International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

An Efficient and Secure Authentication and Key Agreement Protocol of LTE Mobile Network for an IoT System

Mariya Ouaissa[1]* Mariyam Ouaissa[1] Abdallah Rhattoy[2]

[1]*Information and Communication Systems Engineering Research Team, High School of Technology,*
Mathematical Modeling and Computer Science Laboratory,
Ecole Nationale Supérieure des Arts et Métiers Moulay-Ismail University, Meknes, Morocco
[2]*Department of Computer, Information and Communication Systems Engineering Research Team,*
High School of Technology, Moulay-Ismail University, Meknes, Morocco
* Corresponding author's Email: mariya.ouaissa@edu.umi.ac.ma

Abstract: The Internet of Things (IoT) is a new concept that is developed considerably in current wireless communications. The main idea of this paradigm is the exchange of information and data from real-world devices with the internet by using unique addressing systems can communicate and interact with each other to achieve common objectives. With the emergence of next generation battery-powered of smart mobile phone, open source application platforms, security and the terminal's energy consumption have become big issues. Long Term Evolution (LTE) is one of the most popular 4th Generation (4G) technologies defined by 3rd Generation Partnership Projects (3GPP) also IP Multimedia Subsystem (IMS) is a prominent architectural framework for multimedia services delivery in 4G/5G networks. In this paper, we focus on IoT security in particular, we explore authentication that is a critical security mechanism which accords authorized users access to a network. It is observed that the end user requires two authentication steps to access multimedia services. The first is the LTE network layer authentication, and the second is the IMS service layer authentication. The authentication steps utilize energy and are carried out using the Authentication and Key Agreement (AKA) protocol. As defined by 3GPP, IMS- Authentication and Key Agreement protocol (IMS-AKA) is the official authentication procedure in IMS and the standard EPS-Authentication and Key Agreement protocol (EPS-AKA) is proposed to provide the authentication service between the device and the network in Evolved Packet System (EPS) system. However, the procedures are prone to different weaknesses both on security and performances aspects. This paper proposes a secure and efficient AKA protocol that authenticates the user on both the network layer and the service layer without double execution the AKA protocol, simplifies the authentication steps, protects user's identities and reduces the authentication process complexity due to the use of Elliptic Curve Cryptography (ECC). The proposed solution was checked by the security protocol verification tool, Automated Validation of Internet Security Protocols and Applications (AVISPA), which indicated that it is a very secure level. Simulation results showed that our proposed compared to IMS-AKA and EPS-AKA offers better performances in terms of energy consumption and storage cost.

Keywords: IoT, LTE, IMS, 3GPP, Authentication, ECC, Energy consumption.

1. Introduction

The things include not only communication devices, but also physical objects, like cars, computer, and home appliances, which are controlled through wireless communication networks. Smart connectivity of the existing networks and context-aware computation using system resources is the substantial part of the internet of things (IoT). Therefore, IoT technologies make machines smarter capable of processing data intelligently and make communication more effectively and efficiently [1].

Furthermore, IoT is a variety of things (devices), such as Radio Frequency Identification (RFID), sensors, actuators, mobile phones, drone, etc., to communicate with each other and work together for common goals. In addition, IoT is an innovation in the field of wireless communication where many intelligent agents are involved sharing information, making collaborative decisions and accomplishing tasks in an optimal manner. However, big data processing consumes high power. Numerous demands for energy will place new stresses on the society and the environment. To fulfil the smart world development, it became necessary to reduce energy efficiency and power consumption in IoT environment [2].

Traditionally, telecommunication networks followed the vertical integration paradigm, which means that each access network has its own services, features of control and its own terminals and if a service is extended from a given access network to another network, this requires a complete reimplementation of the service and a rehabilitation of the control infrastructure, so it supports the new service. However, with the increasing of users demands for new innovative and varied services and difficulty in maintaining every time a new service was added. The 4th Generation (4G) mobile access network and the core network are evolving towards a common Internet Protocol (IP) based secure and fast transport layer. Within the core network of Long Term Evolution (LTE) [3], the IP Multimedia Subsystem (IMS) [4] is the candidate for providing the next generation wired and wireless Packet Switched Networks (PSN) with multimedia services (i.e., audio, video, text, image, and combinations). However, the future IoT causes different challenges among them we can cite the security of communication and privacy of users. In this paper, we focus on the authentication that is a critical security mechanism that accords authorized user’s access to a network [5]. It is observed that a LTE user device carries out two authentication steps to get access to the multimedia services and this increases authentication complexity and the terminal’s energy consumption. LTE and IMS were both defined by 3rd Generation Partnership Projects (3GPP). In order to access the multimedia services, LTE users have to be authenticated in both the LTE network layer and the IMS service layer. As defined by 3GPP, to access the IMS network and benefit from its services, users must be authenticated by using IMS-Authentication and Key Agreement (IMS-AKA) protocol and the standard EPS-Authentication and Key Agreement (EPS-AKA) protocol is proposed to provide the authentication service between the device and the network in Evolved Packet System (EPS) system.

The procedure of the EPS-AKA, takes place before the establishment of security. During this procedure, the user and the network exchange messages without any protection such as authentication request messages, AKA messages, and authentication data. This opens the way for the different types of attacks that can be made against the disclosure of the identity of the user, messages exchanged or functions used during the EPS-AKA. On another side, The IMS-AKA protocol suffers from some limitation and vulnerable to a Denial of Service (DoS) attack.

Both AKA procedures defined by 3GPP suffer with different weaknesses on security (disclosure of identities) and on performances (complexity) aspects. In this paper, we propose an improved AKA authentication protocol to reduce energy consumption and increase security. A proposed binding of the network layer and service layer authentication by using the IP Multimedia Private-user Identity (IMPI) number to avoid the double execution of the AKA protocol. Furthermore, we adopt a novel mechanism based on the Elliptic Curve Cryptography (ECC) technique to ensure the mutual authentication, confidentiality and integrity aspects. Energy consumption and security against several attacks were modelled and the results are provided in this work.

The remainder of the paper is organized as follows: the next section exposes the network architecture and basic methods used in our protocol. Section 3 describes the 3GPP defined security architecture. A detailed description of the proposed protocol is provided in section 4. In section 5, the security of the designed protocol is analyzed. Section 6 presents an analysis of the energy cost. Finally, we draw our conclusions in section 7.

