Advances in Wireless and Mobile Communications.
ISSN 0973-6972 Volume 10, Number 2 (2017), pp. 341-355

http://www.ripublication.com

IMPROVED CELL AUTHENTICATION & AKA PROTOCOL FOR THE BETTER DELIVERY OF QOS OF 4G NETWORKS

Professor Dr. Sudan Jha
School of Computer Engineering
KIIT University, Bhubaneswar, Odiha – 751024, India

Abstract

With the improvement of versatile correspondence arrange, the necessities of portable clients for information administrations are ever more elevated, which makes information benefit turn out to be more diversiform and different specialist organizations show up on after the other. Accordingly, information benefits progressively turn into the primary administration in versatile system. The Universal Mobile Telecommunications System (UMTS) has provided a very wide domain of 4G frameworks being created inside the structure characterized by IMT-20001. UMTS is targeted to avail to the end users with a broadband, bundled videos, contents of various formats, digitized voice, and sight and sound at information rates. The AKA system is the embodiment of verifying a client to the system and the other way around. Otherwise known as methodology in UMTS have expanded security contrasted and GSM.

Be that as it may, amid its improvement some security issues developed. Despite the fact that the validation and key understanding (AKA) conception illuminate a few, regardless it has a few imperfections, for example, lacking complete confirmation and interworking et cetera. So as to address the above-mentioned issues at their best, considering the security issues for both SAP and ERPs in view of portable systems and the issues with the current AKA, the paper examines the current Authentication and Key Agreement (AKA), and yields out the security imperfections between them with conceivable techniques for assault. For the security imperfections, an enhanced AKA conception is proposed. At last, the paper breaks down the enhanced AKA conceptions.

Keywords: UMTS (Universal Mobile Telecommunication Systems), International Telecommunications Union (ITU); Access Points; IMT-20001; 4G, HTTP, FTP; TELNET protocols, IEEE 802.1x protocol with EAP-TTLS; Mutual Authentication; AKA;

I. INTRODUCTION

As we are in the fourth era of 4G, the third era versatile correspondence framework (3G) not just bolster the custom elocution benefit, it will likewise give different administrations, for example, the sight and sound administrations, the information benefit, electronic business, the gadgets exchange and the Internet serves et cetera. In the event that we apply 4G in the extraordinary space of data based society development, it will unquestionably to improve the procedure of data based society development adequately. As the openness of 4G remote channel, the security issue dependably a key variable of influencing the framework execution. Most data in the unique area is secret data and ought to be controlled in a protected extension, subsequently, it is the key issue that keeping this data from being altered and being got by illicit clients in the remote channel. In the sheltered correspondence, the usage of the validation and the key assertion is the start and assurance of the encoded correspondence.

The AKA conception is a security conception utilized as a part of 4G systems. Otherwise known as is additionally utilized for one-time secret key era system for Digest get to validation. It is a test reaction based instrument that utilizations symmetric cryptography. AKA gives methodology to common verification of the MS and serving framework. The fruitful execution of AKA results in the foundation of a security affiliation (i.e., set of security information) between the MS and serving framework that empowers an arrangement of security administrations to be given. Otherwise known as is regularly keep running in an UMTS IP Multimedia Services Identity Module (ISIM), which lives on a brilliant card like gadget that likewise gives alter safe stockpiling of shared mysteries.

At present the 4GPP-AKA conception utilizing as a part of current 4G framework has the deficiency of security, it can't fulfill the high secure request of the unique area. To those issues best, going for the security debilitate for administrations in view of versatile system and the issues with the current AKA, we broke down the current Authentication and Key Agreement (AKA) conception, and brings up the security defects among it and conceivable strategies for assault. For the security blemishes, an enhanced AKA conception is proposed and it is further examined.

