'}$.
3. MC Generate a new random number r_2.
4. MC Send both r_2 and the encrypted r_1 to BS_i.

Table 1 Notations

Notations	Meaning
AP	Access point (Wi-Fi)
BS	Base station (LTE)
$K_{MC,AP}$	A symmetric key between MC and AP
$K_{MC,ANDSF}$	A symmetric key between MC and ANDSF
$K_{MC,BS}$	A symmetric key between MC and BS
K_{ANDSF,AP_i}	A symmetric key generated between ANDSF and AP
$K_{BS,ANDSF}$	A symmetric key between ANDSF and BS
VHO	Vertical handover
PHO	Prediction handover
r_1, r_2	Random numbers
H	Hash function
MC_{ID}	MC identifier
AP_{ID}	AP identifier
K_{MC}	A symmetric key used for authenticating new AP_S/BS_S

5. After receiving the message from MC, BS_i decrypts the message to get the r_1 and checks If r_1(BS) = r_1 (MC), then the MC is authenticated by BS. Else, BS rejects the MC.
6. If MC is authenticated, BS_i encrypts the random number r_2 using.
7. $K_{MC'}$ and sends the encrypted value to MC.
8. MC decrypts $E_{K_{MC'}}(r_2)$ and checks if r_2(MC) = $r_2(BS_i)$, so mutual authentication is completed, otherwise, MC refuse the BS_i.

After mutual authentication is achieved between the MC and the selected BS, MC can transfer network data flow from Wi-Fi AP to the LTE network. An illustration of the proposed Wi-Fi to LTE authentication protocol is shown in Fig. 5. A pseudo-code of the proposed protocol is presented in Algorithm 1.

Algorithm 1: Proposed Wi-Fi to LTE authentication protocol.

```
Input : MS is connected to the internet using Wi-Fi AP
        MCC shared $K_{MC,AP}$ and $K_{MC,ANDSF}$
Output : transfer network dataflow to authenticated LTE BS
While (handover condition is met)
        ANDSF scan and select appropriate LTE
        Generate random r_1
        Compute $K_{MC'} = H(K_{MC}, r_1, MC_{ID})$
        Send $(K_{MC'}, r_1, MC_{ID})$ encrypted by $K_{ANDSF,BS}$
    Start mutual authentication
        Compute $K_{MC'}$ .
        Encrypt the random number $r_1$ , using $K_{MC'}$ .
        Generate a new random number $r_2$.
        Send both $r_2$ and the encrypted $r_1$ to $BS_i$.
    if ( $r_1$ (BS) = $r_1$ (MC) && $r_2$ (MC) = $r_2$ ($BS_i$))
        mutual authentication is completed
      Else
          BS rejects the MC.
          MC refuse the $BS_i$.
          ANDSF scan and select another LTE
    End if
End While
Return transfer network dataflow to authenticated LTE BS
```

3.2 Case II: Handover from LTE BS to trusted Wi-Fi AP

3.2.1 Initial entry phase

1. MC generates a shared symmetric key K_{MC}
2. MC sends both MC_{ID} and K_{MC} encrypted by $K_{MC,BS}$ to BS.
3. Then BS sends K_{MC} to ANDSF along with MC_{ID} encrypted by the shared key ($K_{BS,ANDSF}$).

3.2.2 Handover decision

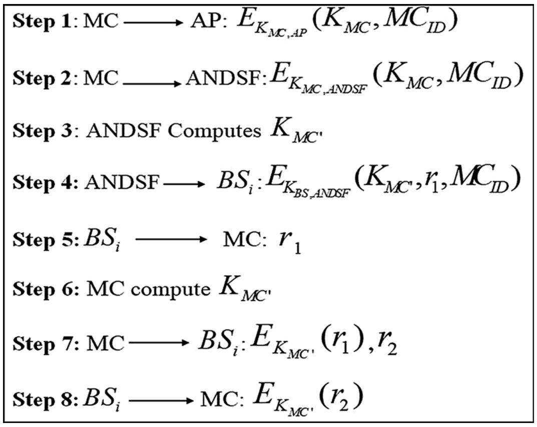
After ANDSF receives [K_{MC},MC_{ID}] from MC:

1. ANDSF generate a random number r_1, and computes $K_{MC'}$.
2. ANDSF establishes a shared key between it and the selected trusted AP K_{ANDSF,AP_i}.
3. Then ANDSF sends the term ($K_{MC'}$,r_1, MC_{ID}) encrypted by K_{ANDSF,AP_i} to selected AP.

3.2.3 Vertical handover authentication phase

After HO decision is made and ANDSF selects AP_i. AP_i sends the random value (r_1) to MC to calculate $K_{MC'}$, to start mutual authentication between MC and AP_i.

1. MC encrypts the random number r_1 using $K_{MC'}$ and generates a new random number r_2.
2. Then MC sends the encrypted r_1 and the random number r_2 to AP_i.



Step 1: MC → AP: $E_{K_{MC,AP}}(K_{MC}, MC_{ID})$

Step 2: MC → ANDSF: $E_{K_{MC,ANDSF}}(K_{MC}, MC_{ID})$

Step 3: ANDSF Computes $K_{MC'}$

Step 4: ANDSF → BS_i: $E_{K_{BS,ANDSF}}(K_{MC'}, r_1, MC_{ID})$

Step 5: BS_i → MC: r_1

Step 6: MC compute $K_{MC'}$

Step 7: MC → BS_i: $E_{K_{MC'}}(r_1), r_2$

Step 8: BS_i → MC: $E_{K_{MC'}}(r_2)$

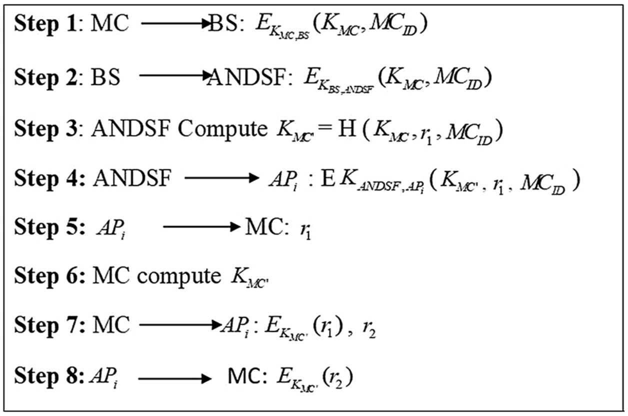
Fig. 5 Illustration of the proposed Wi-Fi to LTE authentication protocol

3. After receiving the message from MC, AP_i decrypts the message to get the value of the random number r_1 and checks if r_1(MC) = r_1(AP) then the MC is authenticated, else the authentication is terminated.
4. If the MC is authenticated.AP_i encrypts the value of r_2 using $K_{MC'}$, and sends it to MC.
5. MC decrypts $E_{K_{MC'}}(r_2)$ and checks if r_2 (MC) = r_2 (AP_i) to finish the mutual authentication, otherwise, MC rejects AP_i.

