An Improved Authentication and Key Agreement Protocol of 3G

Sudan Jha
Scholar
Department of Computer Engineering
OPJS University, Churu – Rajasthan.

Abstract - With the development of mobile communication network, the requirements of mobile users for data services are higher and higher, which makes data service become more diversiform and various service providers appear on after the other. As a result, data services increasingly become the main service in mobile network. The Universal Mobile Telecommunications System (UMTS) is one of the new 'third generation' (3G) mobile cellular communication systems being developed within the framework defined by the International Telecommunications Union (ITU) known as IMT-20001.UMTS aims to provide a broadband, packet-based service for transmitting video, text, digitized voice, and multimedia at data rates of up to 2 Mbps while remaining cost effective. The AKA procedure is the essence of authenticating a user to the network and vice versa. AKA procedures in UMTS have increased security compared with GSM. However, during its development some security problems emerged. Although the authentication and key agreement (AKA) protocol solve some, it still has some flaws such as lacking complete authentication and interworking and so on. In order to those problem preferable, aiming at the security threaten for services based on mobile network and the problems with the existing AKA, we analyzed the existing Authentication and Key Agreement (AKA) protocol, and points out the security flaws among it and possible methods of attack. For the security flaws, an improved AKA protocol is proposed. In the end, we analyzes the improved AKA protocol.

Keywords – Watermarking, Haar Wavelet, DWT, PSNR

I. INTRODUCTION

The third generation mobile communication system (3G) not only support the tradition pronunciation service, it will also provide other services, such as the multimedia services, the data service, electronic commerce, the electronics trade as well as the Internet serves and so on. If we apply 3G in the special domain of information based society construction, it will certainly to enhance the process of information based society construction effectively. As the openness of 3G wireless channel, the security problem always a key factor of affecting the system performance. Most information in the special domain is confidential information and should be controlled in a secure scope, therefore, it is the key problem that preventing this information from being tampered and being got by illegal users in the wireless channel. In the safe communication, the implementation of the authentication and the key agreement is the premise and guarantee of the encrypted communication.

The Authentication and Key Agreement (AKA) protocol is a security protocol used in 3G networks. AKA is also used for one-time password generation mechanism for Digest access authentication. It is a challenge-response based mechanism that uses symmetric cryptography.AKA provides procedures for mutual authentication of the MS and serving system. The successful execution of AKA results in the establishment of a security association (i.e., set of security data) between the MS and serving system that enables a set of security services to be provided. AKA is typically run in a UMTS IP Multimedia Services Identity Module (ISIM), which resides on a smart card like device that also provides tamper resistant storage of shared secrets.

At present the 3GPP-AKA protocol using in current 3G system has the shortage of security, it cannot satisfy the high secure demand of the special domain. In order to those problem preferable, aiming at the security threaten for services based on mobile network and the problems with the existing AKA, we analyzed the existing Authentication and Key Agreement (AKA) protocol, and points out the security flaws among it and possible methods of attack. For the security flaws, an improved AKA protocol is proposed and it is further analyzed.

II. WHEN TO USE AKA?

- Registration of a user in a SN

- After a service request
- Location Update Request
- Attach Request
- Detach request
- Connection re-establishment request

Registration of a subscriber in a SN (Serving Network) typically occurs when the user goes to another country. The first time the subscriber then connects to the SN, he gets registered in the SN. Service Request is the possibility for higher-level protocols/applications to ask for AKA to be performed. E.g. performing AKA to increase security before an online banking transaction. The terminal updates the Home Location Register (HLR) regularly with its position in Location Update Requests. Attach request and detach request are procedures to connect and disconnect the subscriber to the network. Connection re-establishment request is performed when the maximum number of local authentications has been conducted.

III. TRADITIONAL AUHTHENITICATION & KEY AGREEMENT (AKA) PROTOCOL

3.1. PROTOCOL DESCRIPTION

Participators in the implementation of authentication and key agreement (AKA) protocol include:

- User terminal: Mobile Equipment/Universal Subscriber Identity Module(ME/USIM),
- Visit network: Visit Location Register/Serving GPRS Support Node (VLR/SGSN) and
- Ownership network: Home Environment/Home Location Register (HE/HLR).

The implementation of AKA takes the following conditions as the premise:

(1)The user and ownership network shared the system key K.
(2)The user trust the ownership network HE.
(3)The user's HE believes VLR can manage the information safely.
(4)The communication between HE and VLR is secure enough.

