

Extension of Authentication and Key Agreement Protocol (AKA) for Universal Mobile Telecommunication System (UMTS)

Ja'afar AL-Saraireh & Sufian Yousef
Anglia Ruskin University
Chelmsford –UK

Abstract

The current 3GPP authentication and key agreement protocol (AKA) has some shortcomings such as the bandwidth consumption between visitor serving network and home network, the delay time that incurred from generated authentication vector in home network, waste of storage space in VLR to store authentication vectors and the management of sequence number which needed for synchronization between mobile station and its home network.. This paper proposes a new protocol as an extension for the 3GPP AKA to eliminate the 3GPP AKA shortcomings by using temporary security key.

Keywords: UMTS, Authentication Vector, AKA, Temporary Key.

1. Introduction

The rapid growth in wireless networking has brought a number of security concerns to the service providers and end users. Security, Authentication, Encryption and Access Control are vital features that must be presented in any communication network. One of the principal reasons that security is such a significant issue in cellular system because they rely on radio waves to carry communications. These radio waves are not restricted by walls or physical boundaries, but rather they are designed to cover, as large as possible wireless cell. However, because the radio waves are so exposed and available, they can be intercepted or jammed by anyone who is within range [14].

Security has always been an issue for mobile communication networks. First generation analogue phones were susceptible to user traffic eavesdropping and cloning whereby fraudsters were able to change the identity of mobiles so that calls could be charged to another customer's account. Against this background, second generation

system such as General system for Mobile communications (GSM) were developed. GSM was the first public telephone system to introduce integrated cryptographic mechanisms for authentication and confidentiality. These mechanisms have been extremely effective in eliminating technical fraud due to cloning and have provided good protection against user traffic eavesdropping. GSM implements security features, which ensure physical security, data security, user authentication, and user anonymity. However, GSM suffers from security problems such as weak authentication and encryption algorithms, short secret key length (only 32 bits) with no network authentication. This has led to false base station attack and lack of data integrity, allowing denial of service attacks, limited encryption scope and insecure key transmission.

Third generation (3G) mobile systems such as Universal Mobile Telecommunication System (UMTS) specified by Third Generation Partnership Project (3GPP) [8] was built on the success of GSM and other second generation system by introducing new and enhanced security features that are designed to stop threats [9, 12, 13, 15]. These include: Mutual Authentication which allows the mobile user and serving network to authenticate each other [1], Network to Network security that secure communication between serving networks which suggested the use of IP security to do so, wider security scope, secure International Mobile Subscriber identity (IMSI) usage, User to mobile station authentication where more flexibility in that security features can be extended and enhanced as required by new threats and service plus GSM compatibility. As mobile phones become the preferred means of user communications, 3G will offer users and providers of services a level of security which is better than that provided in fixed networks or GSM system.

2. Description of UMTS AKA (3GPP AKA) Protocol

An authentication mechanism is a process designed to allow all participants show their legality and verify the other participant's identities that involved in the networks [11].

In UMTS there are three components that participate in authentication.

1. Mobile station (**MS**) and UMTS Subscriber Identity Module (**USIM**),
2. Visitor Location Register (**VLR**) and Serving Network which **MS** visits,
3. Home Network (**HN**) included Home Location Register (**HLR**) and Authentication Center (**AuC**).

The UMTS is based on the security of 2nd generation mobile system. This mechanism using secret key **K**, and cryptographic algorithms - includes three message authentication codes f_1 , f_1^* and f_2 and four key generation functions f_3 , f_4 , f_5 and f_5^* - [2, 3, 4, 14] that are shared between **MS** and the **HN**, this is known as authentication and key agreement protocol (AKA), also the **HN** maintains a counter called sequence number (SQN_{HLR}), and user mobile station maintains a counter (SQN_{MS}), the initial value for these counters are set to zeros [1, 15].

There are three goals for the UMTS AKA [15]:

1. The mutual authentication between the user and the network;
2. The establishment of a cipher key and an integrity key upon successful authentication; and
3. The freshness assurance to the user of the established cipher and integrity keys.

There are two phases in AKA protocol [15]:

1. The distribution of authentication vectors from the *HN* to the *VLR/SN*.
2. The authentication and key agreement procedure between the *MS* and the *VLR/SN*.

