Vol 6 | Issue 1 | Pages 243-256

Annals of Cognitive Science
ISSN: 2642-4290

Research Article

DOI: 10.36959/447/358

A Robust Vertical Handover Authentication Scheme for SDN Based 5G HetNets

*Alican Ozhelvaci** *and Maode Ma*

School of Electrical and Electronic Engineering, Nanyang Technological University, NTU, Singapore

Abstract

The fifth-generation mobile network is the next paradigm that is expected to bring solutions to the problem of the 4G technology. Also, the expectation is to have the fastest, most reliable network access to support huge data traffic and massively connected nodes with low latency and high throughput with the deployment of the 5G. Hence, there are different new technologies to manage, secure, and fulfill the requirements of 5G. However, the environment of 5G will be very heterogeneous that may cause frequent handoff due to small cell deployment where users join and leave frequently. Additionally, these frequent handoffs would be one of the vulnerabilities which are needed to be secured in 5G. Therefore, in this paper, a scheme has been proposed to have a secure and seamless handover mechanism to supply strong, quick, and mutual authentication. The proposed scheme has been examined for the security proof and the logic of correctness by implementing a security analysis tool which is AVISPA with SPAN and BAN Logic. Also, the result of the performance analysis shows that it is efficient even under attacks. Therefore, the proposed protocol has a mutual vertical handover authentication based on SDN architecture with enough efficiency for the 5G.

Keywords

5G, SDN, Handover Authentication, Heterogeneous Networks, Security

Introduction

The need for the next generation of wireless networks is to become more compatible with information and demand. The new technologies on physical devices are quickly emerging with the fast development of computer networks, mobile telecommunication networks, electronic technology, and control technology as well as the increased intelligent requirements in the modern industry [1]. However, there is still a serious gap between the mobile world where information is exchanged and transformed and the physical world in which we live [2]. In this regard, the evolution of mobile communication networks is getting faster by the new requirements for mobility such as faster speeds, more performance, more energy efficiency, more coverage but less latency, and lower energy consumption. To meet the requirements mentioned before, we are heading to 5th generation mobile networks, shortly 5G, which are the next generation of mobile communication systems beyond 4G or 4G/LTE networks [3]. The next-generation wireless network is being developed and not only evolution of the legacy of other mobile networks such as 3G and 4G, but also with advanced wireless and networking technologies. So, it will be a system with many capabilities [4].

What we expect from the new and next-generation wireless mobile communications network, and what it will enable for us are the questions that are going to be explained. Firstly, all research and developments aim to bring advanced technologies with 5G such as software-defined networking, network function virtualization, and network slicing. Second, 5G will have a higher capacity than 4G LTE much denser in terms of the number of users and user equipment. It will also support device-to-device (D2D) and massive machine-type communications [5]. 5G will have a better connection option for the implementation of the internet of things (IoT) in terms of very low latency and low energy consumption [6]. Moreover, 5G mobile network is expected to enable these 8 high-level features; 1) The speed of 5G is expected to be between 1 to 10 Gbps, 2) The latency will be lower than 5 milliseconds, 3) At least 1000 times bandwidth than 4G, 4) The number of connected devices will be 10 to 100 times, 5) All-time availability, 6) 100 percent coverage, 7) Reducing the usage of network energy and 8) More secure or the securest network compare to last generations [7]. With the

***Corresponding author:** Alican Ozhelvaci, School of Electrical and Electronic Engineering, Nanyang Technological University, NTU, Singapore

Accepted: May 12, 2022

Published online: May 14, 2022

Citation: Ozhelvaci A, Ma M (2022) A Robust Vertical Handover Authentication Scheme for SDN Based 5G HetNets. Ann Cogn Sci 6(1):243-256

5G era, new various network services will utilize what 5G enables for them. These services are the vehicle to vehicle communication, machine-to-machine communication, smart grid, smart cities, smart homes, smart nations, block chain-based services, mobile fog computing, eHealth services, unmanned aerial vehicle (UAV), and so on. Hence, the expectation for commercialization of 5G is that around 2020 and beyond, after that, gradually this next-generation mobile network will be deployed all over the world.

To achieve the requirements of 5G such as high throughput, 100 percent coverage, 90 percent energy consumption reduction, and low cost the concept of Heterogeneous networks must be used in the 5G system. The capabilities of HetNet are wide coverage, high capacity, and better performance with heterogeneity characteristics. There are different cell technologies to support immanent coverage for 5G such as microcells, femtocells, and relays [8]. Therefore, the 5G which is the next generation of wireless technology will be much more heterogeneous compared to legacy networks. Also, because of the densified small cell deployment, there will be frequent handover from one base station to another, thus, the handover authentication is considered to be fast and efficient enough to make sure that low latency is maintained.

In such a heterogeneous environment, the vertical handover is a very important point for the integration of various networks. This allows you to use the best features of existing networks. The authentication is required to grant access to network resources to a specific and registered user. In addition, ensuring interaction between communication assets and protecting against different attacks with keeping data integrity, confidentiality can be made through mutual authentication. Therefore, a smooth and secure transfer registration authentication scheme is required because users often move between different networks is leading to serious security vulnerabilities against various attacks.

Related Work

Designing an efficient, fast, and secure authentication protocol is a tough task to give access to the user equipment in a foreign network. Therefore, there are only a few research projects to design an authentication scheme in order to meet the requirement of the 5G wireless mobile network. In [9], the proposed architecture for the 5G mobile network centrally integrates SDN (Software Defined Network) technology to utilize SDN capabilities such as intelligence and programmable networking by extending LTE (Long-Term Evolution) hierarchical architecture which is provided by 3GPP. Hence, an authentication handover module (AHM) is used in the architecture to monitor user equipment's movements and its previous and next locations based on SDN functions. Hence, the AHM can predict the next potential cells from user equipment's movements, locations and it will prepare the potential cells to make them ready for handover procedure in order to reduce and optimize the induced signaling delay. In [10], the proposed authentication method is based on EAP-AKA using ECDH (Elliptic Curve Diffie-Hellman) and private key cryptography for authentication in the environment of LTE networks. The downsides of the EAP-AKA mechanism are overcome by adding a local authenticator. Therefore, the proposed method can keep user identity safe against various attacks and ensure data integrity and mutual authentication. However, a large number of users and small cells can add an additional delay in the 5G mobile network. So, the method may not be efficient and scalable.

In another proposed authentication scheme, in [11], the authors have proposed two privacy-preserving key agreement protocols to set up an anonymous D2D group session. These approaches generate a group session key to protect users' privacy. But each resource-constrained terminal needs to perform (n+2) bilinear pairing operations for setting up one D2D session, which results in significant computational overhead. Moreover, in the process of user registration, these schemes are vulnerable to man-in-the-middle (MITM) attacks. However, the authentication server is located remotely in the architecture, so this can cause the latency can go up to hundreds of milliseconds. Because of the requirements of 5G, the solution is unsatisfactory due to the frequent handovers between the authentication server and small cells. In [12], the proposed scheme claims to have an efficient authentication method to overcome various vulnerabilities of EAP-AKA and it is called EPS-AKA (Evolved Packet System AKA) in LTE networks. Also, the scheme claims that it has reduced computational overhead, authentication delay and meets security requirements. This proposed scheme is called EEAP-AKA and is based on SPEKE (Simple Password Exponential Key Exchange). The proposed scheme aims to overcome the disclosure of the UE. Another aim is to make the protocol faster by using symmetric key cryptography and reducing the size of exchanged messages. Although the aims of the proposed scheme, the latency can become higher because the environment of small cell deployment may cause a frequent number of inquiries in 5G networks.