The process of authentication includes five steps as followed:
(1)MS→VLR: IMSI, HLR
(2)VLR→HLR: IMSI
(3)HLR→VLR: AV=RAND||XRES||CK||IK||AUTN
(4)VLR→MS:RAND||AUTN
(5)MS→VLR: RES

The exact process is showed in Fig1.

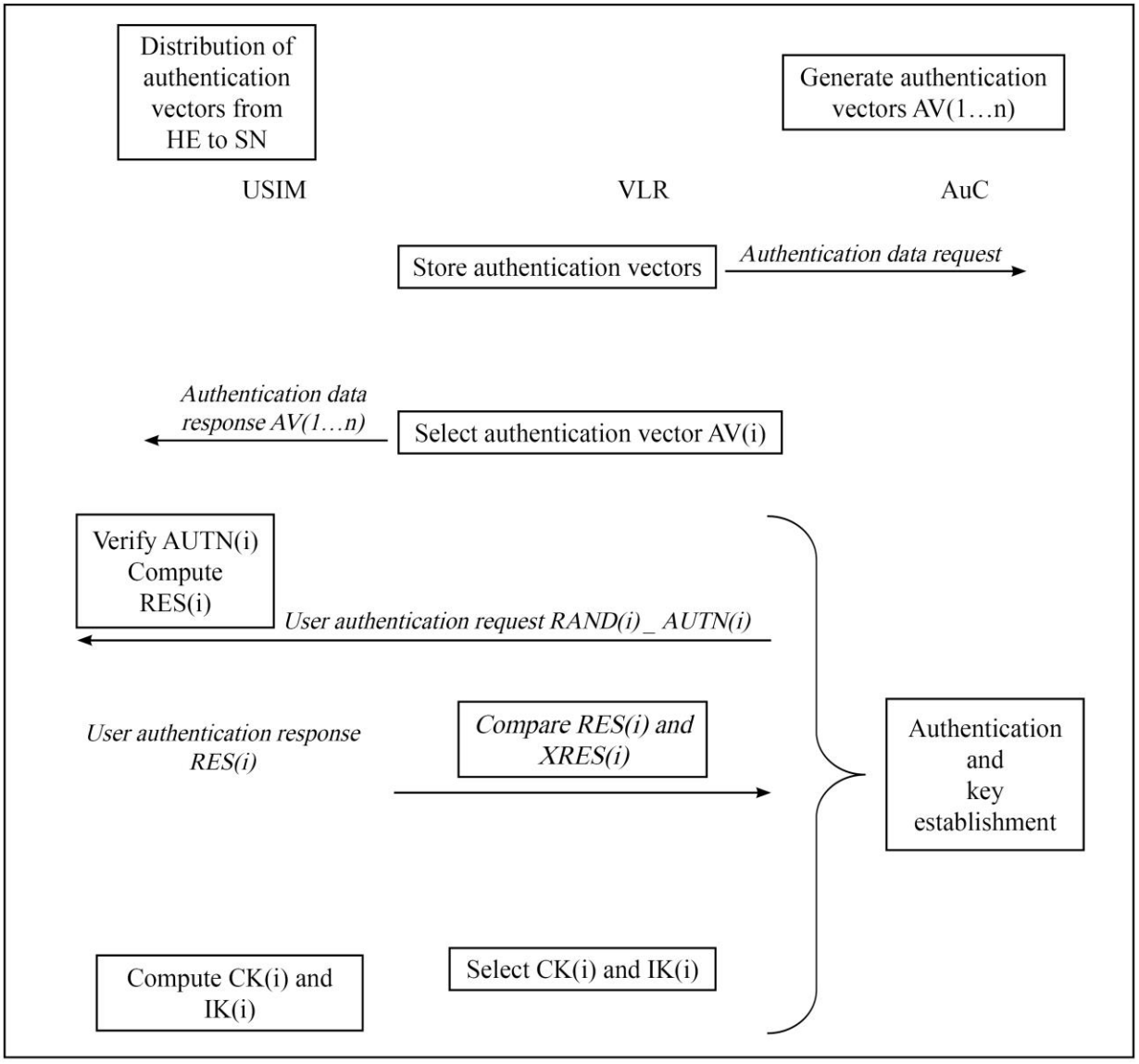


Fig 1: *Overview of Authentication and Key Agreement*

The cornerstone of the authentication mechanism is a master key or a subscriber authentication key K, which is shared between the USIM of the user and the home network database, Authentication Centre (AuC).The key is permanently kept secret and has a length of 128 bits. The key is never transferred from these two locations (i.e., the user has no knowledge of the master key).