After mutual authentication is achieved, MC can transfer network data flow from the LTE network to Wi-Fi AP. Figure 6 illustrates the proposed protocol. A pseudo-code for the proposed protocol is presented in Algorithm 2.

Algorithm 2: Proposed LTE to trusted Wi-Fi authentication protocol.

```
Input : MS is connected to the internet using LTE BS
        MCC shared $K_{MC,BS}$ and $K_{BS,ANDSF}$
Output : transfer network dataflow to authenticated Wi-Fi
While (handover condition is met)
    ANDSF scan and select appropriate AP
    If (AP is trusted)
        Generate random r1
        Compute $K_{MC'} = H(K_{MC}, r_1, MC_{ID})$
        Send $(K_{MC'}, r_1, MC_{ID})$ encrypted by $K_{ANDSF,APi}$
    End if
    Start mutual authentication
        Compute $K_{MC'}$ .
        Encrypt the random number $r_1$ , using $K_{MC'}$ .
        Generate a new random number $r_2$.
        Send both $r_2$ and the encrypted $r_1$ to $BS_i$.
    IF ( $r_1 (AP_i) = r_1$ (MC) && $r_2$ (MC) = $r_2$ $(AP_i)$)
        mutual authentication is completed
        Else
            $AP_i$ Rejects the MC.
            MC refuse the$AP_i$.
            ANDSF scan and select another AP
    End if
End While
Return transfer network dataflow to authenticated Wi-Fi
```



Step 1: MC $\longrightarrow$ BS: $E_{K_{MC,BS}}(K_{MC}, MC_{ID})$

Step 2: BS $\longrightarrow$ ANDSF: $E_{K_{BS,ANDSF}}(K_{MC}, MC_{ID})$

Step 3: ANDSF Compute $K_{MC'} = \mathrm{H}(K_{MC}, r_1, MC_{ID})$

Step 4: ANDSF $\longrightarrow$ AP_i : E $K_{ANDSF,AP_i}(K_{MC'}, r_1, MC_{ID})$

Step 5: AP_i $\longrightarrow$ MC: r_1

Step 6: MC compute $K_{MC'}$

Step 7: MC $\longrightarrow$ AP_i: $E_{K_{MC'}}(r_1)$, r_2

Step 8: AP_i $\longrightarrow$ MC: $E_{K_{MC'}}(r_2)$

Fig. 6 Illustration for proposed LTE to trusted Wi-Fi authentication protocol

3.3 Case III: Handover From LTE to untrusted Wi-Fi

In this case, MC discovers an untrusted Wi-Fi connection and wants to initiate handover to this station. Before connecting to the new station, MC must first authenticate it for a secure connection. In other words, it must create a secure channel to secure the data flow to the untrusted station. IP-sec [38] is the most common way to establish this secure channel. The main disadvantage of IP-sec is taking a long time to execute, approximately 1 s. Therefore, a handover prediction scheme is introduced to predict the next station so that the secure channel can be established before the handover condition is met.

3.3.1 The proposed handover prediction scheme

The benefit of handover prediction is to reduce the intrusion in hard handover and accomplishment of the perfect variety set size in the soft handover case. In the case that an appropriate and proficient handover prediction is achieved, redundant handover' numbers (unnecessary handover) can be minimized. Numerous techniques can be applied for minimizing the redundant handover' numbers; like Hysteresis Margin HM [39] and Time-To-Trigger (TTT) [40]. All techniques depend on postponing the handover for a pre-defined period of time. The use of these methods for prediction purposes does not need to take care of overhead since the components are already aggregate in MAC administration messages. Hence, these parameters are passed on inside the network paying little mind to whether MS uses the prediction information or not [41].

The proposed technique is based on continuously reporting the quality of the signal (channel) coming from the network in MS's scanning process. In the HM case, a comparison of one or numerous signal parameters between the current and predicted station is performed. The decision and initiation of the handover process are dependent on that comparison. Once the signal factor of the predicted objective station surpasses the signal factor of the current in addition to HM, the handover is started. As particular by the accompanying condition:

$$S_i^{\Pr ed} > S_i^{Ser} + HM \tag{2}$$

where $S_i^{\Pr ed}$ and S_i^{Ser} denote the signal, quality factors of the predicted target and current serving station correspondingly. Mobile networks can detect and correct three types of triggering TTT issues (too early, too late, and to a wrong cell) supported by Mobility robustness optimization. Several techniques are proposed from researchers to improve the operation of handover triggering, avoiding these three types of issues, and decreasing the false handover warnings. Traditional handover triggering techniques are generally based on RSS from the current station BS_s/AP_s [41, 42].

The proposed development depends on the description of two independent thresholds. The first threshold $HO\_thrSer_{X,Y}$ defines the received signal level by the MS from the current station BS_s/AP_s, although another threshold $HO\_thr\Pr ed_{X,Y}$ defines the measured signal level by the MS from the possible prediction objective BS_s/AP_s.