This paper presents a certificate authentication based on the symmetric key distribution in order to provide mutual authentication and meet the requirement of a 5G network. Additionally, certificate-based authentication has been used in the proposed scheme to supply high security against various attacks. To the best of our knowledge, there is no single solution among other research for the user equipment that can have certification of foreign networks and at the same time have secured communication between network equipment in this way. In the architecture, SDN (Software Defined Networking) is considered to utilize the capabilities of SDN features such as improving the efficiency of the network, global view of the network, and security management mechanisms. Furthermore, adding a handover authentication module (HAM) makes a smoother handover in the frequent inquiries. The proposed scheme is based on EAP-TLS (Extensible Authentication Protocols - Transport Layer Security) [13]. Besides, pre-initial authentication is proposed in the scheme to issue a certificate only to the registered user. Thus, mutual authentication, key exchange, and agreement can be provided. Moreover, the proposed scheme meets security requirements such as user identity protection, privacy, data integrity, and protection against different attacks.

Hereby, the main contributions of this paper are:

- First, we proposed a light weight vertical handover authentication scheme using the SDN architecture. This not only helps to have a global network view which helps management and security of the network but also, improving the efficiency of the network and the HAM can predict the next potential cells from user equipment's movements, locations and it will prepare the potentially relevant cells and access points to make them ready for handover procedure before the user equipment arrives.
- Second, one of the crucial requirements of a new wireless network is mutual authentication between the UE and the authentication authority. Also, high security should be supplied due to frequent handovers that could cause security issues over the network. Therefore, the proposed EEAP-TLS scheme offers high security and mutual authentication which are achieved by utilizing the EAP-TLS protocol.
- Additionally, due to the environment of 5G, the security properties should be increased to defend against malicious attacks. The proposed scheme ensures a consistent and highly secure vertical handover process by using certificate authentication based on symmetric key distribution. Hence, the SDN controller shares the keys with the user equipment only there is a valid request for handover from the UE. Therefore, the proposed scheme can provide smooth, efficient, and secure handover for the vertical handover process which can high likely happen in the network of 5G.

The remainder of the paper is organized as follows: Section III describes the system background including a system model of the 5G mobile network architecture and the attack model. Section IV details the proposed scheme is explained in detail. Section V provides security proof by BAN Logic and formal verification for the proposed scheme by using AVISPA. Section VI shows the performance and efficiency analysis of the proposed scheme compared with other schemes. And the paper is concluded in Section VII.

System Background

System model

Due to the heterogeneous environment of 5G, security has become one of the important features of the new generation mobile network. The network should have robust security against various attacks such as Man-in-the-Middle and Denial of Service attacks. This new generation network should provide security requirements such as data integrity and privacy of the user, confidentiality of the data, mutual authentication, etc (Figure 1).

Apart from these security requirements, 5G introduces new technologies in order to supply the proposed speed, therefore, one of the new technologies to reach high speed is millimeter waves. However, this technology has poor signal propagation characteristics due to high frequencies that cannot penetrate from obstacles. So, to overcome this issue there will be a large number of small cell deployments in the network but the network will become more heterogeneous. The user equipment can access the 5G core network through a new generation 3GPP radio access system [14]. Therefore, the UE will face many handover connections to different base stations such as from next-generation network nodes (gNBs) to specific access points to access the network. The heterogeneous paradigm and small cell deployment not only provide very high throughput for very high data traffic and ubiquitous coverage but also supports the progress of existing technologies with multi-layer of 5G coverage.

In order to achieve low cost and high capacity communication generally, using low power small cells is proposed as a very important component of the new generation mobile network, 5G. The environment of 5G will may cause frequent handover in the network. In [9], the proposed architecture for the 5G mobile network centrally integrates SDN (Software Defined Network) technology to utilize SDN capabilities such as intelligence and programmable networking by extending LTE (Long-Term Evolution) hierarchical architecture which is provided by 3GPP. Also, the proposed architecture [9] is using an authentication handover module (AHM) which is based on SDN functions to monitor user equipment's movements and its previous and next locations. So, to provide seamless and efficient handovers, a handover authentication module (HAM) is installed in the SDN controller in our architecture similarly in [9]. Thus, the SDN technology will be underlined in the architecture of the 3GPP5G core network.

Furthermore, to support SDN-enabled 5G mobile networks suitable SDN protocols should be installed such as SNMP (Simple Network Management Protocol) and Open Flow to

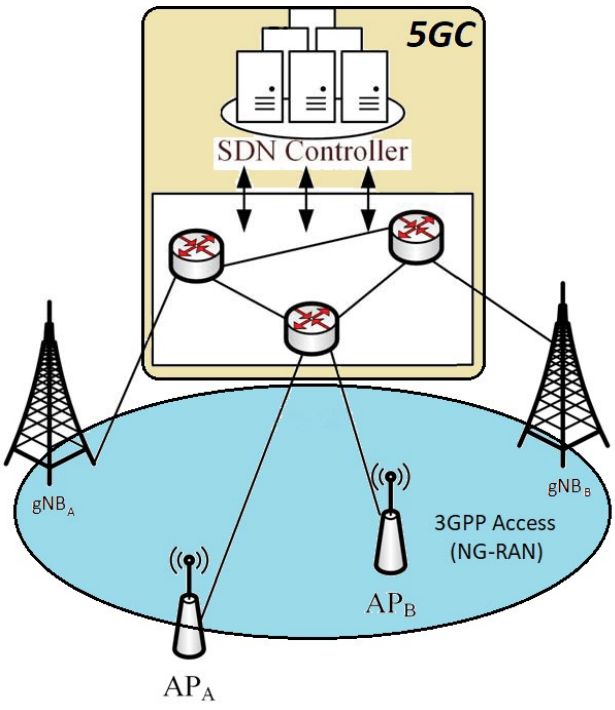

Figure 1: Simplified Architecture of the 3GPP 5G Core and Access Network based on Software-Defined Networking.

all access points (APs), base stations (gNBs), and wireless switches [8]. Implementing the HAM module which is based on SDN functions to monitor user equipment's movements and its previous and next locations. Hence, the HAM can predict the next potential cells from user equipment's movements, locations and it will prepare the potentially relevant cells and access points to make them ready for handover procedure before the user equipment arrives. By using a traffic flow template (TFT) filter, the HAM can collect the physical layer attributes of the UE for storage and analysis of user data. In order to collect user data, pre-initial authentication should be done when the UE connects to the network for the first time.

Consequently, this paper is examining the problem in the SDN-based 5G system which is the handover authentication that is being caused by frequent handovers over small cell deployment. Therefore, we target how handover authentication to be done in a network operated by two different operators namely home network and foreign network.

Attack model

In the nature of the5G network, the devices are resource-constrained which could be usually placed inaccessible and unintended locations without particular surveillance and more vulnerable against any attacks launched by adversaries. Also, compared to conventional equipment which has more resources than the one in the 5G network has more resistance against malicious attacks. The Dolev-Yao intruder model has been used as a threat model in the scheme [15] in order to examine the proposed protocol.

The things that an attacker may have the ability to do are listed below:

1) Eavesdrop on any message exchanged in the network.
2) Impersonate a legitimate principle.
3) Modify, parse, synthesize, imitate, replay or insert any message and send it to a legitimate entity.
4) Decrypt or encrypt messages if obtaining the corresponding secret key.

However, it is believed that there are specific things that the attacker cannot do

1) Predict a nonce chosen from a large enough space.
2) Retrieve the information from a given cipher text or generate a valid cipher text from a given plaintext without a complete and correct key.
3) Calculate a private key with its corresponding public key.

The Proposed Eeap-Tls Scheme

The motivation

In order to design and provide a robust handover authentication scheme for the 5G systems, the EEAP-TLS scheme is designed with novel ideas thanks to SDN's features. Therefore, to increase the security level to defend against malicious attacks, the SDN controller shares the keys with the user equipment only there is a valid request for handover from the UE. Besides, when the UE requests handover, it also sends the information of the base station or the access point that it wants to connect. With that, the SDN controller can check the BS or AP whether legitimate or not. Moreover, after the handover is done, the scheme is utilizing EAP-TLS to supply high security and mutual authentication in a more efficient way.