Apart from mutual authentication, keys for encryption and integrity checking are also derived. These are temporary keys (with the same length of 128 bits) and are derived from the permanent key K during every authentication event. It is a basic principle in cryptography to keep the use of permanent keys to a minimum and, instead, derive temporary keys from it for protection of bulk data.

This process is the key part of the protocol. Authentication and key agreement (Fig. 1) consists of two procedures. First, the HE distributes authentication information to the SN. Second, an authentication exchange is run between the user and the SN. The authentication information consists of the parameters necessary to carry out the authentication exchange and provide the agreed keys.

The authentication procedure begins when the user is identified in the SN.Identification occurs when the identity of the user (i.e., permanent identity International Mobile Subscriber Identity (IMSI), or temporary identity Temporary Mobile Subscriber Identity (TMSI), or Packet TMSI (P-TMSI), has been transmitted to the VLR or SGSN.When user ME roams to the visit network VLR and initiates the service request, VLR will send authentication request to the ownership network HE of the use. The AuC contains the master key of each user. Once HE receives the request, it generates an ordered array of n authentication vectors based on the knowledge of the IMSI.

Each authentication vector consists of five components (and hence may be called a UMTS 'quintet' in analogy to GSM 'triplets'): a random number RAND, an expected response XRES, a cipher key CK, an integrity key IK and an authentication token AUTN. This array of n authentication vectors is then sent from the HE to the SN. It is good for n authentication exchanges between the SN and the USIM.VLR saves these authentication vectors. In an authentication exchange the SN first selects the next (the i-th) authentication vector from the array and sends the parameters RAND (i) and AUTN (i) to the user. Authentication vectors in a particular node are used on a FIFO basis. In the SN, one authentication vector is needed for each authentication instance (i.e., for each run of the authentication procedure).This means that the (potentially long distance) signaling between SN and AuC is not needed for every authentication event and that in principle this signaling can be done independently of user actions after initial registration.Indeed, the VLR/SGSN may fetch new authentication vectors from AuC well before the number of stored vectors runs out.

The user receives the information which VLR sends, and calculates the anticipated XMAC=f1K (SQN||RAND||AMF), then compares it with MAC which received, if the result is inconsistent, then the user will receive the report of authentication failure, and the authentication process is over. Finally, VLR gives a report to the HE about the failure, and restarts an authentication process. The USIM checks whether AUTN(i) can be accepted and, if so, produces a response RES(i), which is sent back to the SN.AUTN(i) can only be accepted if the sequence number contained in this token is fresh.

At the same time, user begins to produce CK and IK. After VLR receives RES, compares with memory XRES, if consistent, then considers the authentication and the key agreement is success. The established keys CK(i) and IK(i) will then be transferred by the USIM to the mobile equipment and by the VLR (or SGSN) to the RNC(Radio Network Controller); the keys are then used by the ciphering and integrity functions in the MS(Mobile Station) and in the RNC when encryption and integrity protection start.

VLR/SGSNs can offer secure service even when HE/AuC (Authentication Centre) links are unavailable by allowing them to use previously derived cipher and integrity keys for a user so that a secure connection can still be set up without the need for an authentication and key agreement. Authentication is in that case based on a shared integrity key, by means of data integrity protection of signaling messages.

3.1.2. AUTHENTICATION VECTOR DISTRIBUTION:

Fig 2 shows the generating process of authentication vector. The process begins by picking an appropriate sequence number (SQN).Roughly speaking, what is required is that SQNs are chosen in ascending order. The purpose of the SQN is to provide the user (or more technically the USIM) with proof that the generated authentication vector is fresh (i.e., it has not been used before in an earlier run of authentication. In parallel with the choice of SQN,a 128-bit long unpredictable challenge RAND is generated. This is a mental way so that the output of one function reveals no information about the outputs of the other functions. For each user the HE/AuC keeps track of a counter SQN_{HE}.