If RSSI of the serving station BS_s/AP_s descents under $HO\_thrSer_{X,Y}$ and concurrently the RSSI of a nearby BS_s/AP_s surpasses $HO\_thr\Pr ed_{X,Y}$, the prediction conclusion is the probability of MS handover from BSx/APx to BSy/APy. As a result, BSy/APy is considered as the predicted objective BS_s/AP_s. The average of few past signal levels prompting the handover beginning is computed which used to decide the mean estimations of the ordinary thresholds for the handover. Necessary RSSI samples number is determined, which is the purpose of the examination to be specified additionally in this proposed protocol. The following equations define the mean thresholds.

$$avg\_HO\_thrSer_{X,Y} = \frac{1}{HO_{BS_Y,BS_X}} \sum_{i=1}^{HO_{BS_X,BS_Y}} RSSI_{MS,BS_X}^{HO_i} \tag{3}$$

$$avg\_HO\_thr\Pr ed_{X,Y} = \frac{1}{HO_{BS_Y,BS_X}} \sum_{i=1}^{HO_{BS_X,BS_Y}} RSSI_{MS,BS_Y}^{HO_i} \tag{4}$$

where HO_{BS_X,BS_Y} is the number of handovers that happened among the current serving BS_s/AP_s and the possible target BS_s/AP_s through the observed time period. $RSSI_{MS,BS_X}^{HO_i}$ and $RSSI_{MS,BS_Y}^{HO_i}$ are RSSIs received from BSx/APx and BSy/APy correspondingly at the instant time, and Index I states the separate handover occurrence.

The MS may reach to an area where more than one possible target BS_s/AP_s satisfies prediction conditions, a few techniques for the assurance of the absolute most probable target BS_s/AP_s to be very much characterized. This technique relies upon the computation of the most minimal contrast between the two thresholds ($HO\_thrSer_{X,Y}$, $HO\_thr\Pr ed_{X,Y}$) and the present ($RSSI_{MS,BS_X}$ and $RSSI_{MS,BS_Y}$) correspondingly.

Algorithm 3: Proposed Prediction handover scheme

```
Input : Initialize a fixed location of $BS_s$
        Randomly initialize location of $AP_s$
Output : Predicted target station
Monitor RSSI for $BS_s / AP_s$
Compute $avgHO\_thrSer_{X,Y}$
Compute $avgHO\_thr\Pr ed_{X,Y}$
Find $\Pr edTar(BS_s / AP_s)$ = Predicted target station(s)
While ( $RSSI_{Ser} \leq HO\_thrSer_{X,Y}$ )
    Scan area for available $BS_s / AP_s$
    Register no_ $\Pr edTar(BS_s / AP_s)$
    if ( $RSSI_{\Pr ed} \geq HO\_thr\Pr ed_{X,Y}$ )
        if (no_ $\Pr edTar(BS_s / AP_s) = =1$)
            use the existing $\Pr edTar(BS_s / AP_s)$
        if ( no_ $\Pr edTar(BS_s / AP_s) >1$)
            $\Pr edTar(BS_s / AP_s) = \min ( ListPred(BS_s / AP_s)$
    end if
end while
return $\Pr edTar(BS_s / AP_s)$
```

This is performed for all likely targets BS_s/AP_s. These stations are recorded in $ListPred(BS_s/AP_s)$. The predicted target BS_s/AP_s is the determination of the predicted target BS_s/AP_s, it is performed according to the output of the following equation:

$$DiffBS_X, BS_Y = |avg\_HO\_thrSer_{X,Y} - RSSI_{MS,BS_X}| + |avg\_HO\_thr\Pr ed_{X,Y} - RSSI_{MS,BS_Y}| \quad (5)$$

The BS_s/AP_s with the lowest $(DiffBS_X, BS_Y)$ is determined as the predicted target BS_s/AP_s, as shown in the following equation.

$$\Pr edTar(BS_s/AP_s) = \min(ListPred(BS_s/AP_s)) \quad (6)$$

The advantages of the proposed PHO process are that it increases the efficiency of the proposed authentication protocol without adding any overhead to the authentication process. Algorithm 3 illustrates the proposed PHO. The proposed protocol from LTE 3GPP to untrusted Wi-Fi is described in 3 phases, initial entry, HO Decision, and HO authentication.

3.3.2 Initial entry phase

After MC generates the shared symmetric key K_{MC} and sends both MC_{ID} and K_{MC} encrypted by $(K_{MC,BS})$ to BS, BS sends K_{MC} to ANDSF along with MC_{ID} encrypted by the shared key $K_{BS,ANDSF}$

1. MC generates a shared symmetric key K_{MC}.
2. MC sends both MC_{ID} and K_{MC} encrypted by $K_{MC,BS}$ to BS.
3. Then BS sends K_{MC} to ANDSF along with MC_{ID} encrypted by the shared key $(K_{BS,ANDSF})$.

3.3.3 Handover decision phase

When the BS signal comes under a predefined threshold, the prediction handover scheme begins. After PHO predicts the untrusted target AP station, ANDSF will start a key agreement with this AP to create a secure channel between the expected AP and ANDSF. Then ANDSF generate K_{ANDSF,AP_i} and sends it to the predicted AP_i. Thus, there is a secure channel between ANDSF and predicted AP_i.

3.3.4 Vertical handover authentication phase

The remaining steps will be performed for the authentication phase as documented in the trusted Wi-Fi to LTE protocol. The diagram of the proposed authentication protocol and the algorithm are presented as shown in Fig. 7 and Algorithm 4 respectively.

Algorithm 4: Proposed LTE to un-trusted Wi-Fi authentication protocol.

```
Input : MS is connected to the internet using LTE BS
        MCC shared $K_{MC,BS}$ and $K_{BS,ANDSF}$
Output : transfer network dataflow to authenticated Wi-Fi
While (handover condition is met)
    ANDSF scan and select appropriate AP
    If (AP is untrusted)
        Run PHO
        Key agreement with predicted AP
        Send $K_{ANDSF,APi}$ to selected AP
        Generate random r1
        Compute $K_{MC'} = H(K_{MC}, r_1, MC_{ID})$
        Send ($K_{MC'}, r_1, MC_{ID}$) encrypted by $K_{ANDSF,APi}$
    End if
    Start mutual authentication
        Compute $K_{MC'}$ .
        Encrypt the random number $r_1$ , using $K_{MC'}$ .
        Generate a new random number $r_2$.
        Send both $r_2$ and the encrypted $r_1$ to $BS_i$.
    IF ( $r_1$ ($AP_i$) = $r_1$ (MC) && $r_2$ (MC) = $r_2$ ($AP_i$))
            mutual authentication is completed
        Else
            $AP_i$ Rejects the MC.
            MC refuse the$AP_i$.
            ANDSF scan and select another AP
    End if
End While
Return transfer network dataflow to authenticated Wi-Fi
```