Overview of EAP-TLS Protocol

One of the crucial requirements of a new wireless network would be mutual authentication between the UE and the authentication authority as the 5G will be more heterogeneous than legacy networks such as 3G, 4G LTE. Due to the EAP-TLS having robust security and mutual authentication, the proposed scheme is utilizing these EAP-TLS features. Also, apart from mutual authentication and its high-security features, the EAP-TLS has other remarkable features, for example, reauthentication (reconnection), fragmentation and reassembly, key exchange, and agreement. In terms of security, EAP-TLS can resist against active attacks such as MitM and replay attacks.

The detailed definition of if EAP-TLS is as follows:

1. It is based on asymmetric key infrastructure known as PKI.
2. It uses a client-side certificate.
3. The certification authority issues the certificate to the UE and authentication server.
4. Communication happens between the UE and authentication server.
5. The UE must have a valid client-side certificate to establish a connection with the authentication server during its lifetime in the network.
6. In order to do verification of the client-side certificate, a certificate should be provided by a certification authority.

Proposed Efficient EAP-TLS Protocol

The proposed scheme aims to have a seamless and efficient handover authentication process. In order to do that, it uses the signed certificate that makes the scheme efficient compared with other EAP-TLS schemes [16]. Therefore, the proposed scheme meets the requirement of a heterogeneous environment in 5G networks. Authentication, key exchange, and agreement are based on EAP-TLS specifications in the scheme. The proposed scheme has two steps of authentication. The first step is pre-initial authentication based on symmetric-key cryptography to get shared keys from the home network. These shared keys will be used by the UE to get a certificate and grant access from the foreign network during the handover process.

Instead of sending the certificate directly to the UE, the UE has to ask for the certificate of the foreign network from the certificate authority. This is one of the main features

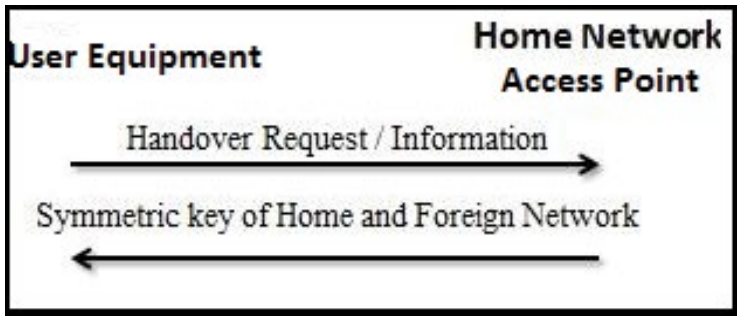

Figure 2: Pre-Initial Authentication.

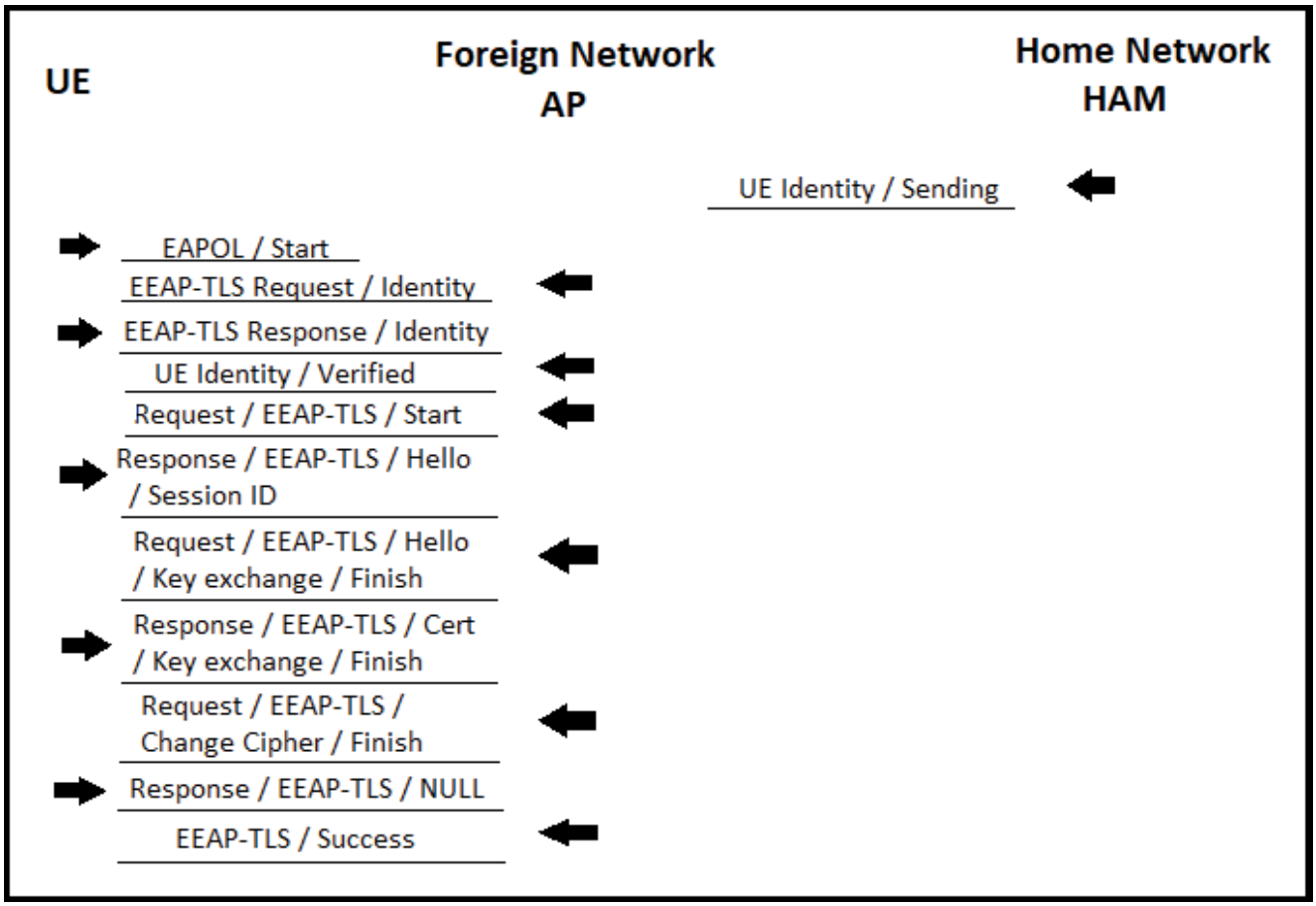

Figure 3: EEAP-TLS Authentication Flow.

of the proposed scheme. Therefore, the identity of the UE has protection against various attacks. The handover authentication process starts from pre-initial authentication as shown in Figure 2 and continues with EEAP-TLS authentication as shown in Figure 3.

Pre-Initial Authentication: When the UE connects to a foreign network's base station or access point, it will send a handover request to its home network eNB with its physical layer attributes to gain access to the foreign network. Then, the HAM checks the next predicted locations of the UE and the information sent by the UE x before sharing the symmetric keys of the Home and Foreign networks. After the verification process is done by the HAM, the home network eNB sends the shared keys as shown in Figure 2.

The Main Part of Handover (Efficient EAP-TLS) Authentication: The UE's identity is shared by the home network eNB to the foreign network AP for the identity verification process. This AP is stated by the UE during handover request before the UE starts the authentication process with the AP as shown in Figure 3. After this point, the UE will send the EAPOL/start packet to the AP. This AP will typically send EEAP-TLS request/identity packet to the UE. The UE responds with its identity information packet to the AP. AP will compare this packet with the information of UE's id which

came from the home network eNB and then verify it once AP receives the UE's identity information. After the verification is done, AP has to, also, send a request of the EEAP-TLS/start packet which is EEAP-TLS packet type and the Start(S) bit set and no data to the UE. The EEAP-TLS conversation will then begin with the UE sending hello message with EEAP-TLS packet type, cipher message, a random number, a session Id to the AP. The AP will then respond with an EAP request packet with EEAP-TLS packet type, hello message, version number, TLS certificate, and acknowledgment for the UE's hello message packet to initiate a key exchange with AP parameters. The UE will then respond with a signed certificate, and the certificate verifies the message, already shared key to the AP for verification. After receiving that packet, the AP will verify the signed certificate and the key, then respond with the finished message which contains the UE's authentication response to the AP. If the verification is successful, the UE responds with a null message after it receives the finish handshake message. The AP will respond with a success message to end this session. As a result, mutual authentication of the EEAP-TLS is successful.