2. Background

In this section, we introduce the network architecture and we present basic methods used in our protocol.

2.1 System architecture

LTE and IMS were both defined by 3GPP and the integrated system architecture is shown in Fig. 1.

The Evolved Packet System (EPS) network supports data services, where services "circuit" migrate to "package" services. It provides IP connectivity between the (User Equipment) UE or IoT Device and the Packet Data Network (PDN) and provides support different radio access networks. The access network, called LTE or Evolved

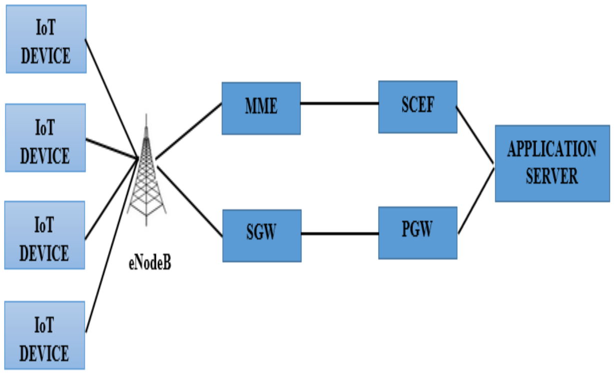


Figure.1 System architecture

UTRAN (E-UTRAN), is composed of nodes Evolved NodeB (eNodeB). The Evolved Packet Core (EPC) consists of several nodes, which are the Mobility Management Entity (MME), the Home Subscriber Server (HSS), the Serving Gateway (SGW) and the PDN Gateway (PGW) [6]. Serving CSCF (SCSCF) is a Session Initiation Protocol (SIP) server and the signaling plane's central node, which registers users and provides services to them. The Interrogating CSCF (ICSCF), a SIP proxy located at the edge of the home network, takes part in user roaming. The HSS is the master user database that supports the IMS network entities to handle calls/sessions. It contains subscription-related information (i.e., user profiles), and performs authentication and authorization of the user [7].

Observe that the home IMS core network (where the HSS and the SCSCF are located) and the Application Server(s) reside within the same administrative domain. In case of roaming, only the (visiting) UE is outside this home network. The user gets her IP connectivity through a remote access network and establishes a SIP session using the Proxy CSCF (PCSCF) of the visited IMS core. More importantly, the user is using the same Application Servers from her home network and her services remain home IMS-based.

2.2 Elliptic curve cryptosystem (ECC)

The security of the ECC is based on the Elliptic Curve Discrete Logarithm Problem (ECDLP), if we have a point P on an elliptic curve EC, then it is easy to calculate the multiplication of points Q = k × P for any integer k, but it is very difficult to find the value of k when we only know P and Q. In ECC, the elliptic curve equation is defined as the form of Ep(a, b) : y2 = x3 + ax + b(mod p) over a finite field of p elements Fp where the points a, b ∈ Fp and $4a^3 + 27b^2 \neq 0 (\mathrm{mod}\ p)$ [8].

ECC is mainly used for data encryption, digital signature, pseudo-random number generation, and many others. Among the most well-known cryptographic schemes are the Elliptic Curve Digital Signature Algorithm (ECDSA) or the Elliptic Curve Diffie-Hellman (ECDH) exchange protocol.

ECDH is a key agreement protocol that allows two parties to establish a shared secret key that can be used for private key algorithms. Both parties exchange public information with each other. Using these public data and their own private data, these parts calculate the shared secret. Any third party, who does not have access to the private details of each device, will not be able to calculate the shared secret from the available public information. An overview of the ECDH process is defined below [9].

To generate a shared secret between A and B using ECDH, both must agree on the parameters of the Elliptic Curve domain on the F2m field.

The domain settings are:

m: is an integer defined for the finite field F2m.

f(x): is the irreducible polynomial of degree m used for elliptic curve operations

a and b: are the parameters defining the curve chosen for cryptographic operations.

n: is the order of the elliptic curve.

Both ends have a key pair consisting of a private key d (a randomly chosen integer less than n, where n is the order of the curve, an elliptic curve domain parameter) and a public key:

$$Q = d \times G \tag{1}$$

G: the generator point, an elliptic curve domain parameter.

Let (dA, QA) be the private key-public key pair of A and (dB, QB) the private key-public key pair of B.

The end A calculates:

$$K = (xK, yK) = dA \times QB \tag{2}$$

The end B calculates:

$$L = (xL, yL) = dB \times QA \tag{3}$$

Since dAQB = dAdBG = dBdAG = dBQA

Therefore K = L and hence xK = xL

Hence the shared secret is xK.

Since it is virtually impossible to find the private key dA or dB from the public key K or L, it is not possible to obtain the shared secret for a third party.

3. 3GPP security architecture

This section presents the security in LTE and IMS networks by explain the process of EPS-AKA

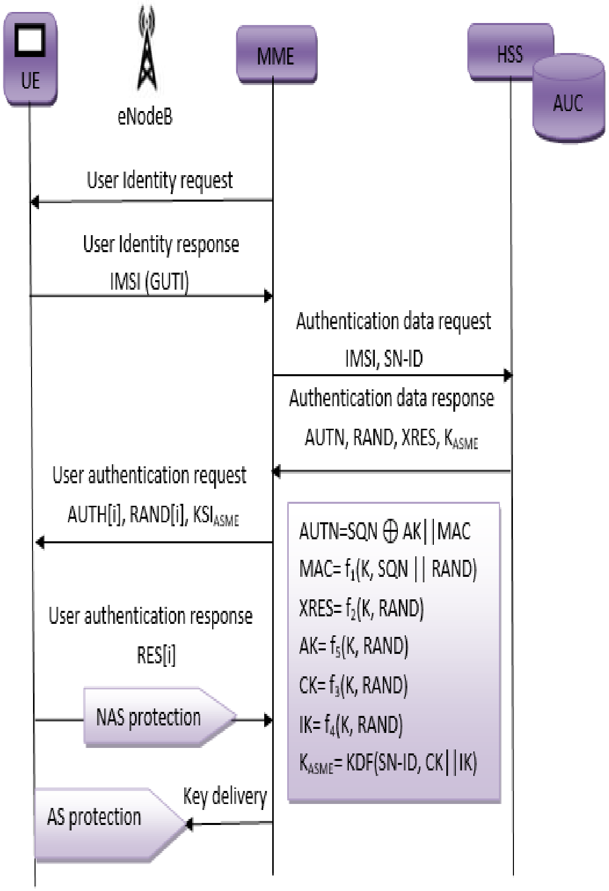

UE
eNodeB
MME
HSS
AUC
User Identity request
User Identity response
IMSI (GUTI)
Authentication data request
IMSI, SN-ID
Authentication data response
AUTN, RAND, XRES, K_{ASME}
User authentication request
AUTH[i], RAND[i], KSI_{ASME}
AUTN=SQN ⊕ AK||MAC
MAC= f_1(K, SQN || RAND)
XRES= f_2(K, RAND)
AK= f_5(K, RAND)
CK= f_3(K, RAND)
IK= f_4(K, RAND)
K_{ASME}= KDF(SN-ID, CK||IK)
User authentication response
RES[i]
NAS protection
Key delivery
AS protection