4 Evaluation of the proposed protocol

4.1 Simulation scenario

The random waypoint mobility model (RWPMM) [49] is utilized as a movement manner of all mobile stations. The LTE base stations are structured in a regular mode with the same height and the same level of transmitting power. The access points (Wi-Fi) are structured in a random manner using the same transmitting power and the same height. The simulation parameters' variables and their ranges are shown in Table 2. The urban macrocell path loss model [43] is used to calculate the RSSI level for the mobile stations and the neighboring stations. In the simulation, we used an MS speed in a random interval from 2 to 10 m/s. The proposed handover prediction schemes are evaluated by using MATLAB16 within different areas. The positions of all MSs and *APs* are produced in a random manner.

4.2 Simulation results

The time between the prediction of a station and the handover occurrence (PHO_Time) is monitored and compared to the time it took to establish a secure channel (VHO_-Time). The PHO_Time is listed in Table 3 and illustrated in Fig. 8. According to the simulation results, the handover the minimum prediction time is 1.8 s which is greater than the time required to perform a complete EAP/TLS authentication, which is about 1000 ms [44]. After running the simulation and monitoring PHO_Time and VHO_Time

Step 1: MC $\longrightarrow$ BS: E (K_{MC} , MC_{ID}) $K_{MC,BS}$

Step 2: BS $\longrightarrow$ANDSF: E (K_{MC} , MC_{ID}) $K_{BS,ANDSF}$

Step 3: Run PHO

Step 4: Key agreement with predicted AP_i , generate K_{ANDSF,AP_i}

Step 5: ANDSF $\longrightarrow$ AP_i **:** K_{ANDSF,AP_i}

Step 6: ANDSF Compute $K_{MC'}$, generate r_1

Step 7: ANDSF $\longrightarrow$ $AP_i : E_{K_{ANDSF,AP_i}}(K_{MC'}, r_1, MC_{ID})$

Step 8: AP_i $\longrightarrow$ MC: r_1

Step 9: MC compute $K_{MC'}$

Step 10: MC $\longrightarrow$ $AP_i : E_{K_{MC'}}(r_1)$, r_2

Step 11: AP_i $\longrightarrow$ MC: $E_{K_{MC'}}(r_2)$

Fig. 7 Illustration for proposed LTE to untrusted Wi-Fi authentication protocol

Table 2 Simulation parameter

Parameter	Value
Number of BS_s	19
Number of AP_s	17
Number of MS_s	70
BS transmitting power [dBm]	46
AP transmitting power [dBm]	46
MS speed [m/s]	2, 4, 6, 8, 10
MS gain [dBm]	10
BS Frequency band [GHz]	2.5
AP Frequency band [GHz]	2.4
Simulation duration [s]	10,800
Scanning reporting period [s]	1
path loss model	Urban Macrocell [43]
Mobility model	RWPMM
Hysteresis margin HM [dB]	5

Table 3 Values of PHO-Time

Speed (m/s)	PHO_Time (s)
2	1.8
4	1.75
6	1.6
8	1.56
10	1.44

under different conditions, the value of PHO_Time is more than VHO_Time, so there is enough time to create the secure channel before handover, so the MC can authenticate the untrusted AP without having trouble creating the secure channel using a key agreement.

The relation between the MS' speed and success percentage of the prediction scheme is illustrated in Fig. 9 with HM = 5 and MS' speed = 2, 4, 6, 8 and 10. The success percentage is 96% in an MS' speed = 2 which is a realistic result because the possibility of delivery from one station to another is reduced as the MS moves at low speed. In most cases, the predicted station is the station with the highest success ratio. Moreover, increasing MS's speed will reduce the accuracy of the prediction scheme due to a large number of handovers that occur and the short time between each handover. Even though, the proposed scheme accomplishes a success ratio of more than 89% with high MS speed = 10 m/s with large HM value.

The relationship between the number of handovers occurred and different MS' speeds are illustrated in Fig. 10. It is observed that the relationship between the number of handovers and the speed of MS is proportional. The optimum case with the smallest number of handovers occurred at MS' speed = 2. Increasing the MS' speed with high HM = 5 increasing the number of handovers. The number of handovers occurred during the simulation period is monitored to recognize the effect of the proposed prediction scheme on the number of handovers an MS might do. The proposed scheme decreases the number of handovers by 50% when compared to the handover without any prediction.

4.3 Performance analysis

A comparison of the proposed protocol with the existing authentication protocols is presented in Table 4, in terms of user cryptography operations, parties number, user anonymity [45], un-traceability [46], and communication overhead [47]. Communication overhead is the handover time in the authentication procedure and key distribution process. The communication cost between the MC and AP/BS is labeled as α and the expected cost of authentication message between AP/BS and ANDSF is β. As shown in the Table 4 the user cryptography operation needed for the proposed handover authentication protocol is only one hash and 2 symmetric key operations which takes less time to compute with more security added from both hash and symmetric cryptography. The proposed protocol requires only two parities (MCC and AP/BS). An authentication server that added extra load and time to the authentication process is not required in the proposed protocol. Therefore, it needed only 3 message flow in the authentication process from the MCC and the authenticated AP/BS. The main advantages of the proposed handover authentication protocol are:

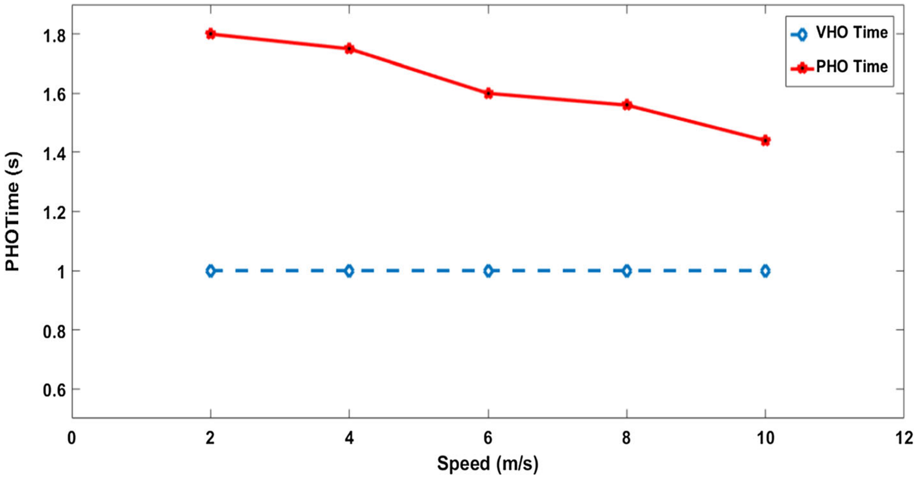


Fig. 8 Comparison between PHO_Time and VHO_Time

- *Reduced bandwidth consumption*: The proposed protocol does not require any sequence number synchronization SQN among the MC and LTE network, which used to decrease bandwidth consumption. In addition, confidential identities for MC and MS can give the ability to reduce bandwidth usage, since the client identity should not be requested again as in EAP-AKA.

Reduced authentication delay: The time it takes for a process to complete the authentication procedure is the authentication delay. Handover delay is monitored between LTE and WLAN and the average value is calculated in different situations and it is found to be approximately 3.408 s. The total authentication time is monitored, and the result is 1.568 s which costs 46% of the full delivery delay. The proposed protocol uses only symmetric encryption operation in the authentication process which presents a delay lower than the usual EAP-AKA and Fast EAP-AKA [29, 48].

4.4 Security analysis

Many authentication protocols are sensitive against some kind of attacks such as impersonation attack [49], replay attack [50, 51], and data leakage attack [52, 53].

- *Impersonation attack*: an attacker assumes the identity of one of the legitimate parties in a communication protocol.
- *Replay attack*: an attacker might use an old authentication challenge-response to respond to a new authentication challenge.
- *Data leakage attack*: an attacker might reveal sensitive data during the authentication process.

As mentioned above, there are three handover cases performed by the MC: (1) From Wi-Fi to LTE, 2) From LTE to trusted Wi-Fi, (3) From LTE to untrusted Wi-Fi. The first two cases are secured due to the assumption that the channel between the base station and the MC and the channel between the MC and the trusted AP are secure. As for the third case, we initiate a scenario game to prove that the proposed vertical authentication protocol is secure

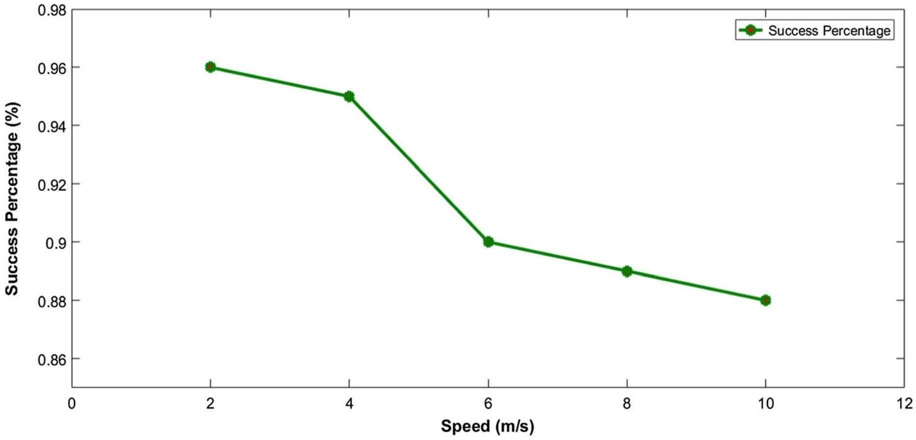


Fig. 9 Success percentage of the prediction scheme

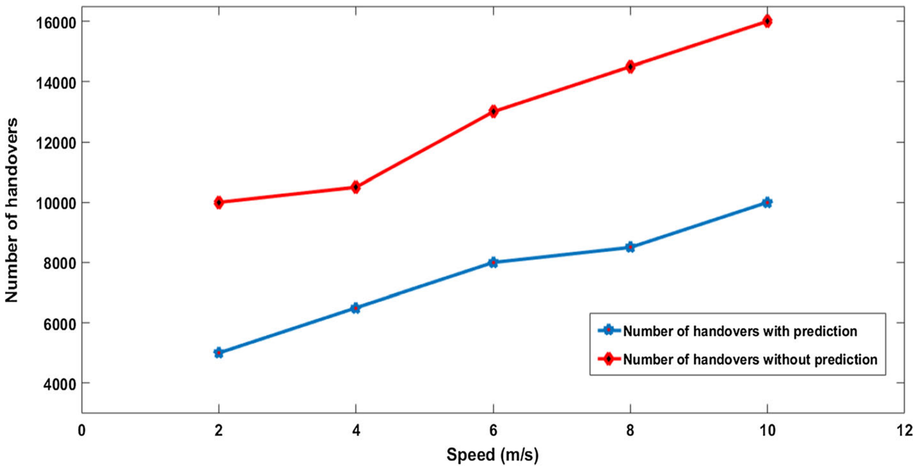


Fig. 10 Number of handovers (with and without prediction) at different speeds

Table 4 Performance comparison

Protocol	User cryptography operations	Number of parities	User anonymity and un-traceability	Communication overhead
Choi et al. [23]	4ME + 1RV	2	No	3α
Yang et al. [24]	8.75ECSM + 3Pairing	2	No	2α
He et al. [21]	10H + 3S	3	Yes	$2\beta + 3\alpha$
He et al. [25]	15.75ECSM + 4Pairing	2	Yes	3α
He et al. [29]	1ECSM + 1Pairing + 3H	2	Yes	2α
Cao et al. [30]	3.25ECSM	2	No	3α
He et al. [34]	3H + 1Pairing	3	Yes	2α
Anmin et al. [47]	5 MM	2	yes	3β
Odelu et al. [36]	9 ECSM + 2Pairing	2	Yes	3α
Proposed protocol	1H + 2S	2	Yes	3α