The scenario for the vertical handover process is as follows: Assuming that the UE has SIM and it is registered and a symmetric key is shared by its home network. For instance, a UE is connected to cell A and the next cell it will be connected to is B and cell B is in a foreign network operated by a different operator, therefore, the UE needs to access that foreign network when it moves from its home network. Thanks to the signed roaming agreement, thus, both networks can authenticate each other, and the UE knows the public keys of both networks. Home and foreign networks public keys are shared between these two networks and have a certificate which is issued by the certification authority.

The HAM which is inside the SDN controller will share user identity with the AP of the foreign network according to the UE location before authentication starts. Therefore, the UE identity verification has been done faster on foreign network AP and so, the proposed scheme provides seamless authentication handover, moreover, the handover processing time is reduced by eliminating sending identity verification to the HAM. The HAM will check the list of registered UEs if the UE comes back to its home network back whether it is in the list or not. If the UE is in the list, the access will be given to its home network by HAM (Table 1).

Security Analysis and Validation

Logic proof

One of the basics of security is the authentication protocols, therefore, it is necessary to maintain that authentication protocols are secure and work properly. In this sense, we used Ban Logic [17] which is proposed by Burrows-Abadi-Needham (BAN) is a set of rules for analyzing the logic correctness of information exchange in authentication protocols. The aim of using BAN logic is to determine whether packets or information exchanged between legitimate users are secure, secured against attacks, or both. The expected results of the protocol should be secure by deriving the logical belief of each legitimate entity involved during the handover process. A typical BAN logic verification basically has three steps which are verification of message origin, verification of message freshness, and verification of the trustworthiness of origin. The logical correctness of the EEAP-TLS scheme will be proofed by using BAN logic.

The goal of the proposed EEAP-TLS scheme is to ensure that handover authentication is done correctly, the UE and FeNB are mutually authenticated to each other, and the UE and FeNB have a belief in each other that both of them have the symmetric key. By using Ban Logic, the first step is to convert the protocol messages into an idealized form specified by BAN logic formulas. We apply this logic of

Table 1: Notation used in BAN Logic.

Notations	Description
$P \mid \equiv X$	*P* believes *X*.
$P \lhd X$	*P* sees *X*.
$P \mid \sim X$	*P* once said *X*.
$P \Rightarrow X$	*P* has jurisdiction over *X*.
$\#(X)$	The formula *X* is fresh.
$P \overset{K}{\longleftrightarrow} Q$	*P* and *Q* may communicate with each other using the shared key *K*, which is a good key.
$P \overset{X}{\longleftrightarrow} Q$	The secret formula *X* is only known to *P* and *Q*.
$\{X\}_K$	The formula *X* is encrypted with key *K*.
$\langle X \rangle_Y$	The formula *X* is combined with secret *Y*.

correctness for both parts of the proposed protocol starting with pre-initial authentication and following with a vertical handover authentication process. For simplicity, A, B, and S notations will be used and they stand for, respectively, the UE, FeNB, and HeNB.

The goal of the EEAP-TLS authentication is as follows: $A\equiv A\xleftrightarrow{K_{AB}}B$ *and* $B\equiv A\xleftrightarrow{K_{AB}}B$

The idealization of the proposed protocol is formulated as follows:

Message 4: $A\rightarrow B:[15]_{K_{AB}^{-1}}$

Message 5: $B\rightarrow A:[15K]_{K_{AB}^{-1}}$

Message 6: $A\rightarrow B:\{A\xleftrightarrow{K_{AB}}B,TLS,K'\}_{K_{AB}^{-1}}$

Message 7: $B\rightarrow A:\{TLS,C'\}K_{AB}^{-1}$

The plaintext and messages are omitted because they do not contribute beliefs of recipients as in the first three messages. Assuming that, each entity believes its own messages to be fresh (Table 2). The assumptions for the pre-authentication are shown as follows:

$$S\equiv A\xleftrightarrow{K_{AS}^{-1}}S,\ ,\ S\equiv A\xleftrightarrow{K_{AS}^{-1}}S,$$

$$A\equiv A\xleftrightarrow{K_{AB}^{-1}}B,\ B\equiv A\xleftrightarrow{K_{AB}^{-1}}B,$$

$$A\equiv\#(H_B),\#(TLS),\#(SID'),\#(K),$$

$$A\equiv\#(C'),\#(TLS),$$

$$B\equiv\#(H_A),\#(TLS),\#(SID),$$

$$B\equiv\#(A\xleftrightarrow{K_{AB}}B),\#(TLS),(K')$$

$$A\equiv(S\Rightarrow(A\xleftrightarrow{AB}B)),$$

$$B\equiv(S\Rightarrow(A\xleftrightarrow{K_{AB}}B))$$

The next step is to verify whether the security goal of the proposed scheme has been achieved by using rules of BAN logic. The following presents an analysis of the proposed scheme.

(1) $B\triangleleft\{H_A,TLS,SID\}_{K_{AB}^{-1}}$

From assumption $B\equiv A\xleftrightarrow{K_{AB}^{-1}}B$ and by the message-meaning rule, (1), we get (2):

(2) $B\equiv A\sim\{H_A,TLS,SID\}_{K_{AB}^{-1}}$

From the assumption $B\equiv\#(H_A),\#(TLS),\#(SID)$ and by the freshness conjuncatenation rule and (2), we get (3):

(3) $B\equiv\#(H_A,TLS,SID)$

By (2), (3), and nonce verification rule, we get (4):

(4) $B\equiv A\equiv\{H_A,TLS,SID\}_{K_{AB}^{-1}}$

(5) $A\triangleleft\{H_B,TLS,SID',K\}K_{AB}^{-1}$

From the assumption $A\equiv A\xleftrightarrow{K_{AB}^{-1}}B$ and by the meaning-message rule and (5), we get (6):

(6) $A\equiv B\sim\{H_B,TLS,SID',K\}K_{AB}^{-1}$

From the assumption $A\equiv\#(H_B),\#(TLS),\#(SID'),\#(K)$ and by (6), the freshness conjuncatanation rule, we get (7)

(7) $A\equiv\#(H_B,TLS,SID',K)$

Table 2: BAN Logic Rules.

Notations	Description
Message-Meaning Rule	$\dfrac{P\equiv P\xleftrightarrow{X}Q,P\triangleleft\{X\}_K}{P\equiv Q\sim X}$
Nonce-Verification Rule	$\dfrac{P\equiv\#(X),P\equiv Q\sim X}{P\equiv Q\equiv X}$
Jurisdiction Rule	$\dfrac{P\equiv Q\Rightarrow X,P\equiv Q\equiv X}{P\equiv X}$
Belief Conjuncatenation Rule	$\dfrac{P\equiv X,P\equiv Y}{P\equiv(X,Y)}$
Freshness Conjuncatenation Rule	$\dfrac{P\equiv fresh(X)}{P\equiv fresh(X,Y)}$

By (6), (7), and nonce verification rule, we get (8):

(8) $A\left| \equiv B\right| \equiv \left\{ H_B, TLS, SID', K \right\}_{K_{AB}^{-1}}$

(9) $B \lhd \left\{ A \xleftarrow{K_{AB}} B, TLS, K' \right\}_{K_{AB}^{-1}}$

From assumption $B\left| \equiv A \xleftarrow{K_{AB}^{-1}} B \right.$ and by the message-meaning rule, (9), we get (10):

(10) $B\left| \equiv A \sim \left\{ A \xleftarrow{K_{AB}} B, TLS, K' \right\} K_{AB}^{-1} \right.$

From the assumption $B\left| \equiv \#\left(A \xleftarrow{K_{AB}} B \right), \#(TLS), \#(K') \right.$ and by (10), freshness conjuncatanation rule, we get (11)