Figure.2 EPS-AKA procedure

and IMS-AKA procedures used to realize mutual authentication between the user and the network.

3.1 Authentication in the LTE network

The AKA protocol for UMTS has been adopted by 3GPP and proposed at the network to authenticate 3G mobile subscribers and also to address the vulnerabilities of the Global System for Mobile (GSM) system. Due to a major modification of the 4G LTE architecture, the AKA has been replaced by a new protocol (EPS-AKA) based on its predecessor to ensure compatibility with earlier versions. In this paragraph, the EPS-AKA procedure is described, as well as the key derivation procedure and the functionality of the keys used [10].

3.1.1. EPS-AKA protocol

In the EPS-AKA protocol, as shown in Fig. 2, the UE first sends an access request message to the MME, then the MME initiates an authentication procedure by querying the identity of the user [11].

When the UE returns its identity by sending its International Mobile Subscriber Identity (IMSI), the service network sends an authentication data request message containing the identity of the UE to the HSS for the acquisition of authentication vectors. All AV (Authentication Vector) consists of four parameters, XRES, AUTN, the K_{ASME} intermediate key (based on Confidentiality Key (CK) and Integrity Key (IK)) and other parameters such as SN ID (the identity of the network service) and RAND. The HSS server generates AVs for the MME and returns an authentication request message including the generated AVs. Upon receipt of the AVs, the MME sends RAND and AUTN on the UE authentication request, thereby verifying the sequence number associated with that IMSI and calculating the RES. The validity of SQN is checked by calculating the Message Authentication Code (MAC) and comparing it with the MAC routed to AUTN. If so, the UE calculates and returns the corresponding RES response to the Serving Network (SN) in an authentication response message, once the MME receives and verifies the validity of the RES, it selects the corresponding K_{ASME} intermediate key as a session key to protect its communication with the UE. At the same time, the UE calculates its K_{ASME} accordingly. Finally, both the UE and MME have a symmetric session key from which other encryption and integrity protection keys will be derived.

3.1.2. EPS key hierarchy

After authentication, all the cryptographic keys needed for the various security mechanisms are derived from the intermediate key K_{ASME} [12]. The key derivations procedure is illustrated in Fig. 3.

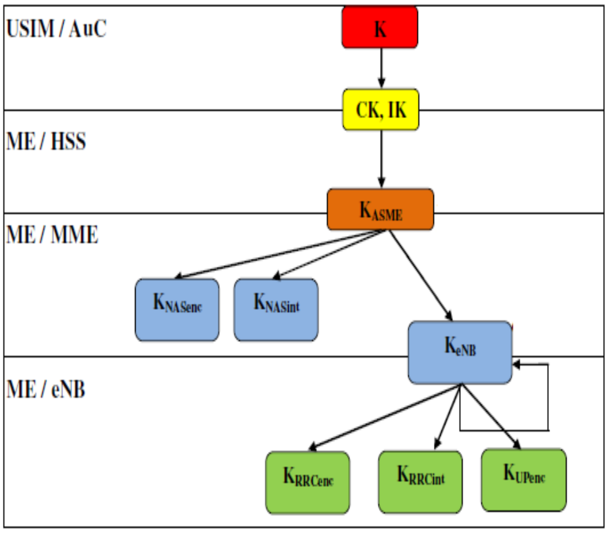


Figure.3 LTE key hierarchy

In the following, the purpose and functionality of each of the principal and specific derived keys related to network access security are explained.

- **K** is the subscriber-specific primary key, stored in the Universal Subscriber Identity Module (USIM) and the Authentication Center (AuC), and is not derived from any other key.
- **CK** and **IK** are 128-bit keys derived from K using additional input parameters.
- $\mathbf{K_{ASME}}$ is derived from CK and IK using two additional entries to become a master local key in MS.
- $\mathbf{K_{eNB}}$ is derived from K_{ASME} and the additional COUNT entry that is a counter parameter. This parameter is necessary to ensure that each new K_{eNB} derived from K_{ASME} differs from those previously derived. The purpose of this key is to be a local master key in an eNB.
- $\mathbf{K_{RRCenc}}$ is a key used to encrypt Radio Resource Control (RRC) signaling traffic. It is derived from K_{eNB} and two additional parameters, the first (algorithm type separator) indicates that this key is used for RRC encryption, and the second is the identifier of the encryption algorithm.
- $\mathbf{K_{RRCint}}$ is used to protect the integrity of RRC signaling traffic. It is derived from K_{eNB} and two parameters, the first indicates that this key is used for the integrity of RRC, and the second is the identifier of the integrity algorithm.
- Finally, $\mathbf{K_{UPenc}}$ is used to encrypt the user plan traffic. This key is derived from K_{eNB} and two parameters, the first indicates that this key is used for user plane encryption, and the second is the identifier of the encryption algorithm [13].

3.2 Authentication in IMS domain

After registration in the network domain, the user must register in the IMS domain. Mutual authentication in this step is required to avoid impersonation attacks. Thus, in this step the user and the IMS are authenticated to each other using the IMS-AKA procedure.

3.2.1. IMS-AKA protocol

Through the PCSCF and ICSCF, the terminal sends a request to the SCSCF; the SCSCF requests the AVs from the HSS, which was generated by the user's IMPI number; and then the SCSCF sends the AVs to the ICSCF, PCSCF and the terminal. The terminal and the network entities authenticate each other by using the received AV. After a successful service layer authentication, the terminal can access the multimedia services in IMS layer [14].