ECSM elliptic curve scalar multiplication, *ME* modular exponentiation, *MM* modular multiplication, *RV* RSA verification, *H* hash operation, *S* symmetric operation (encryption/decryption)

against the mentioned attacks. The game is conducted as follows:

- *Initial entry:* MC generates a shared symmetric key K_{MC} and sends both MC_{ID} and K_{MC} encrypted by $K_{MC,BS}$ to BS. Then, BS sends K_{MC} to ANDSF along with the MC_{ID} encrypted by the shared key $K_{BS,ANDSF}$
- *Handover decision:* ANDSF predicts the untrusted target AP_i and perform a key agreement through an SSL channel between the predicted AP_i and the ANDSF.
- *Authentication:* After the handover, the decision has been taken for selecting the appropriate AP_i. The MC and the selected AP_i starts to authenticate each other before transferring any data. The AP_i sends a random value (r_1) to the MC in order to compute the $K_{MC'}$. Then, the MC encrypts the random number r_1 using the computed $K_{MC'}$ and sends it along with another random number r_2 to AP_i. The AP_i decrypts the message to check the validity of r_1, if it is valid then the MC is authenticated, else the authentication is terminated.
- *Forge*: If the MC is authenticated, an attacker can send a valid authentication response in an attempt to deceive the MC.
- *Output:* MC verifies the authentication response to finish the mutual authentication. An attacker wins the game if it was a valid response.

The proposed vertical authentication protocol is proved to be secure under the above security model as follows:

Theorem 1 *An attacker cannot intercept the communication and impersonate the MC or the* AP_i.

Proof Initial entry: MC generates a shared symmetric key K_{MC} and sends both MC_{ID} and K_{MC} encrypted by $K_{MC,BS}$

to BS. Then, BS sends K_{MC} to ANDSF along with the MC_{ID} encrypted by the shared key ($K_{BS,ANDSF}$).

Handover decision: ANDSF predicts the untrusted target AP_i and sends K_{ANDSF,AP_i} to it through an SSL channel between the predicted AP_i and the ANDSF. Therefore, there is no chance for an impersonation attack to occur as all the channels between the parties are secured by using the SSL connection. □

Theorem 2 *An untrusted* AP_i *cannot use an old authentication challenge-response to respond to a new authentication challenge.*

Proof Authentication: After the handover, the decision has been taken for selecting the appropriate AP_i. The AP_i sends a random value (r_1) to the MC in order to compute the $K_{MC'}$. Then, the MC encrypts the random number r_1 using the computed $K_{MC'}$ and sends it along with another random number r_2 to AP_i. The AP_i decrypts the message to check the validity of r_1, if it is valid then the MC is authenticated, else the authentication is terminated.

Forge: If the MC is authenticated, the AP_i sends backs the encrypted value of r_2 using $K_{MC'}$, and caches it in order to deceive the MC in the future authentication challenges. Finally, the MC decrypts $E_{K_{MC'}}(r_2)$ to finish the mutual authentication.

Output: Each authentication challenge is independent of the previous challenges. In other words, each challenge is performed with different random numbers. In the next authentication challenge, new random numbers will be generated. Therefore, if the untrusted AP_i retrieved the cached value of r_2 and sent it to the MC. The MC will decrypt $E_{K_{MC'}}(r_2)$ to find that it is extremely unlikely to be equal to the newly generated random number. Hence, the untrusted AP_i cannot deceive the MC. □

Theorem 3 *An attacker cannot access any sensitive and protected data.*

Proof In the proposed protocol, all sensitive data are encrypted using a strong symmetric encryption algorithm and a hash function. In addition, the MC and the ANDSF continuously create new keys during a predefined time period. Therefore, any unauthorized access to any secret keys or sensitive data is impossible to occur in the proposed protocol. □

5 Conclusion

A new handover authentication protocol for Mobile Cloud Computing paradigm is proposed in this paper. The proposed protocol is based on symmetric-key cryptography and a hash function. The use of the symmetric key cryptosystem and the Hash function to provide a secure connection between LTE and WLAN AP provides similar security features and uses fewer resources than general cryptographic systems with certificates. Thus, the proposed protocol has a lower overhead than the current protocols that rely on public-key cryptosystems with certificates. The proposed protocol provides benefits such as being secure against a number of common attacks like man-in-the-middle attack and replay attack, providing mutual authentication, key confidentiality, robust security, and efficiency. The security and performance analysis shows that the proposed protocol minimizes bandwidth consumption and authentication delay. Hence, using the prediction scheme solves the problematic issue of establishing a secure channel in authenticating untrusted networks without adding any overhead. With these advantages, the new proposal protocol is believed to provide a comprehensive solution to handoff in MCC.

References

1. Ross, P. (2011). How to keep your head above the clouds: Changing ICT worker skill sets in a cloud computing environment. *Employment Relations Record, 11*(1), 62.
2. Umair, S., Muneer, U., Zahoor, M. N., & Malik, A. W. (2015). Mobile computing: Issues and challenges. In *2015 12th international conference on high-capacity optical networks and enabling/emerging technologies (HONET)* (pp. 1–5). IEEE.
3. Umair, S., Muneer, U., Zahoor, M. N., & Malik, A. W. (2016). Mobile cloud computing future trends and opportunities. In *Managing and processing big data in cloud computing* (p. 105).
4. Almorsy, M., Grundy, J., & Müller, I. (2016). An analysis of the cloud computing security problem. arXiv preprint arXiv:1609.01107.
5. Liu, J. K., Au, M. H., Susilo, W., Liang, K., Lu, R., & Srinivasan, B. (2015). Secure sharing and searching for real-time video data in mobile cloud. *IEEE Network, 29*(2), 46–50.
6. Ma, R., Cao, J., Feng, D., Li, H., Zhang, Y., & Lv, X. (2019). PPSHA: Privacy preserving secure handover authentication scheme for all application scenarios in LTE-A networks. *Ad Hoc Networks, 87,* 49–60.
7. Rittinghouse, J. W., & Ransome, J. F. (2016). *Cloud computing: Implementation, management, and security*. Boca Raton: CRC Press.
8. GPP (V 15.2.0 Release 15, 2017). TS 23.402, Architecture enhancements for non-3GPP accesses. In *3rd generation partnership project; technical specification group services and system aspects*.
9. Taleb, T., & Kunz, A. (2012). Machine type communications in 3GPP networks: Potential, challenges, and solutions. *IEEE Communications Magazine, 50*(3), 178–1847.
10. GPP (V 14.1.0, 2017). TS 24.312, access network discovery and selection function (ANDSF) management object (MO). In *3rd generation partnership project; technical specification group services and system aspects*.
11. Yan, X., Şekercioğlu, Y. A., & Narayanan, S. (2010). A survey of vertical handover decision algorithms in Fourth Generation

heterogeneous wireless networks. *Computer Networks, 54*(11), 1848–1863.