(11) $B\left| \equiv \#\left(A \xleftarrow{K_{AB}} B_A, TLS, K' \right) \right.$

By (10), (11), and nonce verification rule, we get (12):

(12) $B\left| \equiv A\right| \equiv \left\{ A \xleftarrow{K_{AB}} B, TLS, K' \right\} K_{AB}^{-1}$

(13) $A \lhd \left\{ TLS, C' \right\}_{K_{AB}^{-1}}$

From the assumption $A\left| \equiv A \xleftarrow{K_{AB}^{-1}} B \right.$ and by (13), message-meaning rule, we get (14):

(14) $A\left| \equiv B \sim \left\{ TLS, C' \right\} K_{AB}^{-1} \right.$

From the assumption $A\left| \equiv \#(C'), \#(TLS) \right.$ and by (14), the freshness conjuncatanation rule, we get (15):

(15) $A\left| \equiv \#\left(TLS, C' \right) \right.$

By (14), (15), and nonce verification rule, we get (16):

(16) $A\left| \equiv B\right| \equiv \left\{ TLS, C' \right\} K_{AB}^{-1}$

Therefore, by using the nonce verification rule and (9), (10), (11), we infer (17):

(17) $A\left| \equiv B\right| \equiv \left\{ A \xleftarrow{K_{AB}} B \right\} K_{AB}^{-1}$

By the jurisdiction rule, and assumption $A\left| \equiv (S\left| \Rightarrow \left(A \xleftarrow{K_{AB}} B \right) \right.) \right.$ and (17), we obtain (18):

(18) $A\left| \equiv A \xleftarrow{K_{AB}} B \right.$

From message 6, with a similar method, we can get (19)

(19) $B\left| \equiv A \xleftarrow{K_{AB}} B \right.$

By verifying the validity of the symmetric key which is obtained from the home network, thus, A and B have mutual authentication and key agreement. Therefore, we have achieved the goal of the proposed scheme.

Security analysis

1. **Mutual authentication:** Because the proposed scheme is utilizing EAP-TLS specifications, the scheme has a robust mutual authentication between the UE and both home and foreign networks. During the pre-initial authentication procedure, the UE challenges the HAM with a handover request. Since the HAM can share the shared key with the UE, thus, accessing the foreign network will be granted with that key to the UE.

2. **User identity protection:** The UE can only get access to the foreign network with a valid certificate. To get the certificate, the UE must request to get it. When a new certificate is being issued, timestamp, random variable, the location of the UE is hidden and untraceable. A temporary ID can protect users' identities and is created with a generated random variable for each registered user. Besides, this temporary ID will be changed randomly to make the registered user is untraceable. There is only one entity to know the predicted and the exact location of the UE is the HAM in the SDN controller. Thus, the identity of the UE cannot be disclosed.

3. **Signaling overhead:** The proposed scheme is based on EAP-TLS specification and its features. However, authentication in EAP-TLS occurs between an authentication server and a user. On the other hand, authentication in the proposed scheme occurs between foreign network AP and the UE. Moreover, verification of user ID is shortened with no additional round-trip delays thanks to SDN-enabled 5G networks.

4. **Passive attack:** Because this type of attack does not intervene in the communication channel itself, the attacker cannot decrypt the messages without the private key even though it can obtain valid packages. To generate keys SHA-1 hash function is used. Hence, it becomes hard to tamper with decryption messages without the corresponding private key. So, the scheme has protection against passive attacks.

5. **MitM attack:** A man-in-the-middle attack is an active attack. The proposed scheme can resist against MitM attacks because the user identity is protected by a temporary public key pair that is generated by the UE and it is unknown by other entities so that it cannot be obtained or changed by the attacker. Also, thanks to the SDN-enabled system the HAM has a global network view and can know and predict the location of the UE, in this way, it shares the user identity for verification with foreign network AP if there is a valid handover request from the UE. Thus, the scheme has protection against MitM attacks as well.

6. **Impersonation attack:** An impersonation attack is a kind of attack that an attacker can hide itself as one of the legitimate entities in the system. Since all user equipment is considered to be registered with SDN, if an attacker mimics a UE in the network, the SDN checks the identity and associated address to determine whether it is legal. When a UE moves from one access point or another, HAM will assign a new ID to this UE to communicate more when the UE returns to its original network. SDN will then delete the old UE from the UE's ID list. In this case, the attacker cannot hide itself as a valid UE that still uses the old UE ID (Table 3).

7. **Compromised attack:** According to the proposed scheme, if a UE's ID is compromised, the attacker cannot further threaten the system because the message sent by a BS or AP is all encrypted with a symmetric key shared

Table 3: Comparison between The Proposed and Existing Authentication Protocols.

Parameters	EEAP-TLS	EAP-TLS	EAP-TTLS	PEAS
Server Aut.	PKI Certificate	PKI Certificate	PKI Certificate	PKI Certificate
Mutual Aut.	Yes	Yes	Yes	Yes
UE Aut.	By the certificate	By the certificate	By the certificate	By the certificate
User Identity Protection	Yes	No	No	No
Roaming Capability	Yes	No	No	No
MitM	No	No	Rare cases	Rare Cases
Reply Attack	No	No	No	No
DDoS	No	No	No	No
Impersonation	No	No	No	No
Fast Connection	High	High	Low	Low

between the UE and HAM. The attacker cannot decrypt the message to receive the transmitted information. If the access point is compromised, the attacker can only receive the message sent to this access point. Because each BS and AP has a unique symmetric key shared with SDN, the effects of the compromise attack may be limited. With enough storage and computing capacity, SDN can operate more complex security mechanisms to ensure its security. It is assumed that the proposed protocol is safe.

8. **Reply attack:** One of the examples of an active attack is a reply attack where an attacker re-sends the current transmitted messages to the recipient maliciously. Replay attacks with the proposed scheme can be avoided by using the nonce mechanism. Suppose an attacker receives one of the forwarded messages and sends them again and again. The receiver will compare the received timestamp with the one stored in the memory. If the foreign network AP has a value that is not the same as that received, the message is considered invalid and ignored. Also, because the forwarded messages are not transmitted in plain text and are encrypted in the message, the attacker cannot change or delete the encrypted text.

The existing protocols such as EAP-TLS, EAP-TTLS, and PEAS also provide mutual authentication to have secure communication. Also, these protocols use certificate-based authentication to increase security for the UE. However, the way these protocols generate a certificate and management of it creates overheads to the system. Besides, these existing protocols do not have user identity protection. That makes the UE traceable. In Table 3, a detailed comparison is given to draw a clear picture between the proposed scheme and the existing protocols in terms of security, authentication capabilities, and the table shows which features each protocol has and whether there are certain security attacks on each protocol.

Formal verification

In this sub-section AVISPA (Automated Validation of Internet Security Protocols and Applications) tool [18] is used to do security analysis and validation of the proposed Efficient EAP-TLS protocol. This tool was chosen because; first of all, it is a push-button tool that provides a modular and expressive formal language and applies various protocol analysis techniques. Secondly, it can be used to model and analyze security protocols, and lastly, it is one of the most common and sensitive tools among other security analysis tools. Validation of the proposed EEAP-TLS scheme in AVISPA is done by using The OFMC (On-the-the-Model-Checker) and The ATSE (Constraint-Logic-based Attack Searcher) back ends. One of the most important features of the OFMC backhand is to try to prove whether there are security vulnerability points in the protocol instead of proving that the protocol is safe.

The Dolev-Yao (DY) intrusion model is used to analyze the proposed scheme under attack and to test whether it is protected against many different attacks. If there is an attack to break the protocol, the output will show UNSAFE, otherwise, the protocol is SAFE will be shown.