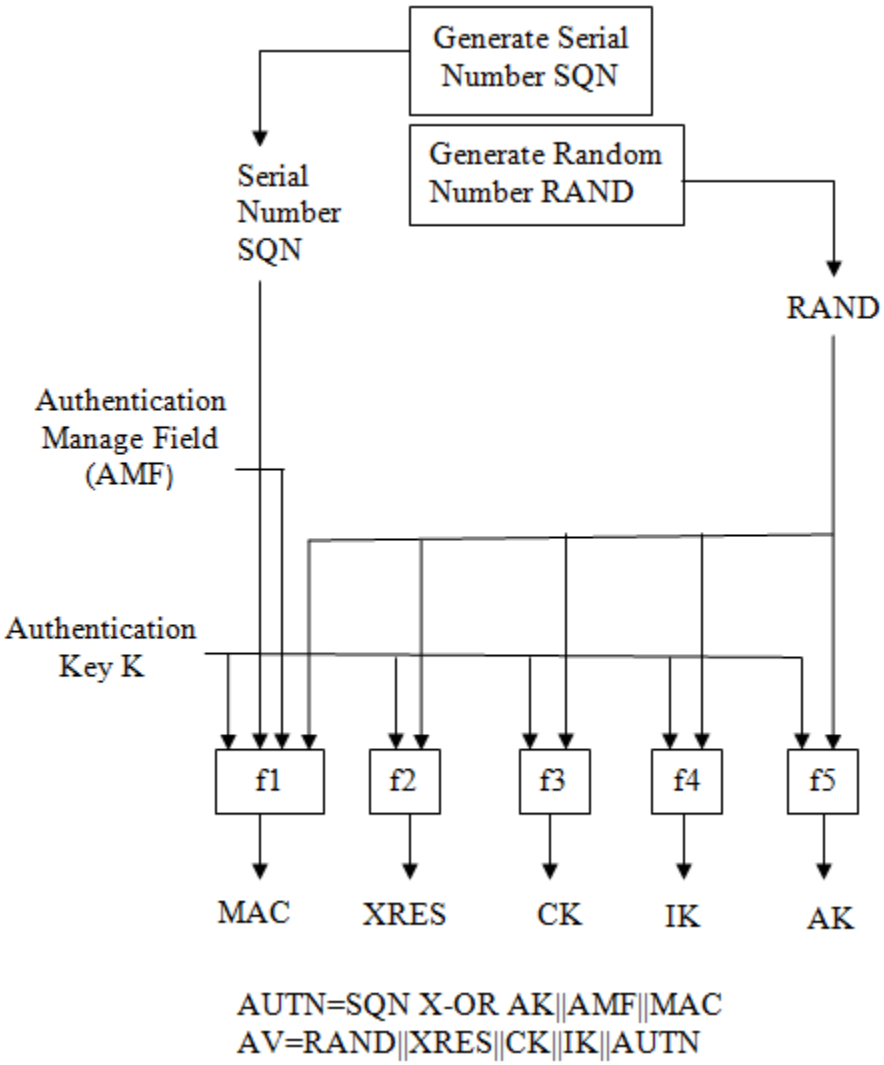


Fig2: Authentication Vector Generating Process

In the Fig 2, f1 and f2 are the key authentication functions, f3, f4 and f5 are the key generating functions, all of them are known algorithm to ME and HE. SQN is the sequence number saved in ME and the HE, when the transmission different or carries on the hideaway with AK with it.

Subsequently the following values are computed:

- a Message Authentication Code M AC=f1K(SQN||RAND||AMF) where f1 is a message authentication function;
- an eXpected RESponse XRES=f2K(RAND) where f2 is a message authentication function;
- a Cipher Key CK=f3K(RAND)where f3 is a key generating function;
- an Integrity Key IK=f4K(RAND)where f4 is a key generating function;
- an Anonymity Key AK=f5K(RAND)where f5 is a key generating function.

Finally the authentication token AUTN=SQN ⊕ AK||AMF||MAC is constructed.

AK is an anonymity key used to conceal the sequence number as the latter may expose the identity and location of the user. The concealment of the sequence number is to protect against passive attacks only.