II. WHY AKA?

The current Authentication and Key Agreement (AKA) has several reasons to be adopted out. It constitutes of significant features like acknowledging Connection re-foundation, Refreshing Location, Administration, along with peeping Registration of a client in a SN, attachments ack, detachments ack, and several other acks. Enlistment of an endorser in a SN (Serving System) commonly happens when the client goes to another nation. The first run through the endorser then associates with the SN, he gets enrolled in the SN. Benefit Ask for is the likelihood for larger amount conceptions/applications to request Otherwise known as to be performed. E.g. performing Otherwise known as to expand security before a web based managing an

account exchange. The terminal updates the Home Area Enroll (VHLR) frequently with its position in Area Refresh Asks. Join ask for and disengage demand are methodology to associate and separate the endorser of the system. Association re-foundation demand is performed when the most extreme number of neighborhood validations has been directed.

III. TRADITIONAL AUTHENTICATION AND KEY AGREEMENT (AKA) PROTOCOL

3.1. Conception Depiction: - Participators in the execution of validation and key understanding (Otherwise known as) conception include:

- User terminal: Versatile Gear/Widespread Supporter Personality Module(ME/USIM),
- Visit arrange: Visit Area Enlist/Serving GPRS Bolster Hub (HVLR/SGSN) and
- Ownership organize: Home Condition/Home Area Enroll (HE/VHLR).

The execution of otherwise known as takes the accompanying conditions as the introduce:

1. The client and proprietorship organize shared the framework key K.
2. The client believes the proprietorship arrange HE.
3. The client's HE trusts HVLR can deal with the data securely.
4. The correspondence amongst HE and HVLR is sufficiently secure.

The procedure of validation incorporates five stages as took after:

i. MS→HVLR: AMSII, VHLR

ii. HVLR→VHLR: AMSII

iii. VHLR→HVLR: AV=RAND||XRES||CK||IK||AUTN

iv. HVLR→MS:RAND||AUTN

v. MS→HVLR: RES

The correct procedure is shown in Fig1 underneath.

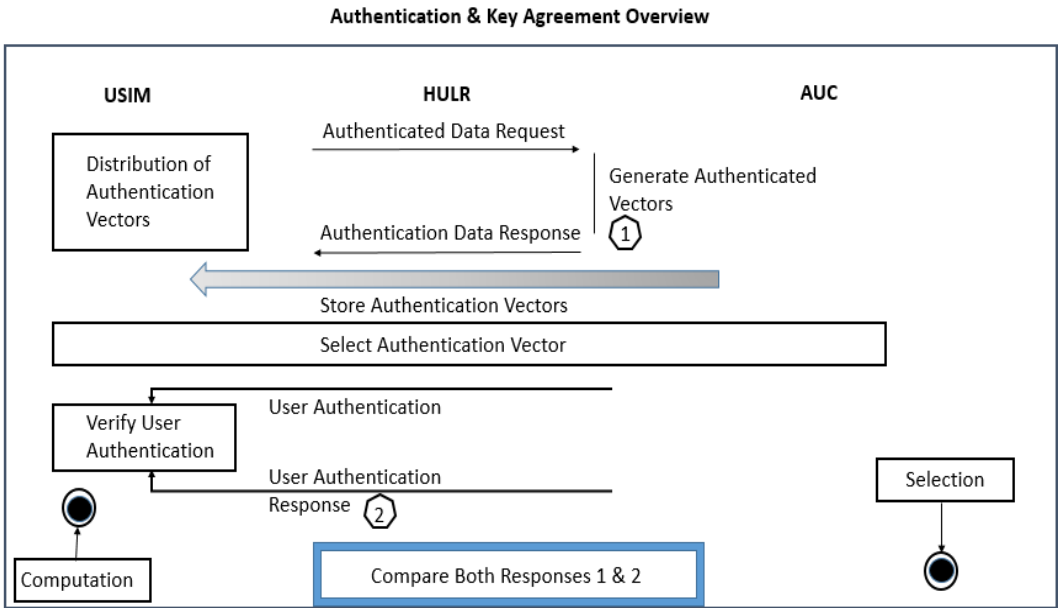

Fig 1: Overview of Authentication and Key Agreement

The fundation of the verification instrument is an ace key or an endorser validation key K, which is shared between the USIM of the client and the home system database, Confirmation Center (AuC).The key is for all time kept mystery and has a length of 128 bits. The key is never exchanged from these two areas (i.e., the client has no learning of the ace key).