The HSPSL (High-Level Protocol Specification Language) is used in AVISPA to test and analyze the proposed scheme. There is also a SPAN (Security Protocol Animator) tool to simulate and analyze the proposed scheme to check if the scheme is secure. Also, the vulnerable points in the protocol can be easily found when the protocol is not safe by using it. The results of these simulations are illustrated as shown in Figure 4 for the OFMC (On-the-Fly-Model-Checker) and as shown in Figure 5 for the ATSE (Constraint-Logic-based Attack Searcher). Hence, the proposed scheme is found safe according to the Doley-Yao (DY) intrusion model.

The result shown in Figure 4 shows that the proposed scheme is safe in the OFMC backend, and goals are achieved as specified. Also, the result shown in Figure 5 shows that the proposed scheme is safe in the ATSE backend, and goals are achieved.

Performance Evaluations

Efficiency analysis

In this section, we analyze the total system delay of the

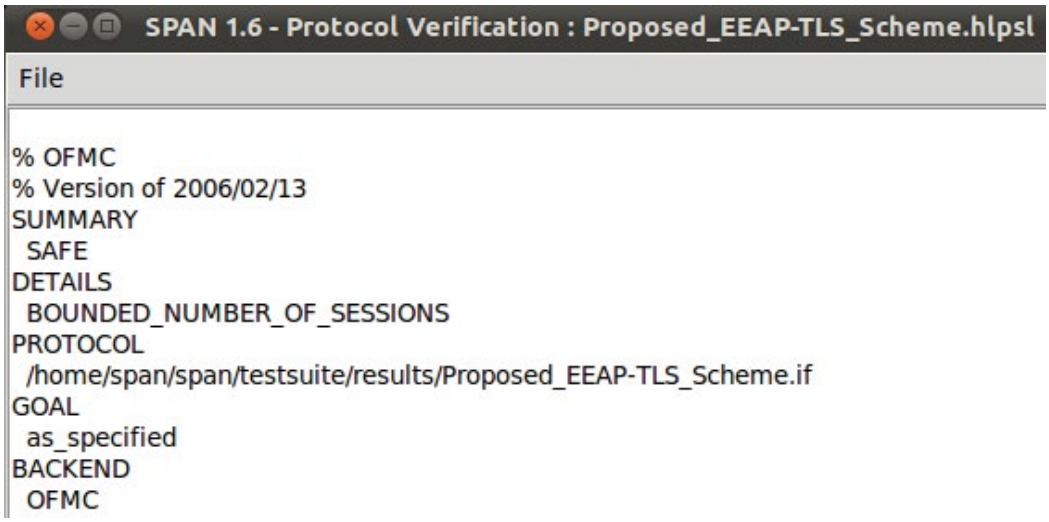

Figure 4: The result of the OFMC backend.

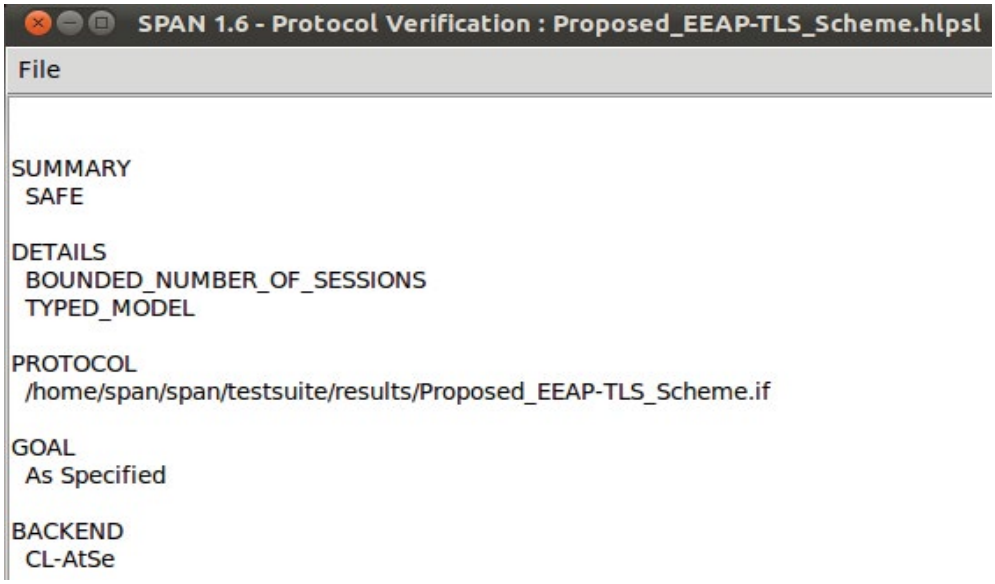

Figure 5: The Result of the ATSE Backend.

Table 4: Definition of Notations.

Parameters	Description
$T_{UE\text{-}FeNB}$	Transmission Delay Between UE and FeNB
$S_{UE\text{-}ENC}$	Encryption Time of UE key
$S_{FeNB\text{-}DEC}$	Decryption UE message in FeNB
P_{UE}	Delay in processing message from UE
P_{SUM}	Total System Delay for processing
T_{SUM}	Total System Delay for transmission
T	Total System Delay

proposed scheme. The notations used in this evaluation are shown in Table 4. The parameters to calculate processing delay, transmission delay, and the total delay of the whole system are given. According to the proposed scheme, the total system delay in the vertical handover authentication process is shown as follow (Table 4):

Total system delay for transmission is given by $T_{SUM} = T_{UE\text{-}FeNB}$

Total system delay for processing is given by $P_{SUM} = P_{UE} + S_{UE\text{-}ENC} + S_{FeNB\text{-}DEC}$

Therefore, the total system delay is given by $T = T_{SUM} + P_{SUM}$

Since the delay of asymmetric cryptography is heavier than symmetric cryptography and small cell APs are resource-constrained, asymmetric cryptography is not used in the handover process. Though the improvement comes from the UE identity verification process, and if we compare with STAVHO [16], since there is no identity verification process time which is $T_{UE\text{-}IDverify}$ and delays, P_{FeNB}, due to the processing message from FeNB in eNB in our proposed scheme thanks to SDN capabilities our authentication scheme has less delay. The comparison of the total time delay of the whole protocol between EEAP-TLS and STAVHO is shown in Figure 6.

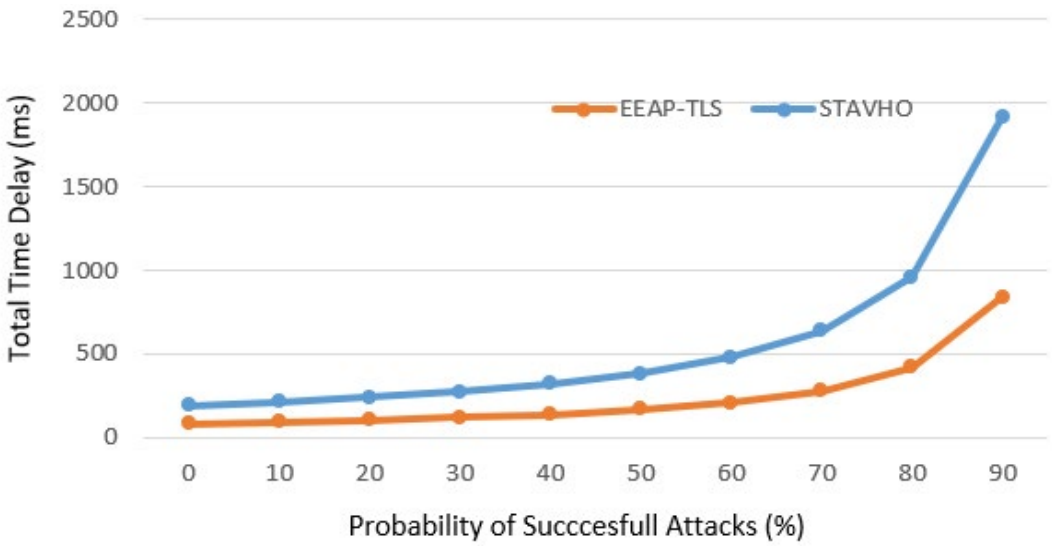

Figure 6: Total Time Delay of whole Protocol.