An authentication and key management field AMF is included in the authentication token of each authentication vector. Example uses of AMF include:

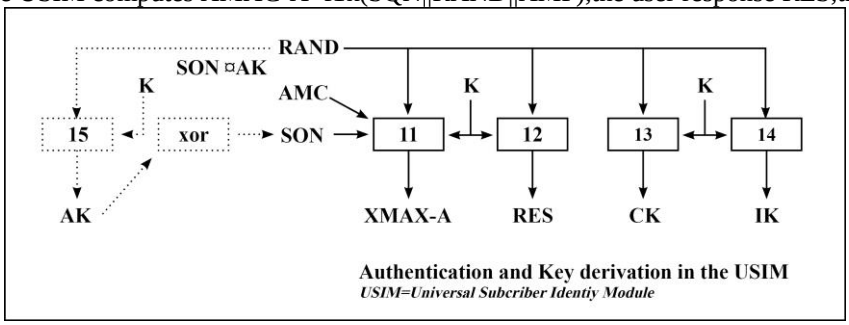
- Support multiple authentication algorithms and keys (This mechanism is useful for disaster recovery purposes.AMF may be used to indicate the algorithm and key used to generate a particular authentication vector.)
- Changing sequence number verification parameters (This mechanism is used to change dynamically the limit on the difference between the highest SEQ accepted so far and a received sequence number SEQ.)
- Setting threshold values to restrict the lifetime of cipher and integrity keys (The USIM contains a mechanism to limit the amount of data that is protected by an access link key set. The AMF field may be used by the operator to set or adjust this limit in the USIM).

Parameter Name	Length
RES	128 bits
IK	128 bits
CK	64 bits
MAC-S	64 bits
MAC	16 bits
AMF	48 bits
AK	48 bits
SQN	128 bits
RAND	128 bits

From Fig 2 we can see that aggressor A may pretend this user to enter the network. But the encryption key (CK) and the integrality key (IK) has not transmitted in the wireless connection, the aggressor is unable to obtain these keys to carry on the normal privacy communication.

3.1.2.1. AUTHENTICATION AND KEY DERIVATION IN THEUSIM

On receipt of a (RAND, AUTN) pair, the USIM acts as follows: First, it retrieves the unconcealed SQN. If the SQN is concealed, the USIM computes AK=f5k(RAND) and retrieves the SQN by computing SQN= (SQN X-OR AK) X-OR AK.Then the USIM computes XMAC-A=f1k(SQN||RAND||AMF),the user response RES,the CK and the IK.



Authentication and Key derivation in the USIM
USIM=Universal Subcriber Identiy Module

3.2. PROTOCOL SECURITY ANALYSIS

The main flaws of the 3GPP-AKA protocol is described as following points:

1. The permanent status information can be intercepted easily.
2. Bidirectional authentication is incompletely;
3. It is difficult to operate sequence number.
4. The transmission of authentication vector in the network is unsecure.
5. The encryption algorithm is fixed, and there is no way to complement key agreement safely and flexibly.
6. ME and HE always share system key K, once divulges to the user is the inestimable loss.
7. The security of the key generating algorithm is determined by algorithm.

3.3. POSSIBLY EXISTS ATTACK

According to the analysis of the protocol process, this authentication plan has realized the authentication of VLR to MS as well as MS to the HLR, but does not request the MS to authenticate VLR. What attacks an aggressor may carry on by intercepting validated user identification/identity are described as following:

1. MS→A: IMSI
2. A→VLR: IMSI
3. VLR→HLR: IMSI
4. HLR→VLR: AV=RAND||XRES||CK||IK||AUTN
5. VLR→A:RAND||AUTN
6. A→MS:RAND||AUTN
7. MS→A: RES
8. A→VLR: RES

Thus, aggressor A may pretend legal user to enter the network. But the encryption key CK and the integrality key IK has not transmitted in the wireless connection, the aggressor is unable to obtain these keys to carry on the normal privacy communication. In addition, the above plan has not considered the authentication and the privacy communication between clients. If the aggressor intercepts the information between VLR and HLR, he can obtain the authentication vector (AV) transmitting from HLR to VLR, thus can obtain encryption key (CK) and integrality key (IK). Therefore, if the aggressor again pretends this validated user to enter the network, he can realize the normal privacy communication, and the information transmitted by validated user also loses secrecy.

IV. WEAKNESSES IN UMTS SECURITY MECHANISMS

To sum up, the main weaknesses in UMTS security mechanism are:

1. Integrity keys used between UE and RNC generated in VLR/SGSN are transmitted unencrypted to the RNC (and sometimes between RNCs).
2. IMSI is transmitted in unencrypted form.
3. For a short time during signaling procedures, signaling data are unprotected and hence exposed to tampering.

V. IMPROVED AKA PROTOCOL

According to the analysis of AKA, the traditional AKA protocol has two security problems, incomplete bidirectional authentication and unsafe vector transmission. Here, we propose an improved AKA protocol, expecting to enhance the security of the traditional protocol.