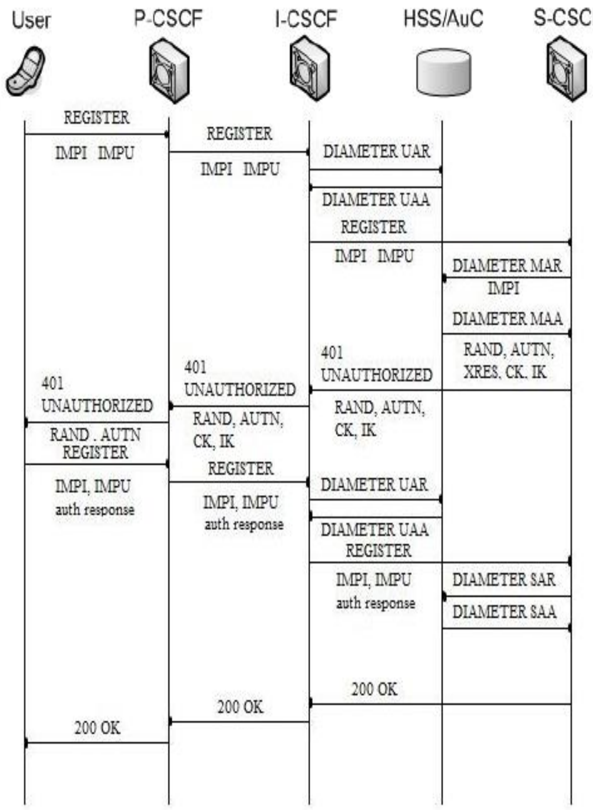


Figure.4 IMS-AKA procedure

The general IMS-AKA algorithm consists of three phases as elucidated by Fig. 4:

- Unauthorized Registration attempt: represented by the 401 message. This phase starts off when HSS receives a REGISTER request that contains user's identities. It generates a user authentication vector (AV) and sends it back.
- IPsec association: It is established between UE and the entry point of IMS network to ensure confidentiality and integrity of exchanged messages.
- Authorization: if UE generates an AV that matches with one calculated by HSS, so the authentication is considered successful and the user is granted access to its subscribed services.

3.2.2. IMS key hierarchy

As shown in Fig. 5, IMS uses the two level key hierarchy to protect traffic, which is a subset of the LTE five level key hierarchy. In IMS, the HSS generates CK and IK by using the pre-shared key K and distributes them to SCSCF and PCSCF. The traffic between the terminal and the PCSCF is confidentiality and integrity protected by CK and IK.

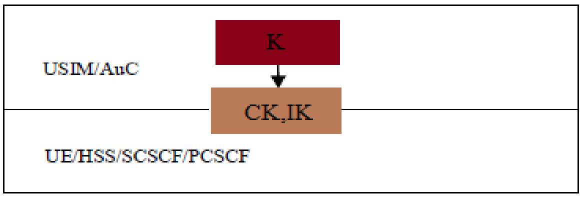


Figure.5 IMS key hierarchy

After receiving a request, the PCSCF/MME sends its to the core network (ICSCF/SCSCF/HSS) to do authentication, which means, a malicious attack could flood the ICSCF/SCSCF/HSS by sending correct packets with invalid IMSI/IMPI numbers.

4. Proposed AKA authentication

Since the 4G LTE and IMS network could provide voice, video and data services in one IP-based network, the IMPI number could be used in both of the network layer and service layer to do registration, authorization, administration and accounting. This paper proposes an improved authentication protocol for IoT system which shows some authentication issues of the existing protocol and supports IoT devices and provides a secure binding of the network layer and service layer authentication by using the IMPI number which avoids the double execution of the AKA authentication protocol. The solution follows absolutely the framework of the EPS-AKA and IMS-AKA protocol and can overcome the security problems found at the standard protocol in order to resist to different attacks such as the replay attack, Man In The Middle (MITM) attack and DoS attacks.

4.1 Proposed EPS authentication

The 3GPP defined EPS-AKA authentication protocol utilizes the IMSI number as the identity to do authentication. The proposed EPS authentication protocol presented in this paper supports mutual authentication by using the IMPI number within the HSS to generate AV and protect messages between the device and the server MME by using the ECDH [15].

The UE calculates the MAC_{UE} by $MAC_{UE}=f1_{Ks}(ID_{HSS} \mid\mid \text{SN id})$, where Ks is the shared secret key between the UE and HSS and then sends them to the MME [16].

A secure communication channel between the MME and the HSS has already been established (based on Diameter protocol [17]) and can provide security services to the transmitted data.

The MME requests to the HSS the authentication vectors AV. This request must include the IMPI, the service network identity 'SN id' of MME, the identity of HSS 'ID_{HSS}' to which the user belongs and to which the MME must route the request and MAC_{UE}. At the reception of the request from the MME, the HSS calculates the vectors and sends them to the MME in a response that contains n authentication vectors AV classified according to the sequence number, AV (1...n). If the user is successfully authenticated, the MME selects the key K_{ASME} contained in AV (i) to use it in the following steps. Otherwise, if the MME finds that XRES is different from RES, so it decides whether to initiate a new procedure or abandon the authentication procedure and send an authentication rejection message to the UE.

On Fig. 6, it is shown the authentication steps of our first proposition:

M1: the MME transmits an attach request to the UE

M2: the UE respond with an attach response include an IMPI number.

M3: If there isn’t a valid AV in the MME, the MME server finds out corresponding HSS according ID_{HSS} and forwards its parameters and its own ID_{MME} to the HSS by authentication data request message in order to generate the AV by using the Diameter protocol. It is proposed that the channel is secured with IP Security (IPsec). Using the signature parameter S_{MME}, the HSS can guarantee a higher level of security and confidence to MME. This signature may be considered where UE is roaming and not directly attached to the network.