Aside from common validation, keys for encryption and trustworthiness checking are additionally determined. These are transitory keys (with a similar length of 128 bits) and are gotten from the perpetual key K amid each confirmation occasion. It is an essential rule in cryptography to keep the utilization of lasting keys to a base and, rather, get brief keys from it for security of mass information.

This procedure is the key some portion of the conception. Validation and key assertion (Fig. 1) comprises of two strategies. To begin with, the HE circulates validation data to the SN. Second, a validation trade is keep running between the client and the SN. The verification data comprises of the parameters important to complete the validation trade and give the concurred keys.

The confirmation technique starts when the client is recognized in the SN. Identification happens when the character of the client (i.e., lasting personality Global Versatile Supporter Personality (AMSII), or brief personality Transitory Portable Endorser Character (TMSI), or Parcel TMSI (P-TMSI), has been transmitted to the HVLR or SGSN.When client ME wanders to the visit organize HVLR and starts the administration ask for, HVLR will send validation demand to the proprietorship arrange HE of the utilization. The AuC contains the ace key of every client. When HE

gets the demand, it creates a requested exhibit of n confirmation vectors in light of the learning of the AMSII.

Every verification vector comprises of five segments (and thus might be known as an UMTS "quintet" in similarity to GSM 'triplets'): an arbitrary number RAND, a normal reaction XRES, a figure key CK, a trustworthiness key IK and a confirmation token AUTN. This variety of n verification vectors is then sent from the HE to the SN. It is useful for n validation trades between the SN and the USIM.HVLR spares these verification vectors. In a confirmation trade the SN first chooses the following (the i-th) validation vector from the exhibit and sends the parameters RAND (i) and AUTN (i) to the client. Verification vectors in a specific hub are utilized on a FIFO premise.

In the SN, one validation vector is required for every verification case (i.e., for each keep running of the confirmation procedure).This implies that the (possibly long separation) motioning amongst SN and AuC is not required for each confirmation occasion and that on a fundamental level this flagging should be possible freely of client activities after introductory enrollment. Surely, the HVLR/SGSN may get new confirmation vectors from AuC well before the quantity of put away vectors runs out.

The client gets the data which HVLR sends, and computes the expected XMAC=f1K (SQN||RAND||AMF), then contrasts it and Macintosh which got, if the outcome is conflicting, then the client will get the report of validation disappointment, and the confirmation procedure is over. At last, HVLR gives an answer to the HE about the disappointment, and restarts a verification procedure. The USIM checks whether AUTN(i) can be acknowledged and, assuming this is the case, delivers a reaction RES(i), which is sent back to the SN.AUTN(i) must be acknowledged if the succession number contained in this token is new.

In the meantime, client starts to deliver CK and IK. After HVLR gets RES, contrasts and memory XRES, if steady, then considers the verification and the key understanding is achievement. The built up keys CK(i) and IK(i) will then be exchanged by the USIM to the versatile hardware and by the HVLR (or SGSN) to the RNC(Radio Arrange Controller); the keys are then utilized by the figuring and honesty works in the MS(Mobile Station) and in the RNC when encryption and trustworthiness security begin.

HVLR/SGSNs can offer secure administration notwithstanding when HE/AuC (Validation Center) connections are inaccessible by permitting them to utilize beforehand inferred figure and respectability keys for a client so that a protected association can in any case be set up without the requirement for a confirmation and key understanding. Confirmation is all things considered in light of a mutual uprightness key, by methods for information respectability security of flagging messages.

3.2. Authentication vector distribution:

Fig 2 demonstrates the producing procedure of confirmation vector. The procedure starts by picking a proper arrangement number (SQN). An uncertainty might be raised

that;, what is required is that SQNs are picked in climbing request. The reason for the SQN is to give the client (or all the more in fact the USIM) with evidence that the created validation vector is new (i.e., it has not been utilized before in a before keep running of confirmation. In parallel with the decision of SQN,a 128-piece long erratic test RAND is created. This is a mental way so that the yield of one capacity uncovers no data about the yields of alternate capacities. For every client the HE/AuC monitors a counter SQNHE.