Figure 1 illustrates Authentication and Key Agreement in UMTS. This protocol is executed as following:

1. *MS* sends (*IMSI*) authentication request to *VLR/SN*.
2. *VLR/SN* passes this authentication request to *HN*.
3. *HN* Generates authentication vectors $AV(1..n)$ and sends authentication data response $AV(1..n)$ to *VLR/SN*. Each authentication vector called a quintet This AV consists of five components: random number ($RAND$), expected response ($XRES$), cipher key (CK), integrity key (IK) and authentication token ($AUTN$). The authentication vectors are ordered by the sequence number. The authentication vector is generated according to the following:
 - a. *HN* generates SQN_{HLR} and $RAND$.
 - b. *HN* computes $XRES = f_2(K,RAND)$, $CK = f_3(K,RAND)$, $IK = f_4(K,RAND)$, $AK = f_5(K,RAND)$, Message Authentication Code $MAC = f_1(K,SQN//RAND//AMF)$, where AMF is Authentication Management Field and $AUTN = (SQN \oplus AK//AMF//MAC)$ where \oplus is exclusive OR operation.
 - c. *HN* increment SQN_{HLR} by 1.
4. *VLR/SN* stores authentication vectors, selects authentication vector $AV(i)$, and sends authentication request ($RAND(i)$, $AUTN(i)$) to *MS*. In the *VLR/SN* one authentication vector is needed for each authentication instance. This means that the signaling between *VLR/SN* and *HN* is not needed for every authentication events.
5. *MS* computes and retrieves the following:
 - a. $AK = F_5(Rand, K)$, $SQN = (SQN \oplus AK) \oplus AK$, computes expected message authentication code $XMAC = f_1(SQN, RAND, AMF)$ and then
 - b. Compares $XMAC$ with MAC which is included in $AUTN$. If $XMAC$ not equal to MAC then *MS* sends failure message to the *VLR/SGSN*, else if $XMAC$ is equal MAC then *MS* checks that received SQN is in the correct range i.e. $SQN > SQN_{MS}$. If SQN is not in correct range then *MS* sends failure message and generates resynchronization message to the *VLR/SGSN*, else if it is in the correct range then *MS* computes the Response $RES = f_2(K, RAND)$, and $CK = f_3(K, Rand)$,
 - c. After that it sends RES to *VLR/SN*.
6. *VLR/SN* compares the received RES with $XRES$. If they match, then authentication is successfully completed.

UMTS uses a sequence number approach with which a subscriber can verify the freshness of an authentication request and thus prevent an attacker's replay [10].

The transmission between the *HN* and *VLR/SN* is usually expensive. Each authentication vector that generated by *HN* is included *m* records, these records ordered by sequence number and send it to *VLR/SN*, when these vector is consumed then *VLR/SN* requested a new authentication vector form *HN* [5, 6]. The following is the length of AV parameters:

- a. The random challenge (*Rand*) has a length of 128 bits.
- b. The authentication response (*XRES*) has a length of 128 bits.
- c. The cipher key (*CK*) has a length of 128 bits.
- d. The integrity key (*IK*) has a length of 128 bits.
- e. The *AUTN* have the following parameters:
 - Sequence number (*SQN*) has the length of 48 bits.
 - Anonymity key (*AK*) has the length of 48 bits.
 - Authentication management field (*AMF*) has the length of 16 bits.
 - Message authentication code (*MAC*) has the length of 64 bits.

The total size of each record in *AV* is **688** bits, if there are *m* records in *AV* then the total size of AV is $(688 * m)$ bits. If there are *N* customers subscribe in *VLR/SN* the *VLR/SN* needs $688 * m * N$ bits to store the authentication information..

The current UMTS authentication protocol has the following shortcomings as shown form the above discussion:

- i. As a lot of data being sent between *VLR/SN* and *HLR*, this has impact on the performance of AKA protocol.
- ii. Bandwidth consumption between visitor serving network and home network, for each authentication data request that generated from *MS* and passes to *VLR/SN*. If there is no authentication vector available in *VLR/SN*, then *VLR/SN* sends request to *HN* to generate authentication vectors.
- iii. The process of generating authentication vectors (*AV*) is expensive and there is delay time that incurred from generated authentication vectors in home network. There are five records as a standard that suggested by 3GPP, included in each *AV*.
- iv. Storage space overhead for *VLR/SN* to store authentication vectors for each *MS* in the relevant *VLR/SN*.
- v. Synchronization problem between the MS and HN. The HN and MS are needed to maintain sequence numbers to provide synchronization between MS and HN.