M4: HSS verify the identity of the device by IMPI and the presence of MME with examination of SNid and calculates the AV parameters: RAND, $AUTH_{HSS}$, XRES and K_{ASME}.

$$AUTH_{HSS} = (SQN||AMF||MAC_{HSS}||ID_{HSS}) \quad (4)$$

$$MAC_{HSS} = f2_{Ks}(SQN||RAND||ID_{HSS}) \quad (5)$$

$$XRES = f3_{KASME}(RAND) \quad (6)$$

$$K_{ASME} = f4_{Ks}(RAND) \quad (7)$$

M5: The MME server receives and stores the parameters and calculates MAC_{MME}, and generates $AUTH_{MME}$. In addition, MME generates a random value a and computes aP, and sends $AUTH_{MME}$ and aP to device:

$$AUTH_{MME} = (ID_{MME}||RAND||MAC_{MME}||MAC_{HSS}) \quad (8)$$

$$MAC_{MME} = f2_{Ks}(ID_{MME}||RAND) \quad (9)$$

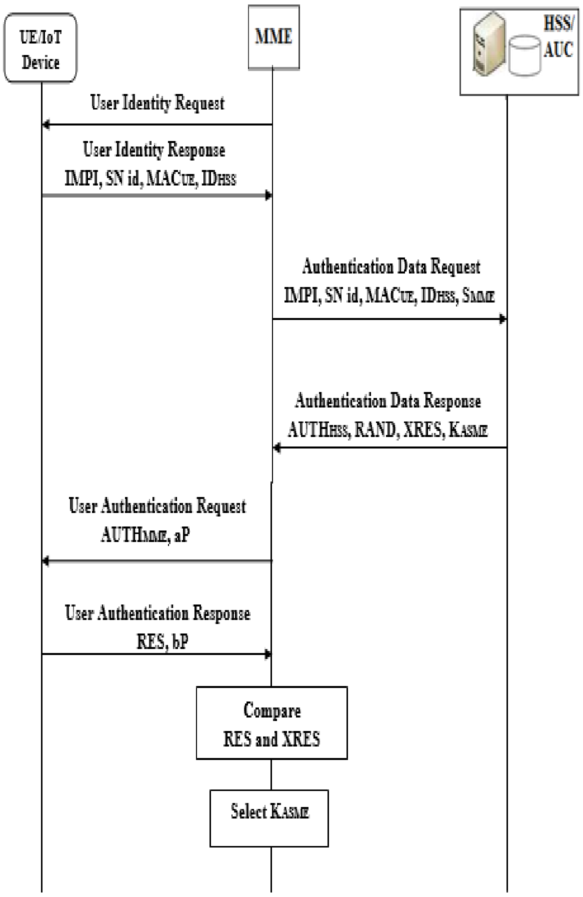

UE/IoT Device
MME
HSS/ AUC
User Identity Request
User Identity Response
IMPI, SN id, MACUE, IDHSS
Authentication Data Request
IMPI, SN id, MACUE, IDHSS, SMME
Authentication Data Response
AUTHHSS, RAND, XRES, KASME
User Authentication Request
AUTHMME, aP
User Authentication Response
RES, bP
Compare RES and XRES
Select KASME

Figure.6 Proposed LTE authentication procedure

The MME transmits the authentication request message to the UE.

M6: The UE computes K_{ASME} then derived the RES response value and sends it to the MME, which authenticates the UE by the validity of the equivalence of RES and XRES and select K_{ASME} key.

Firstly the UE verifies the received MAC_{HSS} and MAC_{MME}:

$$MAC'_{HSS}=f2_{Ks}(ID_{HSS}||RAND) \tag{10}$$

$$MAC'_{MME}=f2_{Ks}(ID_{MME}||RAND) \tag{11}$$

If verification passes, the device computes bP by generating a random value b, also computes the K_{ASME} and RES and sends them to MME.

$$K_{ASME}=f4_{Ks}(abP) \tag{12}$$

After a successful proposed EPS authentication, the UE and the MME have completed the authentication steps and have the same K_{ASME}, which is used to derive more keys for different security protection purposes.

4.2 Proposed IMS authentication

The designed protocol aims to overcome the weaknesses of IMS-AKA protocol. It provides both an identity protection module to preserve privacy aspect and an AKA mechanism to provide mutual authentication, authorization, confidentiality and integrity with a better robustness and performance.

On Fig. 7, it is shown the authentication steps of our second proposition:

M1: The Protection of the user's identities transmitted between UE and PCSCF based on key-less cryptography

M2: The UE sends a SIP REGISTER request to the PCSCF to negotiate the parameters of building SAs with the IMPI number, Global Unique Temporary Identity (GUTI) number and security-setup line. The security-setup line includes the parameters to build the IPSec SAs.

In the first time, when the user connect to the network, he generates a random number vector RAND. This vector contains n ordered random value RANDi. At each authentication request, the user selects the next RAND value to challenge the HSS server. In step i of the proposed protocol the terminal takes a random number RANDi from the RAND vector.

M3: The PCSCF derives the MME address from GUTI and sends a Context Request to the MME to fetch the AV with IMPI and GUTI.

M4: The MME obtains the user's AV by using GUTI number and sends the AV back to the PCSCF

M5: Upon receipt of the AV from the MME, the PCSCF chooses the parameters to build the SA, uses the parameters to construct the security-setup line; and sends it back to the UE.

M6: The UE derives CK and IK and builds the IPSec SAs; then it sends the SIP REGISTER request to the PCSCF through the IPSec SA.

The terminal then calculates the value RESi and derives the two keys CK and IK as follows:

$$RESi = f2(RANDi),\ CKi= f3k(RANDi),\\ IKi= f4k(RANDi) \tag{13}$$

With k is the secret key pre-shared between the terminal and the HSS; fi are the cryptographic algorithms shared between the UE and the HSS: f2 is a function of generation of the message authentication code; f3 and f4 are functions of generation of key.

M7: The PCSCF checks the received SIP packet by decryption and calculation the integrity code. If this is a valid packet, the PCSCF forwards it to the ICSCF.