Performance analysis

In this section, there will be comparisons of computation and transmission overhead between the proposed scheme EEAP-TLS and the existing relevant schemes. MATLAB R2018b is used to conduct the performance evaluation. The applied cryptographic algorithms which are hash function SHA-256, symmetric encryption AES-128, and ECDSA-160 are implemented. Additionally, the simulations have been done at least 11 times to obtain the average value of each cryptographic operation.

Computational overhead: In this subsection, MATLAB is used to analyze the computation overhead of the proposed scheme. The simulation results are in [19] and [20] are used to calculate the time of cryptographic operations. The average time of cryptographic algorithms operation is shown in Table 4. The time for generating of ECC private/public key pair and calculating an ECSH key are respectively T_G = 550 ms and T_{ECDH} = 500 ms. Therefore, if the total computational overhead is calculated for the EEAP-TLS and STAVHO [16] schemes, the results would be 7.78s for EEAP-TLS and 9.209s for STAVHO.

Although EEAP-TLS has been proven to be secure enough against attacks, any other types of malicious attacks, in addition to that unpredictable attacks, may cause interruption of the implementation of the protocol during the handover process. Therefore, it is assumed that any kind of attack may be random at any stage of the protocol implementation during the handover process. If an attack is successfully violated in the process, the protocol cannot continue. As the number of successful attacks increases, the average total time delay will take longer to fully implement the protocol.

Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) is a robust authentication mechanism and because it supports a large number of cipher suites, it has been used in 3G and 4G HetNet environments, and it is supported by public key infrastructure (PKI). EAP-TLS protocol aims to provide a robust authentication mechanism to users

Table 5: The Average time for Cryptographic Algorithms Operation.

Name of Operation	Algorithm	Average Time
Hashing	SHA-256	T_H = 0.286 ms/byte
Encrypting/Decrypting	AES-128	T_{AES} = 0.177 ms/byte
Generation/Verification	ECDSA-160	T_S = 520 ms & T_V = 1020 ms

in the 5G HetNet environment as well. In 5G architecture, the UE must be initially authenticated and registered by the SDN (Software Defined Networking) controller and HAM (Handover Authentication Mechanism). When the UE is in the foreign network, handover authentication information starts to exchange between HAM and UE, and UE will authenticate to a foreign network via EAP-TLS protocol (Table 5).

We should measure the number of authentication messages for the calculation of authentication time for EAP-TLS and make a comparison between our proposed protocol and STAVHO which is for vertical handover authentication for 4G HetNets. The total number of authentication messages for EAP-TLS is the sum of its authentication messages. Therefore, IEEE 802.1x-EAP-TLS [21] has 21 control messages. When a registered user roams to a foreign network, the same number of authentication messages are exchanged. In [22], the calculation of signaling cost is based on authentication messages for registration updates. The signaling cost can be found as the cumulative traffic load (number of hops × message size) for exchanging signaling messages during the communication session. Assuming a number of hops between UE and foreign network base station is 1.

The average message size 'R' is set to 200 bytes and the average session time "Ts" is set to 2000s. Tr which is the average communication time varies from 10 to 100s. N_p = Ts/Tr is the average number of UE movements during a communication session. The number of messages exchanged between the UE and FeNB is $d_{UE\text{-}FeNB}$ = 21. Thus, the authentication signaling cost (C) is as follows,

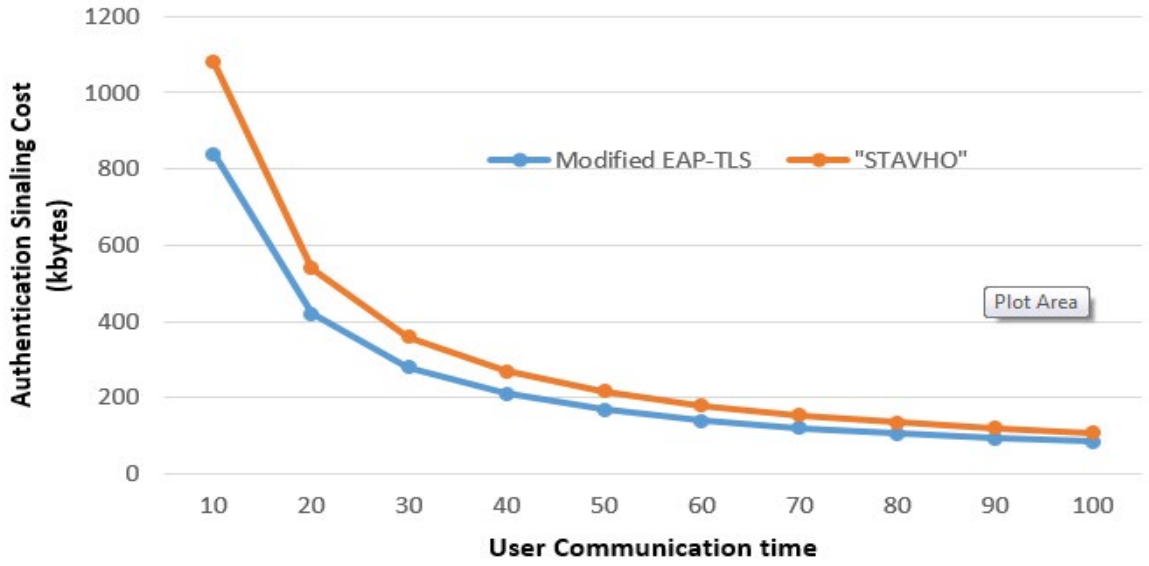

Figure 7: Comparison between EEAP-TLS and STAVHO.

$S_{EAP-TLS} = d_{UE-FeNB} * R * N_P$

From the equation above, we can make a comparison between our proposed EEAP-TLS protocol and STAVHO [16] which is a proposed protocol for vertical handover authentication 4G HetNets. The comparison of authentication signaling cost can be found below in Figure 7. As seen in figure 11, our proposed protocol has reduced authentication overhead cost by more than 25 percent for each time interval.

Transmission overhead: With the vision of the 5G and because of small cell deployment not only new base stations or access points will be resource-constrained but also, 5G devices such as IoTs are resource-constrained. However, since the number of connected devices will be 100 times higher than 4G LTE networks, the cost of energy will be much higher. So, the packet length should be as short as possible to keep the energy consumption as low as possible of the entire 5G network [23]. In the proposed scheme, the simulation results in [19] have been used to calculate the energy consumption of the transmission. Therefore, the transmission overhead for receiving (RX) is 2.631 µJ/byte, and transmitting with 0 dBm power level (TX 0 dBm) is 4.318 µJ/byte.

The evaluation of the energy cost of transmission of data is considered within the 5G wireless network communication as wired communication which is not the 5G network is not considered. Therefore, after the calculation of the total transmission overhead cost of the EEAP-TLS scheme is found as 1.405 mJ.

The total transmission overhead cost of the STAVHO scheme is 2.163mJ which is much higher than the proposed scheme (Table 6). The comparisons of the energy cost between EEAP-TLS and STAVHO are shown in Figure 8.

Comparison of handover operations: The proposed scheme EEAP-TLS is compared with STAVH [16] in terms of handover processes as shown in Table 5. In [24], which is the proposed scheme, a handover authentication scheme is proposed to accomplish a rapid handover process for authentication by using SDN technology underlying in the architecture. However, the pair-wise master key which is shared between all the BSs and APs is neither safe nor scalable. If an attacker can compromise one of the base stations, devices using the same pair wise master key will all be exposed in this network.

However, the symmetric key can only be used in if the mobile device roams in the service area of one of the neighbors' APs. For instance, assume that there are *m* potential target APs for the HAM module, the AP must generate *m*keys, which is energy consuming for the resource-constrained devices in the network.

In the proposed scheme, since the location of the user equipment and the base station or the access point the user equipment wants to connect is known by sending a request to authentication authority to get the symmetric key of the foreign network. Therefore, there will be only one key is generated and used, hence, authentication handover would be fast and secure enough to access foreign networks.