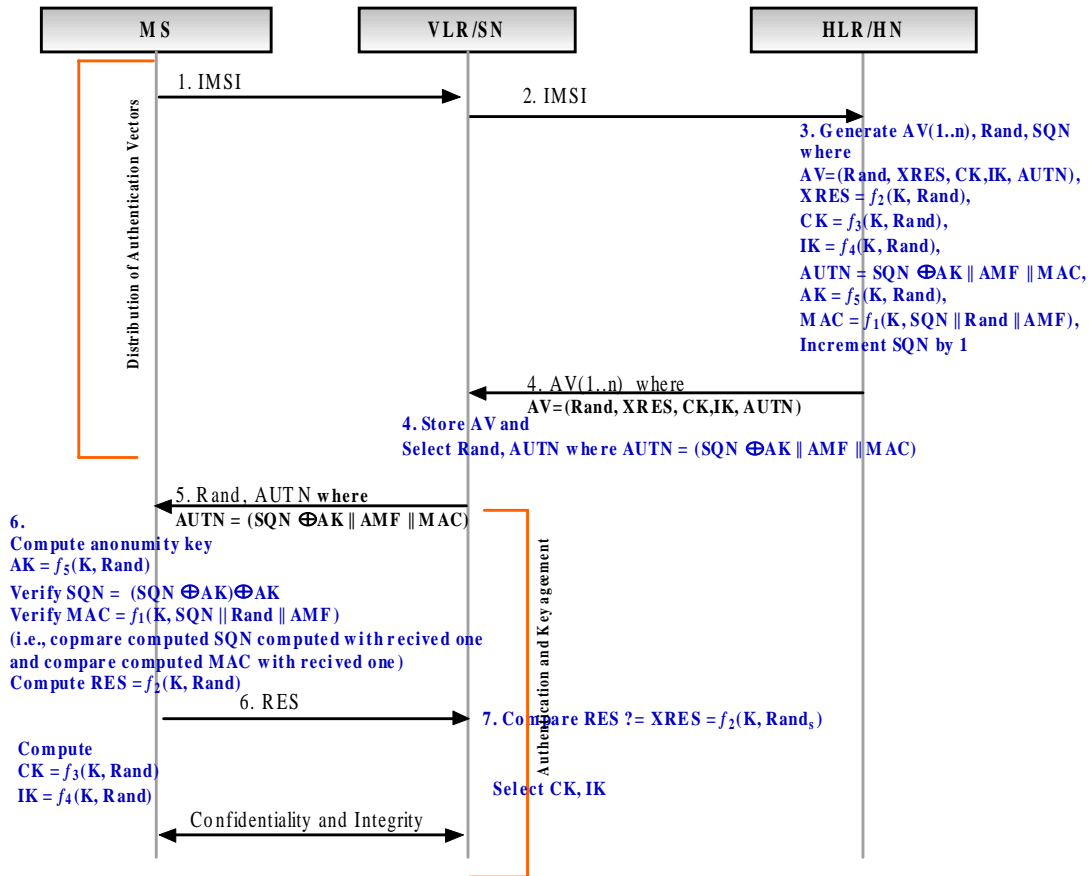


Figure 1: UMTS AKA Protocol

3. Extension of AKA Protocol for UMTS

In this protocol, there is secret key K , and cryptographic algorithms that include two message authentication codes f_1 , and f_2 and three key generation functions f_3 , f_4 , f_5 . The f_5 is a function that is used to produce 128 bit as temporary key K_{temp} . Functions f_1, f_5 are shared between MS and HN . Functions f_1, f_2, f_3, f_4 are shared between MS and VLR/SN . In this protocol no need for synchronization function f_1^* and f_5^* which are used in AKA protocol. The HN and MS maintain a counter called *Count*. This counter is incremented by 1 when the MS sends authentication request to VLR/SN , the initial value for these counters are set to zeros.

There are six goals for the extension of AKA protocol for UMTS:

1. Provides mutual authentication between the user and the home network.
2. Provides mutual authentication between the user and the serving network.
3. The establishment of a cipher key and an integrity key upon successful authentication; and
4. Reduces the signaling traffic between serving network and home network and reduces the size of authentication information which needed to be stored in serving network.

5. Element synchronization between *MS* and *HN*.
6. *HN* grants *SN* to authenticate *MS*, then *VLR/SN* authenticates *MS* without any assistance for the subscriber's *HN*.