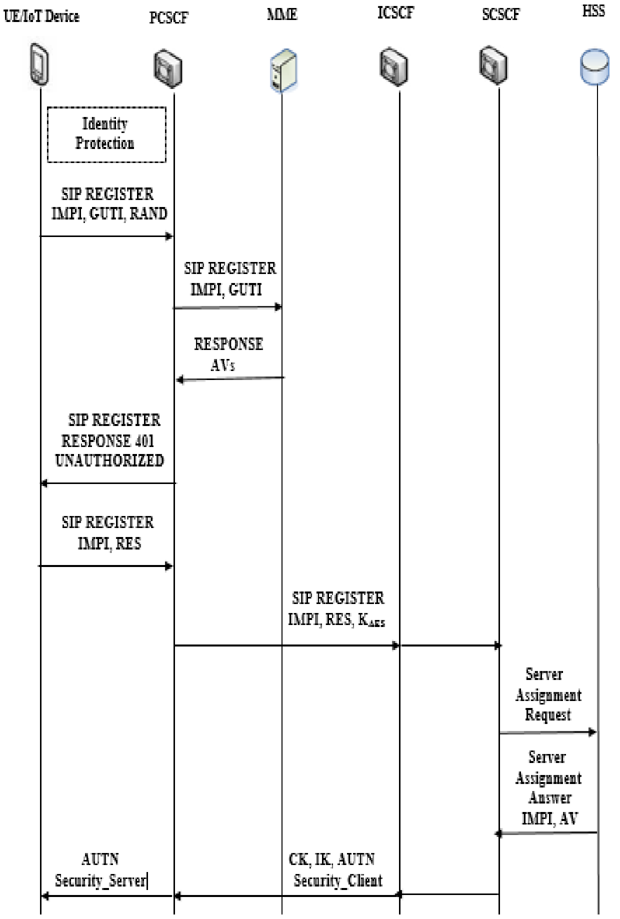

UE/IoT Device
PCSCF
MME
ICSCF
SCSCF
HSS
Identity Protection
SIP REGISTER IMPI, GUTI, RAND
SIP REGISTER IMPI, GUTI
RESPONSE AVs
SIP REGISTER RESPONSE 401 UNAUTHORIZED
SIP REGISTER IMPI, RES
SIP REGISTER IMPI, RES, K_AES
Server Assignment Request
Server Assignment Answer IMPI, AV
AUTN Security_Server
CK, IK, AUTN Security_Client

Figure.7 Proposed IMS authentication procedure

PCSCF generates an Advanced Encryption Standard (AES) key, which will be used to encrypt communications between the PCSCF and the SCSCF for that user during the current session (K_{AES}), and then encrypt the K_{AES} key generated with the public key of the SCSCF using ECC [18]. The PCSCF then adds the encrypted AES key as well and its signature and transmits the message to the SCSCF via ICSCF.

M8: The ICSCF fetches the user and the SCSCF information from the HSS, locates the SCSCF address, and sends the packet to the SCSCF.

SCSCF receives the request and verifies the signature of the PCSCF. If the signature is authentic, it decrypts the K_{AES} key using its private key. Suppose that SCSCF does not have the AVs for this user, and then SCSCF adds its signature to the Multimedia Authentication Request (MAR) message and sends it to the HSS.

M9: The SCSCF sends a Server Assignment Request to HSS with IMPI by using the Diameter protocol.

M10: The HSS verifies the signature of the SCSCF. If it is valid, it uses IMPI to find the secret key pre-shared with this user (K) as well as the RAND vector, if the value RANDi is different from that expected, then the HSS stops the authentication procedure and informs the SCSCF that will send to the a SIP 401 message UNAUTHORIZED to inform him that the authentication is unsuccessful. Otherwise, in the opposite case, the value is that expected, the HSS calculates the AVi. The HSS then generates an AES key that will be used to secure communication between the SCSCF and the HSS until the next MAR/MAA exchange. The HSS then adds the symmetric key and encrypts the Multimedia Authentication Answer (MAA) message using the SCSCF certificate. Finally, he signs the message before sending it to SCSCF. This approach is based on a preliminary system configuration, where HSS generates several security parameters using the ECC cryptography.

M11 and M12: The SCSCF sends the SIP response to the ICSCF and the ICSCF forwards it to the PCSCF.

After receiving the MAA message, SCSCF verifies the validity of the HSS signature. If it is genuine, it decrypts the message and extracts AVi. The SCSCF then checks, using IKi, the hash value received to check the integrity of the request, if the result is positive the SCSCF decrypts the RESi response (using CKi received in the authentication vector AVi). RESi is compared to XRESi also contained in AVi. If they are equal, it means that this user is legitimate.

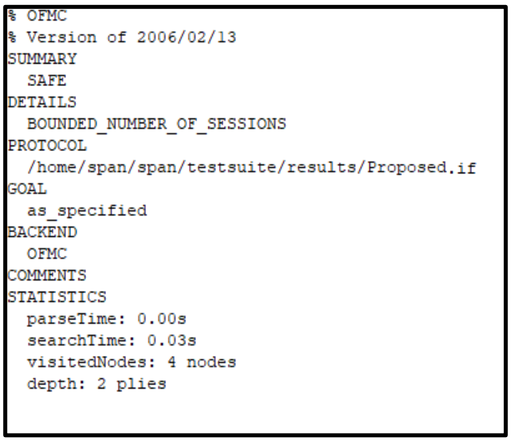
After the SAR/SAA exchanges with the HSS, the SCSCF prepares a SIP message OK. This message includes AUTNi, CKi and Iki, encrypted with the AESPS key. Then he signs it and sends it to the PCSCF.

PCSCF verifies the signature of the SCSCF. If the result is positive, it decrypts the message, stores CKi, IKi and the "Security-Client" field, and then transmits the SIP OK message with AUTNi to the user. This message is encrypted and authenticated by CKi and IKi

M13: By using IPSec, the PCSCF sends the packet to the UE and the UE authenticates the PCSCF by checking the ICV (Integrity Checking Value) of the packet. If this is a valid ICV code, the network entity passes the authentication and continues interacting with the terminal.

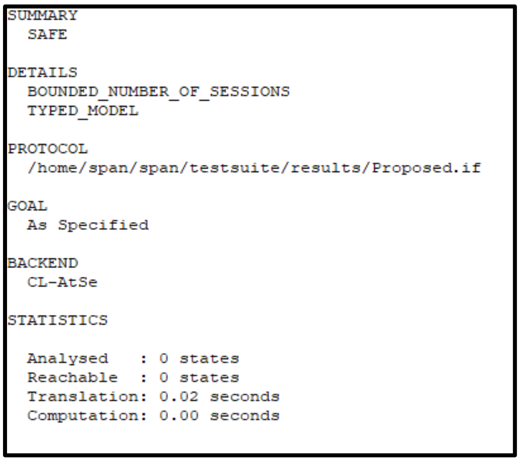
The terminal calculates AUTNi and compares it to that obtained from the SCSCF.