5.1. THE AGREEMENT DESIGN SHOULD FOLLOW PRINCIPLE

When design authentication protocol, there are three key requirements:

1. Secrecy
2. no redundancy, and
3. Authentication identification

In order to fulfill these requirements, therefore, some design principles are proposed as following:

1. *The design goal should be clear, should not have the ambiguity;*
2. *The best way to implement the formalized description of the security protocol is using formal language.*
3. *Proving the security protocol has achieved the design goal through the formalization analysis method.*
4. *The security has nothing to do with the encryption algorithm used.*
5. *We should guarantee the temporary value and the conversation key and other important news be fresh, to prevent the replay attack.*

6. *Select the asynchronous authentication method as far as possible, avoid using the synchronized authentication way.*
7. *Has the ability to resist common attack, specially the replay attack.*
8. *Carry on the risk analysis of the runtime environment, and make the initial securities supposition as few as possible.*
9. *Be usable. It can be used in different protocol layers of different network.*
10. *Reduce the password operation and cost as far as possible, and expand applied scope.*

5.2 DESCRIPTION OF THE IMPROVED PROTOCOL

The improved authentication and key agreement schema is showed in Fig 3. The improved authentication protocol requests the VLR and HLR to share the system key KH, the same encryption algorithm and the same integrality confirmation algorithm.

The protocol flow is showed as following:

i. *VLR found IMSI according to TMSI, and transmitted the E (K, R)||MAC (K, R) and other information to HLR.*

ii. *HLR decrypted the E (K, R) by the shared key between HLR and MS to get the number R, and validated the integrity of the R.*

iii. *HLR used the derived algorithm to produce R1-Rn, and used the shared key between HLR and VLR to encrypt R, then obtained E (KH, R1||R2.||Rn), finally, get the integrity check code MAC (KH, R1||R2. .Rn).*

iv. *HLR uses KH to carry on the encryption of AV vector group and produces the integrity check code for this MS,therefore, obtains the E (KH, AV1||AV2.||AVn) and the MAC (KH, AV1||AV2.||AVn).*

v. *HLR transmit E (KH, AV1||AV2.||AVn), MAC (KH, R1||R2.||Rn), E (KH, R1||R2.||Rn) and MAC (KH, AV1||AV2.||AVn) to VLR.*

vi. *VLR uses KH to decrypt AV1-AVn and R1-Rn, and check their integrity.*

vii. *VLR selects AVn, and attaches the Rn to the reply data transmitted for MS.*

viii. *The user USIM uses derived algorithm to produce R1-Rn,and finds whether there is number among R1 and Rn is equal to the number Rn transmitted from VLR.If yes, then completes the authentication of MS to the VLR.*