There are two phases in this proposed protocol:

1. The distribution of authentication information and temporary key from the *HN* to the *VLR/SN*.
2. The authentication and key agreement procedure between the *MS* and the *VLR/SN*.

Figure 2 illustrates the extension authentication and key agreement protocol for UMTS. This protocol is executed as follows:

The First Phase:

1. *MS* does the following:
 - a. Generates random number $Rand_1$.
 - b. Computes mobile station message authentication code $MAC_{MS} = f_1(K, Rand_1)$.
 - c. Sends authentication request message to *VLR/SN*. This message includes *IMSI*, $Rand_1$ and MAC_{MS} .
2. *VLR/SN* passes this authentication request message to *HN*.
3. *HN* does the following:
 - a. Verifies *MS* by computing $f_1(K, Rand_1)$ and compares the result with the received MAC_{MS} , if the comparison fails then reject authentication, otherwise *HN* continues the authentication process.
 - b. Computes temporary key K_{Temp} , as $K_{Temp} = f_{99}(K, Rand_1)$.
 - c. Computes home network message authentication code $MAC_{HN} = f_1(K, Rand_1 || AMF)$.
 - d. Computes authentication token for home network $AUTN_{HN} = MAC_{HN} || Rand_1 || AMF$.
 - e. *HN* sends $AUTN_{HN}$, K_{Temp} to the *VLR/SN* and *VLR/SN* stores authentication information $AUTN_{HN}$, K_{Temp} which is received from *HN*.

The Second Phase:

4. *VLR/SN* does the following:
 - a. Generates random number $Rand_2$.
 - b. Computes serving network message authentication token $MAC_{VLR/SN} = f_1(K_{Temp}, MAC_{HN} || Rand_2 || Count)$.
 - c. Computes authentication token for serving network $AUTN_{VLR/SN} = MAC_{VLR/SN} || Rand_2 || AMF$.
 - d. Increments the **Count** by 1. The initial value for **Count** is zero.
 - e. *VLR/SN* sends $AUTN_{VLR/SN}$, $Rand_2$ to the *MS*.