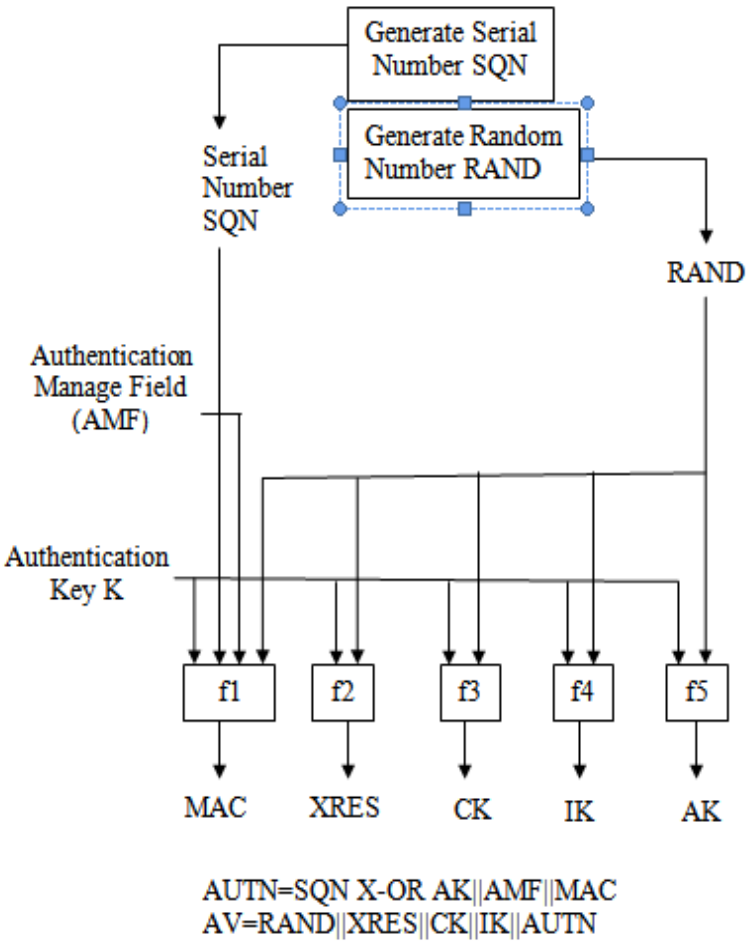

Fig 2: Authentication Vector Generating Process

In the Fig 2, f1 and f2 are the key validation capacities, f3, f4 and f5 are the key creating capacities, every one of them are known calculation to ME and HE. SQN is the succession number spared in ME and the HE, when the transmission distinctive or carries on the hideaway with AK with it. Thusly the accompanying qualities are figured:

- Message Verification Code M where AC=f1K(SQN||RAND||AMF) where f1 is a message confirmation work;
- An eXpected Reaction XRES=f2K(RAND) where f2 is a message verification work;
- A Figure Key CK=f3K(RAND)where f3 is a key creating capacity;
- A Respectability Key IK=f4K(RAND)where f4 is a key creating capacity;
- A Namelessness Key AK=f5K(RAND)where f5 is a key creating capacity.
- At last the verification token AUTN = SQN ⊕ AK || AMF || Macintosh is developed.

Fig 3: Message Verification Procedure

At last the verification token AUTN = SQN ⊕ AK || AMF || Macintosh is developed.

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

AK is a namelessness key used to hide the succession number as the last may uncover the personality and area of the client. The camouflage of the grouping number is to secure against aloof assaults as it were. A verification and key administration field AMF is incorporated into the validation token of every confirmation vector. Illustration employments of AMF include: 1. Support numerous validation calculations and keys (This system is valuable for calamity recuperation purposes

might be utilized to demonstrate the calculation and key used to produce a specific confirmation vector.); 2. Changing succession number check parameters (This instrument is utilized to change powerfully the point of confinement on the contrast between the most astounding SEQ acknowledged up until now and a got arrangement number SEQ.) and 3. Setting edge qualities to confine the lifetime of figure and trustworthiness keys (The USIM contains an instrument to constrain the measure of information that is secured by a get to connection key set. The AMF field might be utilized by the administrator to set or modify this point of confinement in the USIM).