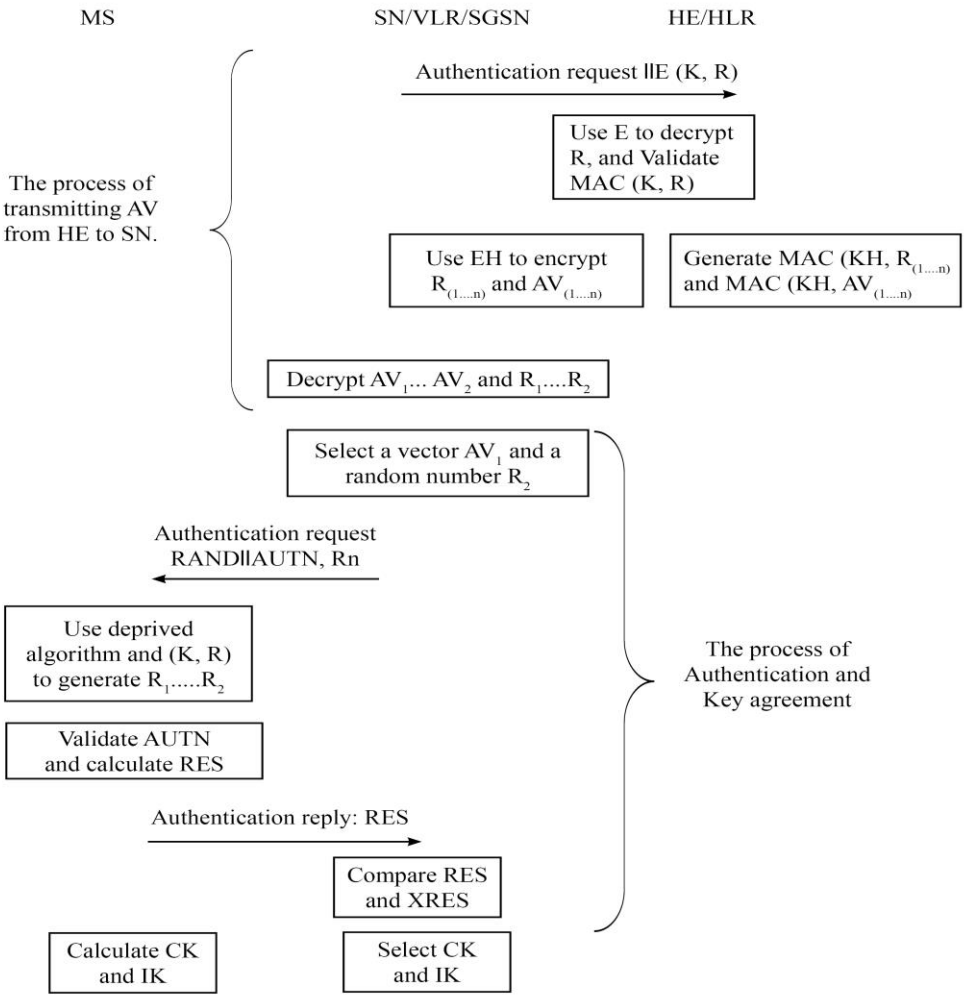
From the protocol flow, we can see that the improved protocol requires the VLR and HLR to share system key KH which used in the process of MS authenticating the identification of the VLR as well as in the process of validating the information integrity and security between VLR and the HLR. In addition, when MS send the request information to the VLR, we add the data E (K, R) into the request information. The generating process of the data E (K, R) is described as following:

Firstly, MS produces a random number R and use the user key K shared between MS and HLR to encrypt it. The encrypted R is E (K, R). Then we should calculate MAC (K, R). Finally, MS send the TMSI, E (K, R) and MAC (K, R) to the VLR.

5.3. ANALYSIS OF THE IMPROVED PROTOCOL

According to the description of the protocol in the above section, we may see that the improved protocol has solved some flaws in traditional AKA protocol. The solved problem is listed as following:

i. The confidentiality of information transmitted in the network: In the improved protocol, we require the VLR and HLR to share the system key KH, the same encryption algorithm and the same integrality confirmation algorithm. Thus, we can guarantee confidentiality of information transmitting between HLR and VLR, and causes the aggressor unable to obtain the authentication vector, thus prevents the pretending MSC/VLR attack.
ii. Authentication of MS to VLR. Because there is no shared secret between MS and VLR, therefore is unable to realize the direct authentication. But we can realize authentication indirectly through the HLR. The authentication of MS to VLR depends on the confidentiality of the random number generated by MS. And only the legal VLR can decrypt the information E (K, R) transmitted by MS correctly. Therefore, once MS receives the correct number R, it can confirm VLR is legal.



VI. ADVANTAGES OF AKA PROTOCOL

The major advantages of AKA include:

- Larger authentication keys (128-bit)
- Stronger hash function (SHA-1)
- Support for mutual authentication
- Support for signaling message data integrity
- Support for signaling information encryption
- Support for user data encryption

VII. FURTHER DEVELOPMENTS IN UMTS SECURITY

Work on the next UMTS release has started. This will introduce new security features. Many of these features will be introduced to secure the new services which will be introduced, e.g. presence services, push services and multicast/broadcast services. Looking more into the future, mobile cellular systems will have to accommodate a variety of different radio access networks including short-range wireless technologies, connected to a common core network. On the user side the concept of a monolithic terminal, as we know it, is dissolving. Distributed terminal architectures are appearing whose components are interconnected by short-range radio links. These new developments represent a major challenge to the UMTS security architecture. A collaborative research project funded by the European Union and called SHAMAN (Security for Heterogeneous Access in Mobile Applications and Networks) have tackled these issues. A separate project is also underway to identify research topics in the area of mobile communications; this project is called PAMPAS (Pioneering Advanced Mobile Privacy and Security).