The SCSCF is then authenticated if the result is positive. Note that we also use both the Security_Client and Security_Server fields to establish an IPsec security association between the terminal and the PCSCF.



```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/Proposed.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.03s
  visitedNodes: 4 nodes
  depth: 2 plies
```

Figure.8 The output of OFMC backend



```
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL

PROTOCOL
  /home/span/span/testsuite/results/Proposed.if

GOAL
  As Specified

BACKEND
  CL-AtSe

STATISTICS

  Analysed   : 0 states
  Reachable  : 0 states
  Translation: 0.02 seconds
  Computation: 0.00 seconds
```

Figure.9 The output of CL-AtSe backend

5. Security analysis

This solution was checked by the security protocol verification tool, Automated Validation of Internet Security Protocols and Applications (AVISPA) [19], which indicated that it is a very secure level. The main advantage of this tool is the ability to use different verification techniques on the same protocol specification. The protocol designer interacts with the tool by specifying a security problem in the High Level Protocol Specification Language (HLPSL). The HLPSL is an expressive, modular, role-based, formal language that is used to specify control-flow patterns, data-structures, alternative intruder models and complex security properties, as well as different cryptographic primitives and their algebraic properties.

The primary goal of our proposed protocol is to provide mutual AKA services between the IoT devices, the MME and the PCSCF. We need to verify that the proposed protocol can provide a successful mutual authentication between the entities by using back-end servers. The output of the model checking results are shown in Figs. 8 and 9.

After running this specification with OFMC and CLAtSe backends, we can conclude that the proposed scheme can accomplish the goal of mutual authentication and can resist those malicious attacks, such as replay attacks, MITM attacks and secrecy attacks under the test of AVISPA.

6. Energy cost analysis

In this section, the energy cost and the storage cost of the user terminal’ s authentication related security activities were calculated for the EPS-AKA [11], IMS-AKA [14] and our proposed AKA.

6.1 Energy consumption

For energy consumption calculation only, energy used in generating AV is considered since it is the most important phase.

For the 3GPP defined and proposed AKA authentication protocols, the terminal’s security activities include the execution of the EPS-AKA and the IMS-AKA authentication protocol. Therefore, $E=E_{EPS\text{-}AKA} + E_{IMS\text{-}AKA}$ where E denotes the energy consumption.

In the 3GPP defined authentication protocol, the terminal’s energy cost to execute the EPS-AKA authentication protocol includes the generation of AUTN number which is made up of generating Anonymity Key (AK) and MAC, generating the RES number, and generating CK, IK and deriving K_{ASME} as shown in (14).

$$E_{3GPP\text{-}EPS\text{-}AKA} = E_{AK} + E_{MAC} + E_{RES} + E_{CK} + E_{IK} + E_{KASME} \quad (14)$$

The energy cost to execute the IMS-AKA authentication protocol is shown in (15).

$$E_{3GPP\text{-}IMS\text{-}AKA} = E_{AK} + E_{MAC} + E_{RES} + E_{CK} + E_{IK} \quad (15)$$

We used the AES as the kernel encryption algorithm. In addition, Keyed Hash MAC-Secure Hash Algorithm (HMAC-SHA-256) is used as the key derivation function. The energy consumption of AES and HMAC was analyzed in [20]. The results showed the energy consumption of AES algorithm is made first in the key setup phase which is 7.87 μJ and the second is in the encryption/decryption phase. In the encryption/decryption phase, the Energy Consumption Per Byte (EPB) is 1.21 μJ. For the HMAC-SHA-256, the EPB is 1.16 μJ. Therefore, the energy can be calculated as shown in (16) and (17).

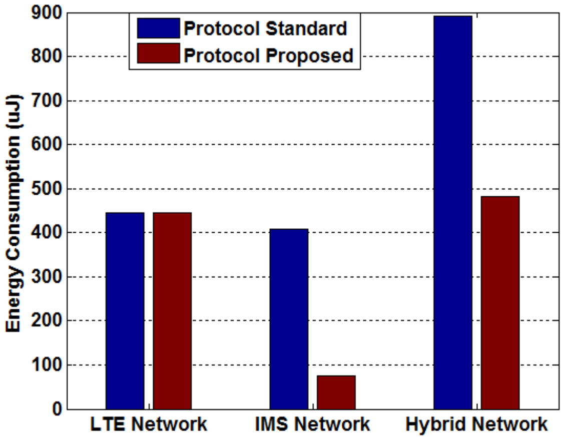


Figure.10 Energy consumption comparison

Table 1. Storage cost

Protocols	Storage Cost (bits)
IMS-AKA	128+1536
EPS-AKA	276+1088
Proposed AKA	276+1088+368 (LTE Domain)
	128+256+192 (IMS Domain)

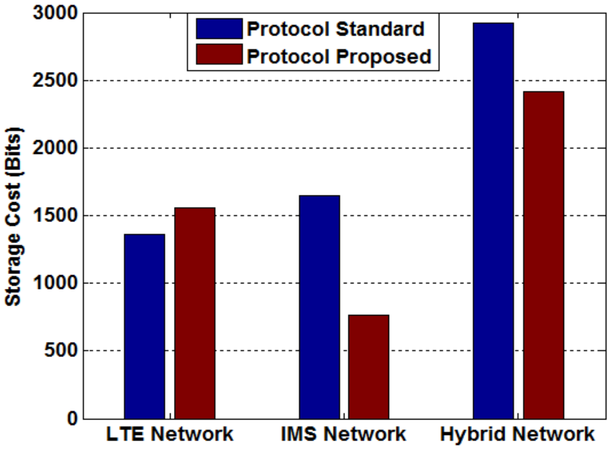


Figure.11 Storage cost comparison

$$E_{AES}(n) = 7.87\ \mu J + 1.21\ \mu J \times n \qquad (16)$$

$$E_{HMAC}(n) = 1.16\ \mu J \times n \qquad (17)$$

Where n is the length of the input string in bytes. Although the MAC, RES, CK, IK, and AK have different lengths, they were all generated by encrypting 16 byte data blocks three times. Therefore, E_{AK}= E_{MAC}= E_{IK} = E_{CK} = E_{RES} = 81.69 μJ. By referring to (14) and (15): $E_{3GPP\text{-}EPS\text{-}AKA}$ = 445.57 μJ and $E_{3GPP\text{-}IMS\_AKA}$ = 408.45 μJ.