From Fig 3 we can see that aggressor A may envision this customer to enter the framework. Regardless, the encryption scratch (CK) and the integrality scratch (IK) has not transmitted in the remote affiliation, the attacker can't procure these keys to hold up under on the run of the mill security correspondence.

3.2. Authentication and Key Derivation in Theusim:

On receipt of a (RAND, AUTN) combine, the USIM goes about as takes after: To begin with, it recovers the unconcealed SQN. In the event that the SQN is disguised, the USIM registers AK=f5k(RAND) and recovers the SQN by figuring SQN= (SQN X-OR AK) X-OR AK.Then the USIM processes XMAC-A=f1k(SQN||RAND||AMF),the client reaction RES,the CK and the IK.

3.3 Protocol Security Analysis

The fundamental defects of the 4GPP-Otherwise known as conception is depicted as taking after focuses:

i. The changeless status data can be captured effortlessly.
ii. The collateral verification is not complete;
iii. Grouping number is a very difficult task.
iv. Unsecured transmission of verification vector.
v. The encryption calculation is settled, and there is no real way to supplement key understanding securely and adaptably.
vi. The security of the key creating calculation is controlled by calculation.

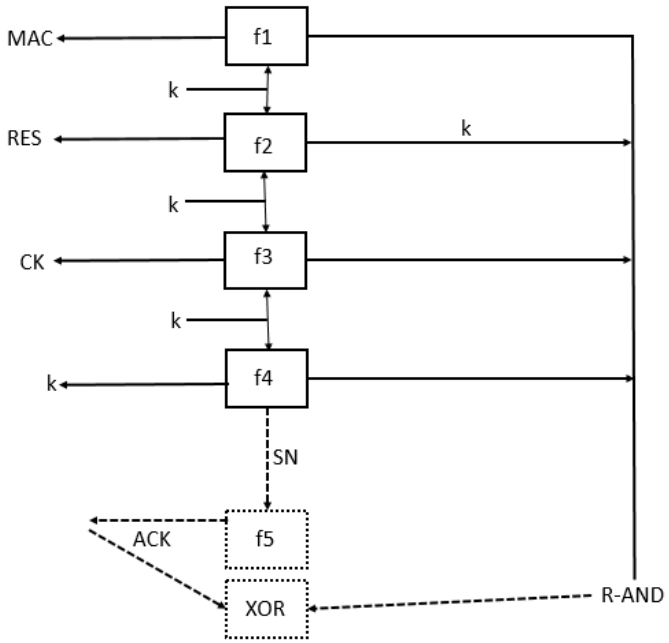

Fig 4: Authentication & Derivation of U(SIM)

3.3 Conceivable Assault: -

As per the investigation of the conception procedure, this confirmation arrange has understood the validation of HVLR to MS and in addition MS to the VHLR, however does not ask for the MS to verify HVLR. What assaults an attacker may bear on by catching approved client distinguishing proof/character are portrayed as taking after:

i. MS→HVLR: AMSII, VHLR

ii. HVLR→VHLR: AMSII

iii. VHLR→HVLR: AV=RAND||XRES||CK||IK||AUTN

iv. HVLR→MS: RAND||AUTN

v. MS→HVLR: RES

Fig 5: Five stages for the procedures of Validation

Consequently, attacker A may imagine lawful client to enter the system. Be that as it may, the encryption scratch CK and the integrality scratch IK has not transmitted in the remote association, the assailant can't acquire these keys to bear on the typical

protection correspondence. Moreover, the above arrangement has not considered the validation and the security correspondence between customers. In the event that the attacker blocks the data amongst HVLR and VHLR, he can get the confirmation vector (AV) transmitting from VHLR to HVLR, hence can acquire encryption key (CK) and integrality key (IK). Thusly, if the assailant again imagines this approved client to enter the system, he can understand the ordinary security correspondence, and the data transmitted by approved client additionally loses mystery.