Conclusion

In this paper, the expectations of new wireless mobile networks have been discussed by explaining the requirements of the 5G and the reasons why it will be more heterogeneous than the legacy network. Also, the emerging technologies have been addressed to explain how to meet those requirements of the 5G. Because of the heterogeneity and densified small cell deployment of the 5G, frequent handoffs will be inevitable. Therefore, there is a need for a fast and efficient enough handover authentication scheme to make sure that low latency is maintained. Also, a smooth and secure transfer registration authentication scheme is required. The reason is that users often move from one network to another. This will lead to serious security vulnerabilities against various attacks. Hence, a robust vertical handover authentication scheme is

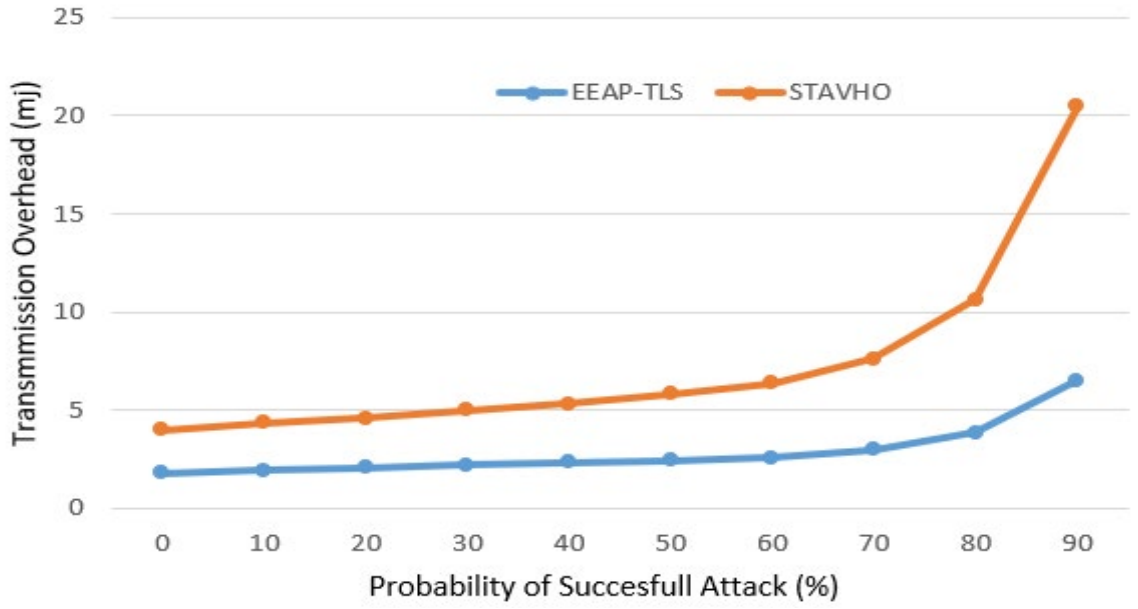

Figure 8: Comparison of Transmission Overhead.

Table 6: Handover Comparison.

The Protocol	Type of Cryptosystem	# of Message Exchange During Handover	Same Pairwise Session Keys
STAVHO [15]	Symmetric	6	Yes
EEAP-TLS [23]	Symmetric	2	No

proposed with having efficiency by using a certificate-based authentication that has symmetric key distribution utilizing the EAP-TLS features to ensure the UE gets the certificate to access the foreign network. The proposed scheme architecture has a global network view thanks to the SDN paradigm, moreover, having the HAM module can ensure seamless and secure vertical handover. As for many emerging industries, it is expected that the use of SDN-enabled security mechanisms. For security verification and analysis, the SPAN-AVISPA tool is used and the result of simulations and analyzes show that the proposed scheme is safe and verified. Moreover, BAN Logic is used for analyzing the logic correctness of information exchange in authentication protocols. The performance analysis shows that the proposed protocol can meet latency requirements and it is compared with another scheme to show the improvement of the proposed scheme. All in all, based on the vision of 5G wireless networks, it will be used in many industry areas such as UAV systems, vehicle communication, mobile fog calculation, small cell smart grids, and e-health services, etc.

Acknowledgment

This work is supported by the MOE AcRF Tier 1 funding for the project of RG 26/18 by the Ministry of Education, Singapore.

References

1. Agiwal M, Roy A, Saxena N (2016) Next generation 5G wireless networks: A comprehensive survey. IEEE Communications Surveys & Tutorials 18: 1617-1655.
2. Ahmad I, Kumar T, Liyanage M, et al. (2018) Overview of 5G security challenges and solutions. IEEE Communications Standards Magazine 2: 36-43.
3. Zhang P, Yang X, Chen J, et al. (2019) A survey of testing for 5G: Solutions, opportunities, and challenges. China Communications 16: 69-85.
4. Fang D, Qian Y, Hu RQ (2017) Security for 5G mobile wireless networks. IEEE Access 6: 4850-4874.
5. Yao J, Han Z, Sohail M (2019) A Robust Security Architecture for SDN-Based 5G Networks. Future Internet 11: 85.
6. Sarraf S (2019) 5G Emerging Technology and Affected Industries: Quick Survey. American Scientific Research Journal for Engineering, Technology, and Sciences (ASRJETS) 55: 75-82.
7. Lien SY, Tseng CC, Moerman I, et al. (2019) Recent Advances in 5G Technologies: New Radio Access and Networking. Wireless Communications and Mobile Computing.
8. Redana S, Kaloxylos A, Galis A, et al. (2016) View on 5G Architecture. White Paper of the 5G-PPP architecture WG.
9. Duan X, Wang X (2015) Authentication handover and privacy protection in 5G hetnets using software-defined networking. IEEE Communications Magazine 53: 28-35.
10. Basin D, Dreier J, Hirschi L, et al. (2018) A formal analysis of 5G authentication. in Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security 1383-1396.
11. Wang M, Yan Z (2017) Privacy-preserving authentication and key agreement protocols for D2D group communications. IEEE Transactions on Industrial Informatics 14: 3637-3647.

12. Ma T, Hu F (2019) A Cross-layer Collaborative Handover Authentication Approach for 5G Heterogeneous Network. Journal of Physics: Conference Series.

13. Simon D, Aboba B, Hurst R (2008) The EAP-TLS authentication protocol.

14. Technical specification group services and system aspects; system architecture for the 5g system; (release 16). 3GPP TR23.501, 2019.

15. Dolev D, Yao A (1983) On the security of public key protocols. IEEE Transactions on information theory 29: 198-208.

16. Prasad M, Manoharan R (2017) A secure certificate based authentication to reduce overhead for heterogeneous wireless network. 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS) 1-5.

17. Burrows M, Abadi M, Needham RM (1989) A logic of authentication. Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences 426: 233-271.

18. von Oheimb D (2005) The high-level protocol specification language HLPSL developed in the EU project AVISPA. Proceedings of APPSEM 2005 workshop 1-17.

19. Piotrowski K, Langendoerfer P, Peter S (2006) How public key cryptography influences wireless sensor node lifetime. Proceedings of the fourth ACM workshop on Security of ad hoc and sensor network 169-176.

20. Backes W, Cordasco J (2010) Mote AODV-an AODV implementation for Tiny OS 2.0. IFIP International Workshop on Information Security Theory and Practices 154-169.

21. Yang CC, Chu KH, Yang YW (2006) 3G and WLAN interworking security: Current status and key issues. International Journal of Network Security 2: 1-13.

22. Narmadha R, Malarkkan S (2011) Performance Analysis of Modified EAP-AKA Protocol Based on EAP-TLS for Beyond 3G Wireless Networks. Networking and Communication Engineering 3: 1-6.

23. Zhang K, Mao Y, Leng S, et al. (2016) Energy-efficient offloading for mobile edge computing in 5G heterogeneous networks. IEEE Access 4: 5896-5907.

24. Ozhelvaci A, Ma M (2018) Secure and Efficient Vertical Handover Authentication for 5G HetNets. 2018 IEEE International Conference on Information Communication and Signal Processing (ICICSP).

DOI: 10.36959/447/358