For K_{ASME}, CKi and IKi, they were derived by using 32 byte data blocks so the energy consumption is 37.12 μJ by using (17). For the 3GPP defined authentication protocol, referring to (14) and (15), $E_{3GPP\text{-}EPS\text{-}AKA}$ = 445.57 μJ, and $E_{3GPP\text{-}IMS\text{-}AKA}$ = 408.45 μJ.

For the proposed AKA authentication protocol, the LTE network layer energy consumption is 445.8 μJ ($E_{P\text{-}EPS\text{-}AKA}$ = $E_{3GPP\text{-}EPS\text{-}AKA}$ + E_{ECDH} = 445.8 μJ). The energy cost of the IMS service layer includes key derivation of CKi and IKi by using HMAC-SHA-256 and key derivation using ECC cryptography ($E_{P\text{-}IMS\text{-}AKA}$ = 74.51 μJ).

Fig. 10 shows a comparison of the consumption energy for standard protocols EPS-AKA, IMS-AKA and our proposed.

We can see that our solution which combine two improved protocols in LTE and IMS networks have the least energy consumption compared to the 3GPP standard protocols, due to the use of the ECC and different methods of security more efficient than the traditional operations used in existing protocols.

6.2 Storage cost

As presented in Table 1 and Fig. 11, the storage cost of the authentication between the device and the server HSS in proposed AKA which contain the secret key AV parameters, ECC and ECDH parameters is more efficient than EPS-AKA and IMS-AKA protocols that comprises the secret key, AV parameters and a sequence number.

7. Conclusion

This paper reviewed the EPS-AKA and IMS-AKA protocols, their weaknesses in term of security (disclosure of identities) and performances aspects. To address them, we proposed a secure and optimized protocol for the 4th generation LTE and IMS in IoT system, which reduces the authentication procedures significantly by a secure binding of the network and service layer authentication using the IMPI number, provide user's identities protection, and used the strength of ECC for AKA. Our proposed protocol authenticates the user on both the network layer and the service layer without double execution the AKA protocol, simplifies authentication steps, reduces storage cost and provides advanced security with less energy. Simulation results showed that our solution compared to IMS-AKA and EPS-AKA offers better performances in terms of energy consumption and storage cost. Future research work will focus to perform a deeper analysis of the proposed AKA running more tests, and experiments within an IoT environment.

References

[1] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey", *Computer Networks*, pp.2787–2805, 2010.

[2] D. C. Yacchirema and C. Palau, "Smart IoT Gateway For Heterogeneous Devices Interoperability", *IEEE Latin America Transactions*, Vol.14, No.8, 2016.

[3] M. Ouaissa and A. Rhattoy, "A Secure Model for Machine to Machine Device Domain Based Group in a Smart City Architecture", *International Journal of Intelligent Engineering and Systems*, Vol.12, No.1, pp. 151-164, 2019.

[4] S. Yang, X. Wen, W. Zheng, and Z. Lu, "Convergence architecture of Internet of Things and 3GPP LTE-A network based on IMS", In: *Proc. of Global Mobile Congress*, pp. 1-7, 2011.

[5] M. Ouaissa and A. Rhattoy, "New Method Based on Priority of Heterogeneous Traffic for Scheduling Techniques in M2M Communications over LTE Networks", *International Journal of Intelligent Engineering and Systems*, Vol.11, No.6, pp. 209-219, 2018.

[6] M. Ouaissa, M. Benmoussa, A. Rhattoy, M. Lahmer, and I. Chana, "Impact of M2M Traffic in Random Access Channel over LTE Networks", *Advances in Electronics, Communication and Computing*, pp. 11-19, ETAEERE, 2016.

[7] 3GPP TS 23.228 V10.0.0, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS), Stage 2 (Release 10), 2010.

[8] V. S. Miller, "*Use of elliptic curves in cryptography*", In: *Proc. of the Advances in Cryptology*, pp. 417–426, 1986.

[9] A. Menezes, *Evaluation of security level of cryptography: the elliptic curve discrete logarithm problem (ECDLP)*, University of Waterloo, 2001.

[10] M. Ouaissa, A. Rhattoy, and M. Lahmer, "New Method to Control Congestion for Machine to Machine Applications in Long Term Evolution System", *International Journal on Communications Antenna and Propagation*, Vol.8, No.4, 2018.

[11] M. Ouaissa, A. Rhattoy, and M. Lahmer, "Analysis of Authentication and Key Agreement (AKA) Protocols in Long-Term Evolution (LTE) Access Network", *Advances in Electronics, Communication and Computing*, pp. 1-9, ETAEERE, 2016.

[12] 3rd Generation Partnership Project, 3GPP TS 35.206 V11.0.0, Technical Specification; 3G Security; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 2: Algorithm Specification, (Release 11), 2012.

[13] M. Ouaissa and A. Rhattoy, "A New Scheme of Group-based AKA for Machine Type Communication over LTE Networks", *International Journal of Electrical and Computer Engineering*, Vol.8, No.2, pp. 1169-1181, 2018.

[14] A. Dutta, A. Ghosh, S. Das, F. J. Lin, K. Manousakis, D. Chee, and A. Idoue, "Security optimization for IMS/MMD architecture", *U.S. Patent No. 9,025,771*, 2015.

[15] J. Zhang and F. Deng, "The authentication and key agreement protocol based on ECC for wireless communications", *International Conference on Management and Service Science*, pp. 1-4, 2009.

[16] M. Ouaissa, A. Rhattoy, and I. Chana, "New Security Level of Authentication and Key Agreement Protocol for the IoT on LTE Mobile Networks", In: *Proc. of the 6th International Conference on Wireless Networks and Mobile Communications*, pp. 1-6, 2018.

[17] *DIAMETER et ses Applications Principes, Architecture et Services*, EFFORT, http://www.efort.com.

[18] L. Wu, Y. Zhang, and F. Wang, "A new provably secure authentication and key agreement protocol for SIP using ECC", *Computer Standards & Interfaces*, Vol.31, No.2, 286-291, 2009.

[19] T. A. Team, "AVISPA v1. 1 User Manual 2006," http://avispaproject.org/.

[20] N. R. Potlapally, S. Ravi, A. Raghunathan, and N. K. Jha, "A study of the energy consumption characteristics of cryptographic algorithms and security protocols", *IEEE Transactions on mobile computing*, Vol.5, No.2, pp. 128-143.