IV. WEAKNESSES IN SECURITY MECHANISMS OF UNIVERSAL MOBILE TELECOMMUNICATION SYSTEMS

To total up, the principle shortcomings in UMTS security instrument are:

i. Integrity keys utilized amongst UE and RNC created in HVLR/SGSN are transmitted decoded to the RNC (and now and then between RNCs).

ii. IMSI is transmitted in decoded frame.

iii. For a brief timeframe amid flagging methodology, flagging information are unprotected and henceforth presented to altering.

V. IMPROVISATION

As per the investigation of otherwise known as, the conceptional Otherwise known as conception has two security issues, deficient bidirectional verification and dangerous vector transmission. Here, we propose an enhanced Otherwise known as conception, hoping to improve the security of the customary conception.

5.1 THE ASSENTATION CONFIGURATION: - The assentation configuration ought to take after guideline according to the details below. At the point when plan validation conception, there are three key prerequisites:

i. secrecy,

ii. no excess, and

iii. Authentication ID.

So as to satisfy these necessities, along these lines, some outline standards are proposed as taking after:

i. The outline objective ought to be clear, ought not have the vagueness;

ii. The most ideal approach to execute the formalized depiction of the security conception is utilizing formal dialect.

iii. Proving the security conception has accomplished the outline objective through the formalization investigation strategy.

iv. The security has nothing to do with the encryption calculation utilized.

v. We ought to ensure the brief esteem and the discussion key and other essential news be crisp, to keep the replay assault.

vi. Select the nonconcurrent verification strategy beyond what many would consider possible, abstain from utilizing the synchronized validation way.

vii. Has the capacity to oppose normal assault, uniquely the replay assault.

viii. Carry on the hazard examination of the runtime condition, and make the underlying securities supposition as few as could be expected under the circumstances.

ix. Be usable. It can be utilized as a part of various conception layers of various system.

x. Reduce the secret word operation and cost beyond what many would consider possible, and grow connected degree.

5.2 Description of the Improved Protocol

The enhanced validation and key assention construction is appeared in Fig 3. The enhanced validation conception asks for the HVLR and VHLR to share the framework key KH, a similar encryption calculation and a similar integrality affirmation calculation. The conception stream is appeared as taking after:

1) HVLR discovered AMSII as per TMSI, and transmitted the E (K, R)||MAC (K, R) and other data to VHLR.

2) VHLR unscrambled the E (K, R) by the common key amongst VHLR and MS to get the number R, and approved the uprightness of the R.

3) VHLR utilized the determined calculation to create R1-Rn, and utilized the common key amongst VHLR and HVLR to encode R, then acquired E (KH, R1||R2.||Rn), at long last, get the uprightness check code Macintosh (KH, R1||R2. .Rn).

4) VHLR utilizations KH to bear on the encryption of AV vector gathering and creates the respectability check code for this MS,therefore, acquires the E (KH, AV1||AV2.||AVn) and the Macintosh (KH, AV1||AV2.||AVn).

5) VHLR transmit E (KH, AV1||AV2.||AVn), Macintosh (KH, R1||R2.||Rn), E (KH, R1||R2.||Rn) and Macintosh (KH, AV1||AV2.||AVn) to HVLR.

6) HVLR utilizations KH to unscramble AV1-AVn and R1-Rn, and check their respectability.

7) HVLR chooses AVn, and connects the Rn to the answer information transmitted for MS.

8) The client USIM utilizes inferred calculation to deliver R1-Rn,and finds whether there is number among R1 and Rn is equivalent to the number Rn transmitted

from HVLR. On the off chance that yes, then finishes the verification of MS to the HVLR.

From the conception stream, we can see that the enhanced conception requires the HVLR and VHLR to share framework enter KH which utilized as a part of the procedure of MS verifying the recognizable proof of the HVLR and additionally during the time spent approving the data honesty and security amongst HVLR and the VHLR. Also, when MS send the demand data to the HVLR, we include the information E (K, R) into the demand data. The creating procedure of the information E (K, R) is portrayed as taking after as appeared in fig 3:

Firstly, MS delivers an irregular number R and utilize the client key K shared amongst MS and VHLR to scramble it. The encoded R is E (K, R). At that point we ought to figure Macintosh (K, R). At long last, MS send the TMSI, E (K, R) and Macintosh (K, R) to the HVLR.