VIII. CONCLUSION

AKA procedures in UMTS have increased security compared with GSM All messages should be integrity checked, but indirectly by requiring confidentiality protection together with integrity. AKA concept is used to perform authentication of the user and network, as opposed to 2G systems, which only authenticated users in a system. The confidentiality algorithm is stronger than its GSM predecessor. The integrity mechanism works independent of confidentiality protection and provides protection against active attacks. The design of cryptographic algorithms is open and they are extensively crypto analyzed. Moreover, the architecture is flexible and more algorithms can be added easily. In view of the flaw existed in traditional AKA protocol, we have designed an improved AKA protocol. The improved protocol has realized MS to the VLR authentication and the confidentiality of information transmitted in network, and enhanced the security of information transmitted in the wireless channel.

REFERENCES

[1] Education Technology and Computer Science, 2009. ETCS '09. First
[2] International Workshop on, 7-8 March 2009, Wuhan, Hubei.
[3] Engr.Mujtaba Hassan, Engr.Munaza Razzaq and Engr.Asim
[4] Shahzad,"Comprehensive Analysis of UMTS Authentication and Key
[5] Agreement" in International Journal of Computer and Network Security,
[6] Vol. 2, No.2, February 2010.
[7] K. Boman, G. Horn, P. Howard, and V. Niemi,"Umts Security", October 2003
[8] Valtteri Niemi and Kaisa Nyberg,"UMTS Security", 2003.

[9] B. Corona, M. Nakano, H. Pérez, "Adaptive Watermarking Algorithm for Binary Image Watermarks", *Lecture Notes in Computer Science, Springer, pp. 207-215, 2004.*
[10] A. A. Reddy and B. N. Chatterji, "A new wavelet based logo-watermarking scheme," Pattern Recognition Letters, vol. 26, pp. 1019-1027, 2005.
[11] P. S. Huang, C. S. Chiang, C. P. Chang, and T. M. Tu, "Robust spatial watermarking technique for colour images via direct saturation adjustment," Vision, Image and Signal Processing, IEE Proceedings -, vol. 152, pp. 561-574, 2005.
[12] F. Gonzalez and J. Hernandez, " A tutorial on Digital Watermarking ", In IEEE annual Carnahan conference on security technology, Spain, 1999.
[13] D. Kunder, "Multi-resolution Digital Watermarking Algorithms and Implications for Multimedia Signals", Ph.D. thesis, university of Toronto, Canada, 2001.
[14] J. Eggers, J. Su and B. Girod," Robustness of a Blind Image Watermarking Scheme", Proc. IEEE Int. Conf. on Image Proc., Vancouver, 2000.
[15] Barni M., Bartolini F., Piva A., Multichannel watermarking of color images, IEEE Transaction on Circuits and Systems of Video Technology 12(3) (2002) 142-156.
[16] Kundur D., Hatzinakos D., Towards robust logo watermarking using multiresolution image fusion, IEEE Transcations on Multimedia 6 (2004) 185-197.
[17] C.S. Lu, H.Y.M Liao, "Multipurpose watermarking for image authentication and protection," *IEEE Transaction on Image Processing*, vol. 10, pp. 1579-1592, Oct. 2001.
[18] L. Ghouti, A. Bouridane, M.K. Ibrahim, and S. Boussakta, "Digital image watermarking using balanced multiwavelets", *IEEE Trans. Signal Process*., 2006, Vol. 54, No. 4, pp. 1519-1536.
[19] P. Tay and J. Havlicek, "Image Watermarking Using Wavelets", in *Proceedings of the 2002 IEEE*, pp. II.258 – II.261, 2002.
[20] P. Kumswat, Ki. Attakitmongcol and A. Striaew, "A New Approach for Optimization in Image Watermarking by Using Genetic Algorithms", *IEEE Transactions on Signal Processing*, Vol. 53, No. 12, pp. 4707-4719, December, 2005.
[21] H. Daren, L. Jifuen,H. Jiwu, and L. Hongmei, "A DWT-Based Image Watermarking Algorithm", in *Proceedings of the IEEE International Conference on Multimedia and Expo*, pp. 429-432, 2001.
[22] C. Hsu and J. Wu, "Multi-resolution Watermarking for Digital Images", *IEEE Transactions on Circuits and Systems- II*, Vol. 45, No. 8, pp. 1097-1101, August 1998.
[23] R. Mehul, "Discrete Wavelet Transform Based Multiple Watermarking Scheme", in *Proceedings of the 2003 IEEE TENCON*, pp. 935-938, 2003.