12. Xenakis, D., Passas, N., Di Gregorio, L., & Verikoukis, C. (2011). A context-aware vertical handover framework towards energy-efficiency. In *2011 IEEE 73rd vehicular technology conference (VTC spring)* (pp. 1–5). IEEE.
13. Xenakis, D., Passas, N., Merakos, L., & Verikoukis, C. (2015). Advanced mobility management for reduced interference and energy consumption in the two-tier LTE-advanced network. *Computer Networks, 76,* 90–111.
14. Yang, M., Li, Y., Jin, D., Zeng, L., Wu, X., & Vasilakos, A. V. (2015). Software-defined and virtualized future mobile and wireless networks: A survey. *Mobile Networks and Applications, 20*(1), 4–18.
15. GPP (V 15.0.0 Release 15, 2018). TS 33.401, 3GPP system architecture evolution (SAE); Security architecture. In *3rd generation partnership project; technical specification group services and system aspects*.
16. Abdo, J. B. B., Chaouchi, H., & Aoude, M. (2012). Ensured confidentiality authentication and key agreement protocol for EPS. In *2012 symposium on broadband networks and fast internet (RELABIRA)* (pp. 73–77). IEEE.
17. Fu, J., Bertze, Å., Da Silva, I. L., Kuivinen, F., & Wang, Y. (2016). Handover prediction using historical data. Google Patents.
18. Xu, X., Xue, Y., Qi, L., Yuan, Y., Zhang, X., Umer, T., et al. (2019). An edge computing-enabled computation offloading method with privacy preservation for internet of connected vehicles. *Future Generation Computer Systems, 96,* 89–100. https://doi.org/10.1016/j.future.2019.01.012.
19. Chen, Y., Deng, S., Ma, H., Yin, J. J. M. N., & Applications. (2019). Deploying data-intensive applications with multiple services components on edge. *Mobile Networks and Applications*. https://doi.org/10.1007/s11036-019-01245-3.
20. Wan, C., Hu, A., & Zhang, J. (2011). An elliptic curve based handoff authentication protocol for WLAN. *Chinese Journal of Electronics*, *20*(1), 165–169.
21. He, D., Ma, M., Zhang, Y., Chen, C., & Bu, J. (2011). A strong user authentication scheme with smart cards for wireless communications. *Computer Communications, 34*(3), 367–374.
22. El Bouabidi, I., Daly, I., & Zarai, F. (2012). Secure handoff protocol in 3GPP LTE networks. In *2012 third international conference on communications and networking (ComNet)* (pp. 1–6). IEEE.
23. Choi, J., & Jung, S. (2010). A handover authentication using credentials based on chameleon hashing. *IEEE Communications Letters, 14*(1), 54–56.
24. Yang, G., Huang, Q., Wong, D. S., & Deng, X. (2010). Universal authentication protocols for anonymous wireless communications. *IEEE Transactions on Wireless Communications, 9*(1), 168–174.
25. He, D., Bu, J., Chan, S., Chen, C., & Yin, M. (2011). Privacy-preserving universal authentication protocol for wireless communications. *IEEE Transactions on Wireless Communications, 10*(2), 431–436.
26. Nakanishi, T., & Funabiki, N. (2005). Verifier-local revocation group signature schemes with backward unlinkability from bilinear maps. In *International conference on the theory and application of cryptology and information security* (pp. 533–548). Springer.
27. Sharma, M. J., & Leung, V. C. (2011). Improved IP multimedia subsystem authentication mechanism for 3G-WLAN networks. *International Journal of Security and Networks, 6*(2–3), 90–100.
28. Sharma, M. J., & Leung, V. C. (2012). IP multimedia subsystem authentication protocol in LTE-heterogeneous networks. *Human-Centric Computing and Information Sciences, 2*(1), 16.
29. He, D., Chen, C., Chan, S., & Bu, J. (2012). Secure and efficient handover authentication based on bilinear pairing functions. *IEEE Transactions on Wireless Communications, 11*(1), 48–53.
30. Cao, J., Ma, M., & Li, H. (2012). An uniform handover authentication between E-UTRAN and non-3GPP access networks. *IEEE Transactions on Wireless Communications, 11*(10), 3644–3650.
31. Cao, J., Li, H., Ma, M., Zhang, Y., & Lai, C. (2012). A simple and robust handover authentication between HeNB and eNB in LTE networks. *Computer Networks, 56*(8), 2119–2131.
32. Sithirasenan, E., Ramezani, K., Kumar, S., & Muthukkumarasamy, V. (2013). EAP-CRA for WiMAX, WLAN and 4G LTE Interoperability. In *Selected topics in WiMAX*. InTech.
33. Liu, J. K., Chu, C. K., Chow, S. S., Huang, X., Au, M. H., & Zhou, J. (2015). Time-bound anonymous authentication for roaming networks. *IEEE Transactions on Information Forensics and Security, 10*(1), 178–189.
34. He, D., Chan, S., & Guizani, M. (2015). Handover authentication for mobile networks: Security and efficiency aspects. *IEEE Network, 29*(3), 96–103.
35. Degefa, F. B., Lee, D., Kim, J., Choi, Y., & Won, D. (2016). Performance and security enhanced authentication and key agreement protocol for SAE/LTE network. *Computer Networks, 94,* 145–163.
36. Odelu, V., Zeadally, S., Das, A. K., Wazid, M., & He, D. (2018). A secure enhanced privacy-preserving key agreement protocol for wireless mobile networks. *Telecommunication Systems*, *69*(4), 431–445.
37. Jo, H. J., Paik, J. H., & Lee, D. H. (2014). Efficient privacy-preserving authentication in wireless mobile networks. *IEEE Transactions on Mobile Computing, 13*(7), 1469–1481.
38. Wang, G., Sun, Y., He, Q., Xin, G., & Wang, B. (2018). A content auditing method of IPsec VPN. In *2018 IEEE third international conference on data science in cyberspace (DSC)* (pp. 634–639). IEEE.
39. Yusof, A. L., Ya'acob, N., & Ali, M. T. (2013). Hysteresis margin for handover in long term evolution (LTE) network. In *2013 international conference on computing, management and telecommunications (ComManTel)* (pp. 426–430). IEEE.
40. Khan, M., & Han, K. (2014). An optimized network selection and handover triggering scheme for heterogeneous self-organized wireless networks. *Mathematical Problems in Engineering, 2014*.
41. Luo, Y., Tran, P. N., An, C., Eymann, J., Kreft, L., & Timm-Giel, A. (2013). A novel handover prediction scheme in content centric networking using nonlinear autoregressive exogenous model. In *2013 IEEE 77th vehicular technology conference (VTC spring)* (pp. 1–5). IEEE.
42. Bae, S. J., Chung, M. Y., & So, J. (2011). Handover triggering mechanism based on IEEE 802.21 in heterogeneous networks with LTE and WLAN. In *2011 international conference on information networking (ICOIN)* (pp. 399–403). IEEE.
43. Sgora, A., & Vergados, D. D. (2009). Handoff prioritization and decision schemes in wireless cellular networks: A survey. *IEEE Communications Surveys & Tutorials, 11*(4), 57–77.
44. Mattos, D. M. F., & Duarte, O. C. M. B. (2016). AuthFlow: Authentication and access control mechanism for software defined networking. *Annals of Telecommunications, 71*(11–12), 607–615.
45. Gulati, S., Sharma, S., & Agarwal, G. (2018). The hidden truth anonymity in cyberspace: Deep web. In *Intelligent computing and information and communication* (pp. 719–730). Springer.
46. Xu, G., Qiu, S., Ahmad, H., Xu, G., Guo, Y., Zhang, M., et al. (2018). A multi-server two-factor authentication scheme with untraceability using elliptic curve cryptography. *Sensors, 18*(7), 2394.