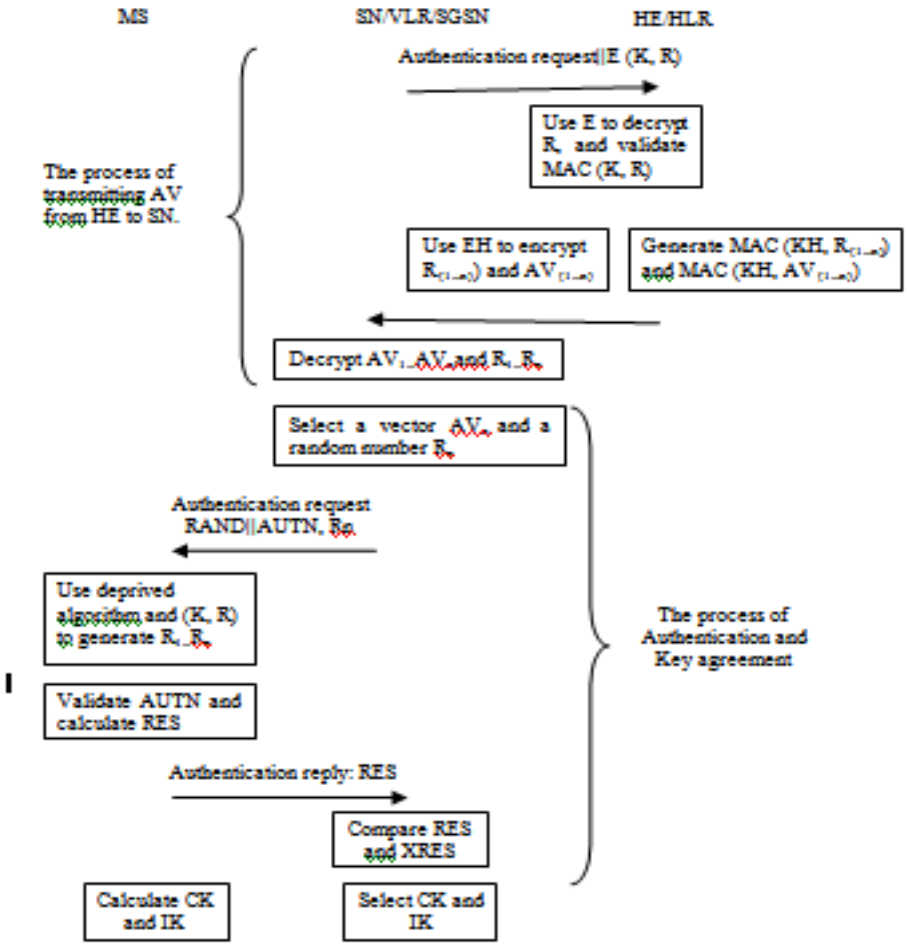

Fig 3: Improvement Authentication Agreement

5.3 Analysis of the Improved Protocol

As indicated by the depiction of the conception in the above area, we may see that the enhanced conception has understood a few defects in customary Otherwise known as conception. The tackled issue is recorded as taking after:

1. The secrecy of data transmitted in the system: In the enhanced conception, we require the HVLR and VHLR to share the framework key KH, a similar encryption calculation and a similar integrality affirmation calculation. In this way, we can ensure classification of data transmitting amongst VHLR and HVLR, and causes the attacker not able to acquire the confirmation vector, along these lines keeps the imagining MSC/HVLR assault.

2. Authentication of MS to HVLR. Since there is no mutual mystery amongst MS and HVLR, along these lines can't understand the immediate confirmation. Be that as it may, we can understand confirmation by implication through the VHLR. The validation of MS to HVLR relies on upon the classification of the irregular number produced by MS. What's more, just the lawful HVLR can unscramble the data E (K, R) transmitted by MS accurately. Consequently, once MS gets the right number R, it can affirm HVLR is lawful.