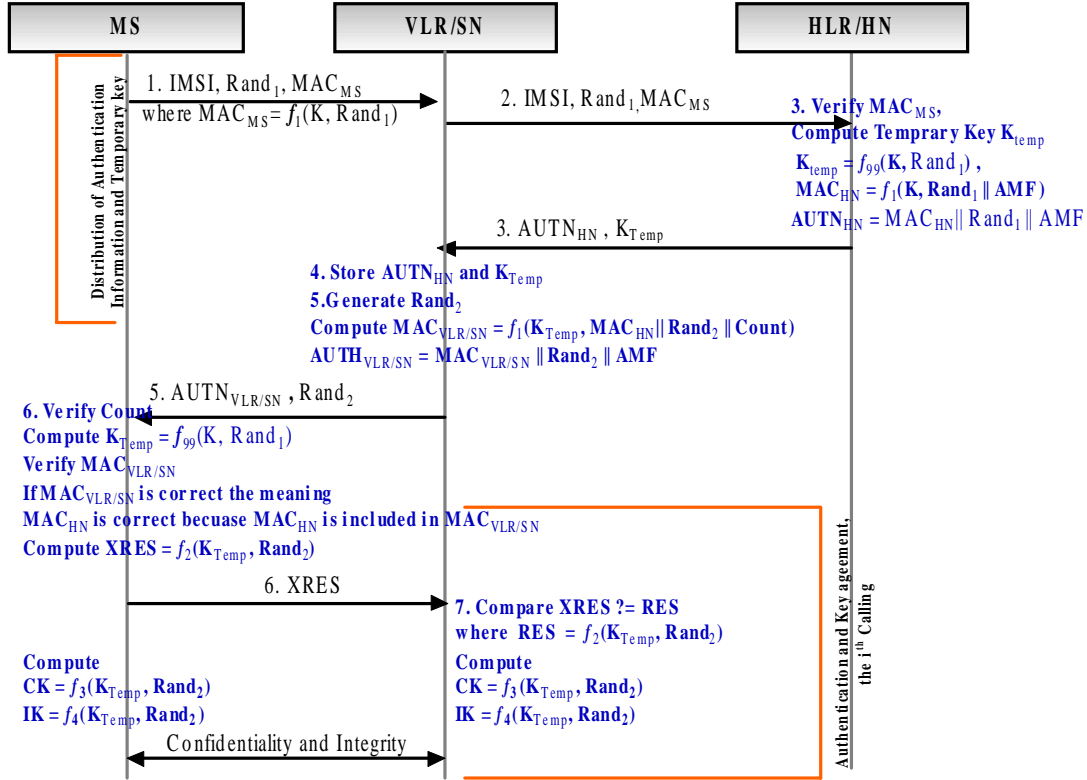


Figure 2: Extension for AKA Protocol

5. **MS** does the following:
 - a. Verifies the **Count**, if **Count** is equals or larger than that owned by **MS**, set the **Count** as that owned by **MS**. Otherwise the **MS** rejects the authentication procedure.
 - b. Computes temporary key K_{Temp} , as $K_{Temp} = f_{99}(K, Rand_1)$.
 - c. Verifies $MAC_{VLR/SN}$, by computing $MAC_{HN} = f_1(K, Rand_1 || AMF)$, and then computes $f_1(K_{Temp}, MAC_{HN} || Rand_2 || Count)$ and compares the result of computing with the received $MAC_{VLR/SN}$ if the two values, computed value and received value are matching, then this means that **MS** authenticates **HN** because the value of $MAC_{VLR/SN}$ is correct. Then this leads to infer that MAC_{HN} is correct because MAC_{HN} is included in $MAC_{VLR/SN}$.
 - d. Computes expected response **XRES** value to authenticate **VLR/SN**, $XRES = f_2(K_{Temp}, Rand_2)$.
 - e. Sends **XRES** to the **VLR/SN**.
6. When **VLR/SN** has received **XRES**, the **VLR/SN** computes and compares **XRES** with $f_2(K_{Temp}, Rand_2)$. If the two values are matching, then the authentication successful, otherwise the authentication is failed.

If the authentication is successful, then **MS** and **VLR/SN** compute cipher key and integrity key to provide secure communication between **MS** and **VLR/SN**. The cipher

key and integrity key is computed as follows: $CK = f_3(K_{Temp}, Rand_2)$ and $IK = f_4(K_{Temp}, Rand_2)$.

For every execution of the second phase, the *VLR/SN* generates a new *Rand₂* and a new $MAC_{VLR/SN}$ and $AUTN_{VLR/SN}$. When *MS* needs to authenticate itself to network then the *VLR/SN* is responsible for authenticating *MS* (i.e., only the second phase is executed). Also, the *MS* and *VLR/SN* maintains track of the times (*Count*) of executing authentication procedures.

4. Security Analysis for Extension of AKA Protocol for UMTS

The proposed protocol maintains the security features which are provided by UMTS AKA to provide the following security objectives:

- i. Mutual authentication between *MS* and *VLR/SN*.
- ii. Entity authentication between *MS* and *VLR/SN*.
- iii. Confidentiality of user data and signaling data.
- iv. Data integrity that the *MS* and *VLR/SN* is able to verify that signaling data has not been modified in an unauthorized way.

The proposed protocol includes the following security features. These features are not provided by UMTS AKA protocol:

- v. Provides mutual authentication between *MS* and it *HN*:
 - *HN* authenticates *MS* by computing $f_1(K, Rand_1)$ and compares the result with the received MAC_{MS} , if the comparison fails then rejects authentication, otherwise *HN* continues the authentication process
 - *MS* authenticates *HN* by verifying $MAC_{VLR/SN}$. To verify $MAC_{VLR/SN}$ we need to compute $MAC_{HN} = f_1(K, Rand_1 || AMF)$, $f_1(K_{Temp}, MAC_{HN} / |Rand_2 || Count)$ and compare the result of computing with the received $MAC_{VLR/SN}$. If the two values, computed value and received value are matching then this means that *MS* authenticates *HN* because the value of $MAC_{VLR/SN}$ is correct then this leads to infer that MAC_{HN} is correct because MAC_{HN} is included in $MAC_{VLR/SN}$.
- vi. No need to generate authentication vector in *HN* and send it to *VLR/SN*. The *VLR/SN* is responsible for generating one authentication vector, when *MS* sends authentication request, because *HN* generates temporary key and sends it to the *VLR/SN* and this key is used to generate authentication vector, and to compute cipher key and integrity key. This leads to avoid the bandwidth consumption between *SN* and *HN*. Also, *HN* is not involved in every authentication data request and temporary key is used to generate authentication vector.

5. Comparison between the Proposed Protocol and Other Authentication Protocols

Table 1 shows the comparison among the UMTS authentication and Key agreement protocol [1, 7, 15] with the proposed protocol.