47. Fu, A., Qin, N., Wang, Y., Li, Q., & Zhang, G. J. W. N. (2017). Nframe: A privacy-preserving with non-frameability handover authentication protocol based on (t, n) secret sharing for LTE/LTE-A networks. *Wireless Networks, 23*(7), 2165–2176. https://doi.org/10.1007/s11276-016-1277-0.
48. El Idrissi, Y. E. H., Zahid, N., & Jedra, M. (2012). Security analysis of 3GPP (LTE)—WLAN interworking and a new local authentication method based on EAP-AKA. In *2012 international conference on future generation communication technology (FGCT)* (pp. 137–142). IEEE.
49. Conti, M., Dragoni, N., & Lesyk, V. (2016). A survey of man in the middle attacks. *IEEE Communications Surveys & Tutorials, 18*(3), 2027–2051.
50. Mo, Y., & Sinopoli, B. (2009). Secure control against replay attacks. In *47th annual Allerton conference on communication, control, and computing, 2009. Allerton 2009* (pp. 911–918). IEEE.
51. Na, S., Hwang, D. Y., Shin, W., & Kim, K.-H. (2017). Scenario and countermeasure for replay attack using join request messages in LoRaWAN. In *2017 international conference on information networking (ICOIN)* (pp. 718–720). IEEE.
52. Stallings, W., Brown, L., Bauer, M. D., & Bhattacharjee, A. K. (2012). *Computer security: Principles and practice*: Pearson Education, ISBN 0273764497.
53. Zhu, Y., Huang, Z., & Takagi, T. (2016). Secure and controllable k-NN query over encrypted cloud data with key confidentiality. *Journal of Parallel and Distributed Computing, 89,* 1–12.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Walid I. Khedr received the Ph.D. degree in computer science from Ain Shams University. He is currently working as associate professor of information technology at faculty of computers and informatics, Zagazig University. His current research interests are primarily in network security protocols, key management protocols, and cloud security. Another field of interest is Internet of Things security.

Khalid M. Hosny was born in 1966, Zagazig, Egypt. He is a professor of information technology, faculty of Computers and Informatics at Zagazig University. Dr. Hosny received the B.Sc., M.Sc. and Ph.D. from Zagazig University, Egypt in 1988, 1994, and 2000 respectively. From 1997 to 1999 he was a visiting scholar, University of Michigan, Ann Arbor and University of Cincinnati, Cincinnati, USA. He is a senior member of ACM and IEEE. His research interests include image processing, pattern recognition, computer vision and multimedia security. Dr. Hosny published 3 edited books and more than 70 papers in international journals. He is an editor and scientific reviewer for more than 35 international journals.

Marwa M. Khashaba was born in 1985, Zagazig, Egypt. She is a lecturer of information technology, faculty of Computers and Informatics at Zagazig University. Dr. Marwa received the B.Sc., M.Sc., and Ph.D. from Zagazig University. Her research interests include network security, cloud computing, fog computing, mobility in computing environments, and Internet of Things security.

Fathy A. Amer was born in 1947, Cairo, Egypt. He is a professor of information technology, faculty of Computers and Informatics at Cairo University. Prof. Dr. Fathy received the B. Sc. Degree of Bachelor of Elec. Eng. and Comm. from Military Technical College, Cairo Univ. 1970, M.Sc. Master of Science in Elec. Eng. and Comm. from Elec. Eng. Dep., Faculty of Eng. Al-Azhar Univ. 1985, and Ph. D. Doctor in Computer Science in subject of Computer Networks Comp. Sci. Dep. Faculty of Eng., Al-Azhar Univ., 1989. Hi research interests include Computer Networks, Distributed Systems, Database systems, Database management systems, Internet Security, Space Communication, Internet and ATM protocols, Voice over IP, Multimedia communications. Electronical circuits design and Implementation.