VI. ADVANTAGES OF AKA PROTOCOL

In conclusion, the major advantages of AKA come out to be / include:

1. Larger authentication keys (128-bit)
2. Stronger hash function (SHA-1)
3. Support for mutual authentication
4. Support for signaling message data integrity
5. Support for signaling information encryption
6. Support for user data encryption

VII. CONCLUSION & FURTHER DEVELOPMENTS IN UMTS SECURITY

Take a shot at the following UMTS discharge has begun. This will present new security highlights. Huge numbers of these components will be acquainted with secure the new administrations which will be presented, e.g. nearness administrations, push administrations and multicast/communicate administrations. Looking more into the future, portable cell frameworks should suit an assortment of various radio get to systems including short-extend remote advances, associated with a typical center system. On the client side the idea of a solid terminal, as we probably am aware it, is dissolving. Appropriated terminal designs are showing up whose segments are interconnected by short-go radio connections. These new advancements speak to a noteworthy test to the UMTS security engineering. A community oriented research extend supported by the European Union and called SHAMAN (Security for

Heterogeneous Access in Versatile Applications and Systems) have handled these issues. A different venture is additionally in progress to recognize inquire about themes in the territory of portable interchanges; this venture is called PAMPAS (Spearheading Propelled Versatile Protection and Security).

Otherwise known as systems in UMTS have expanded security contrasted and GSM All messages ought to be uprightness checked, however by implication by requiring privacy assurance together with honesty. Otherwise known as idea is utilized to perform confirmation of the client and system, instead of 2G frameworks, which just validated clients in a framework. The privacy calculation is more grounded than its GSM forerunner. The respectability instrument works autonomous of secrecy security and gives insurance against dynamic assaults. The outline of cryptographic calculations is open and they are broadly crypto broke down. Also, the design is adaptable and more calculations can be included effortlessly. In perspective of the defect existed in customary Otherwise known as conception, we have composed an enhanced Otherwise known as conception. The enhanced conception has acknowledged MS to the HVLR validation and the classification of data transmitted in system, and improved the security of data transmitted in the remote channel.

REFERENCES

[1] IEEE XPLORE “Education Technology and Computer Science, 2009. ETCS '09. First International Workshop on, 7-8 March 2009, Wuhan, Hubei.

[2] Engr.Mujtaba Hassan, Engr.Munaza Razzaq and Engr.Asim Shahzad,”Comprehensive Analysis of UMTS Authentication and Key Agreement” in International Journal of Computer and Network Security, Vol. 2, No.2, February 2010.

[3] K. Boman, G. Horn, P. Howard, and V. Niemi,”Umts Security”, October 2003

[4] Valtteri Niemi and Kaisa Nyberg,”UMTS Security”, 2003.

[5] STEPHEN NORTHCUTT, JUDY NOVAK, Network Intrusion Detection

[6] CURRY, D., AND DEBAR, H. Intrusion Detection Message Exchange Format data model and Extensible Markup Language (XML) Document Type Definition

[7] W. R. CHESWICK, S. M. BELLOVIN , “Firewalls and Internet Security : Repelling the wily hacker “

[8] ”SunSHIELD Basic Security Module Guide” Sun MicroSystems Inc.

[9] Loris Degioanni, Fulvio Eisso, and Piero Viano, "Windump". http://netgroup- serv.polito.it/windump, erald Combs et al. "Ethereal". Available at http://www.ethereal.eom.

[10] "Etherpeek nx". http://www.wildpaekets.eom.

[11] "Gaim:A multi-protocol instant messaging (im) client", "http: //gaim.sourceforge.net/".

[12] Van Jacobson, Craig Leres, and Steven MeCanne, "tepdump : A Network Monitoring and Packet Capturing Tool". Available via anonymous FTP from ftp://ftp.ee.lbl.gov and www.tcpdump.org.

[13] Neeraj Kapoor. "Design and Implementation of a Network Monitoring Tool". Technical report, Department of Computer Science & Engineering, IIT Kanpur, Apr 2001. http://www.cse.iitk.ac.in/research/mtech2000 /Y011111.html.

[14] Steve MeCanne and Van Jacobson. "The BSD Packet Filter: A New Architecture for User-level Packet Capture". In *Proceedings of USENIX Winter Conference*, pages 259-269, San Diego, California, Jan 1993.