	UMT S- AKA	Lin& Hsia	AP- AK A	Propos ed AKA
Mutual Authentication between MS and SN	Yes	Yes	Yes	Yes
Mutual Authentication between MS and HN	No	No	No	Yes
User Traffic Confidentiality	Yes	Yes	Yes	Yes
Signaling Data Integrity	Yes	Yes	Yes	Yes
Prevent Replay Attack	Yes	Yes	Yes	Yes
Reduction of Bandwidth Consumption between SN and HN	No	No	No	Yes
Reduction of Storage Space overhead for SN Database	No	Yes	No	Yes
Need Synchronization between MS and HN	Yes	No	No	No
Use Temporary Key	No	No	No	Yes
HN Involved in each Authentication Data Request	Yes	Yes	Yes	No

Table 1: Comparison between the UMTS Authentication and Key Agreement Protocols and the Proposed Protocol.

6. Conclusion

To enhance the authentication procedure several enhancements have been developed in this proposed protocol. The proposed protocol has the following advantages when compared with UMTS authentication and key agreement protocols:

- i. Reducing the bandwidth consumption between MS and its HN.
- ii. Reducing storage space overhead of the SN.
- iii. Eliminating SQN resynchronization between MS and its HN.
- iv. Using temporary key and bilateral authentication between MS and its HN.

All these advantages have been verified by software simulation, although a complete performance analysis for the proposed protocol is open for any further works.

References

- [1] 3GPP TS 21.133. 3GPP Security; Security Architecture.
- [2] 3GPP TS 35.205. 3GPP Security; Specification of the MILENAGE Algorithm Set; Document 1: General.
- [3] 3GPP TS 35.206. 3GPP Security; Specification of the MILENAGE Algorithm Set; Document 2: Algorithm specification.
- [4] 3GPP TS 35.207. 3GPP Security; Specification of the MILENAGE Algorithm Set; Document 3: Implement test data
- [5] Al-Muhtadi, J., Mickunas, D. and Campbell, R. (2002). A Lightweight Reconfigurable Security Mechanism for 3G/4G Mobile. *IEEE Wireless Communications*, Vol. 9 (2002) pp. 60-65, April 2002.
- [6] Chung-Ming, H. And Jian-Wei, L. (2005). Authentication and Key Agreement Protocol for UMTS with Low Bandwidth Consumption. *AINA'05, 19th International Conference on Advanced Information Networking and Applications (AINA'05) Vol. 1 (2005)*, pp. 392-397.
- [7] Harn, L. and Wen-Jung, H. (2003). On the Security of Wireless Network Access with Enhancements. In *Proceedings of the 2003 ACM workshop on Wireless Security, WISE 2003*, page 88-95.
- [8] IP Security Protocol. (2002). Internet Engineering Task Force (IETF). Working Group. [Internet Accessed 12 April 2003] <http://www.ietf.org/html.charters/upsec-charter.html>.
- [9] Johnson, M. (2002). Revenue Assurance, Fraud and Security in 3G Telecom Services. *VP Business Development Visual Wireless AB, Journal of Economic Management*, 2002, Volume 1, Issue 2.
- [10] L. Salgarelli, L., Buddhikot, M. Garay, J., Patel, S. and Miller, S. (2003). The Evaluation of wireless LANs and PANs – Efficient Authentication and Key Distribution in Wireless IP Networks. *IEEE Personal Communication on Wireless Communication* 10(6):52-61, December 2003.
- [11] Lin, H. (1999). Security and Authentication in PCS. *Computers & Electrical Engineering*, Vol. 25, No. 4, July 1999, pp. 225-248.
- [12] Stalling, W. (2003). *Cryptography and Network Security, Principles and Practice*. 3rd edition. USA, Prentice Hall.
- [13] Stefan, P, and Fridrich R. (1998). Authentication Schemes for 3G mobile radio Systems. *The Ninth IEEE International Symposium on*, 1998. pp. 126-130.
- [14] Walker, M. (2003). On the Security of 3GPP Networks, [Internet Accessed 20 April 2003] http://www.esat.kuleuven.ac.be/cosic/eurocrypt2000/mike_walker.pdf
- [15] Zhang, M. and Fang, Y. (2005). Security Analysis and Enhancements of 3GPP Authentication and Key Agreement Protocol. *IEEE Transactions on wireless communications*, Vol. 4, No. 2.