Security Evaluation of CDMA2000

L. Ertaul[1], S. Natte[2], and G. Saldamli[3]
[1]Mathematics and Computer Science, CSU East Bay, Hayward, CA, USA
[2] Mathematics and Computer Science, CSU East Bay, Hayward, CA, USA
[3]MIS, Bogazici, Istanbul, Turkey

Abstract - *In cellular industry, security has been a major concern for both service providers and subscribers. Service providers are primarily concerned with security to prevent fraudulent operations such as cloning or subscription fraud, while subscribers are mainly concerned with privacy issues. This paper gives a description of the access security mechanism found in CDMA2000 technology and discusses how CDMA2000 solves the three major features of mobile security: authentication, data protection, and anonymity.*

Keywords: Access security, Security, Security in CDMA2000, Wireless Security.

1 Introduction

CDMA2000 is a technology for the evolution of cdmaOne/IS-95 to 3rd generation services (3G). CDMA2000 will provide enhanced services to cdmaOne subscribers, as is backward compatible as well. Unlike other 3G standards, it is an evolution of an existing wireless standard. CDMA2000 supports 3G services as defined by the International Telecommunications Union (ITU) for IMT-2000 [1]. 3G networks will deliver wireless services with better performance, greater cost-effectiveness and significantly more content. One of the other 3G architectures that CDMA2000 competes with is the UMTS architecture [2] specified by 3G Partnership Project (3GPP). CDMA2000 and UMTS share lots of common features including a common basis for authentication and key distribution. The goal of this paper is to present the access security architecture in CDMA2000.

2 Objectives for CDMA2000 Security

CDMA2000 [1] has evolved from the older 2G-cdmaOne architecture. The changes were motivated by

- Extensive cryptanalysis of algorithms used in 2G systems.
- 64-bit keys used in 2G systems are found to be too short for strong encryption.
- There are new requirements like the need for mutual authentication.

The requirements for CDMA2000 security [3] were first laid out by TIA (Telecommunications Industry Association) and could be summarized as follows.

- CDMA2000 security will build on the security of the second-generation systems. This feature basically ensures that the existing infrastructure can still be used.
- CDMA2000 security will improve on the security of 2G systems. CDMA2000 will tackle the weaknesses in 2G systems and counteract attacks like denial of service attack, impersonation of network, impersonation of user attacks.
- CDMA security will offer new security features, like security within and between networks

3 CDMA2000 Security Architecture

There are four entities participating in the CDMA2000 security architecture. These are:

1). The *home networ*k, in particular the home location register and authentication center (HLR/AC).

2). The *serving networ*k (SN), in particular the visited location register and the Mobile station controller/packet data serving node (VLR and MSC/PDSN).

3). The mobile station (MS, the phone handset).

4). The user identity module (UIM). The UIM may or may not be removable from the handset; if it is removable (like the UMTS USIM) it is referred to as the R-UIM. In either case it is designed to be tamper resistant and capable of a reasonable level of protection for key material.

The primary user identity is the International Mobile Subscriber Identity (IMSI) number. Before the user identity can be authenticated, the user should first present the identity. And since session keys used for encryption are produced after the authentication procedure, we have a situation where the permanent identity IMSI will be visible on the over-the-air interface. This is undesirable since it allows for subscriber location tracking.

To alleviate this problem the serving network may issue a local temporary identity called the TMSI to be used for subsequent identification. The user equipment (UE) first presents itself with its IMSI the first time it enters a new service area or visited location register (VLR). Then, after encryption has commenced, the SN issues a TMSI number to the UE. The TMSI is issued in encrypted form. It is therefore hard to track a particular subscriber since there is no apparent relationship between the IMSI and the TMSI. The use of the TMSI thus provides a measure of identity/location confidentiality or user anonymity.

Here is the list of abbreviations that are used frequently in describing the CDMA2000 security architecture.

AuC	Authentication Center
AK	Anonymity Key
AKA	Authentication and key agreement
AMF	Authentication management field
AUTN	Authentication Token
AV	Authentication Vector
CK	Cipher Key
HE	Home Environment
HLR	Home Location Register
IK	Integrity Key
IMSI	International Mobile Subscriber Identity
TMSI	Temporary IMSI.
MAC	The message authentication code
MS	Mobile Station
RAND	Random challenge
SQN	Sequence number
SQN_{HE}	Individual sequence number for each user maintained in the HLR/AuC
SQN_{MS}	The highest sequence number the UIM has accepted
SGSN	Serving GPRS Support Node
SN	Serving Network
TMSI	Temporary Mobile Subscriber Identity
UE	User Equipment.
UIM	User Identity Module
UMTS	Universal Mobile Telecomm. Systems
UAK	UIM Authentication Key
VLR	Visitor Location Register
XRES	Expected Response

3.1 Authentication and Key Agreement

The important requirement of the security architecture is feeding the initial subscriber authentication key K into the UIM and AuC. Once the subscriber key exists, it can be used in an authenticated key agreement protocol to generate session keys and establish a secure connection between the user equipment and the serving network. There are two approaches to provide the Subscriber key K. In the first approach, the customer or salesperson would put in a special code of 26 digits provided by the home service provider. In the second approach the customer or a salesperson calls a special phone number, and while on the call a Diffie-Hellman key establishment algorithm is performed between the UIM and AC. This approach is also called as over-the-air service provisioning (OTASP) [4, 5].

The authentication and key agreement (AKA) [2] protocol used in CDMA2000 is very similar to the one used in UMTS. CDMA2000 added an optional extension that involves UIM authentication key and a function called UMAC [6].

The AKA achieves mutual authentication by the user and the network. They both share the knowledge of a secret key K which is available only to the USIM and the AuC in the user's HE. In addition the USIM and the HE keep track of counters SQN_{MS} and SQN_{HE} respectively to support network authentication. The sequence number SQN_{HE} is an individual counter for each user and the sequence number SQN_{MS} denotes the highest sequence number the USIM has accepted.

The AKA is executed in two stages [2]. The first stage involves transfer of security credentials (authentication vector, AV) from home environment (HE) to the serving network (SN). The second stage involves one-pass challenge-response procedure to achieve mutual entity authentication between the USIM and the network. An overview of the AKA procedure is shown in Figure 1.

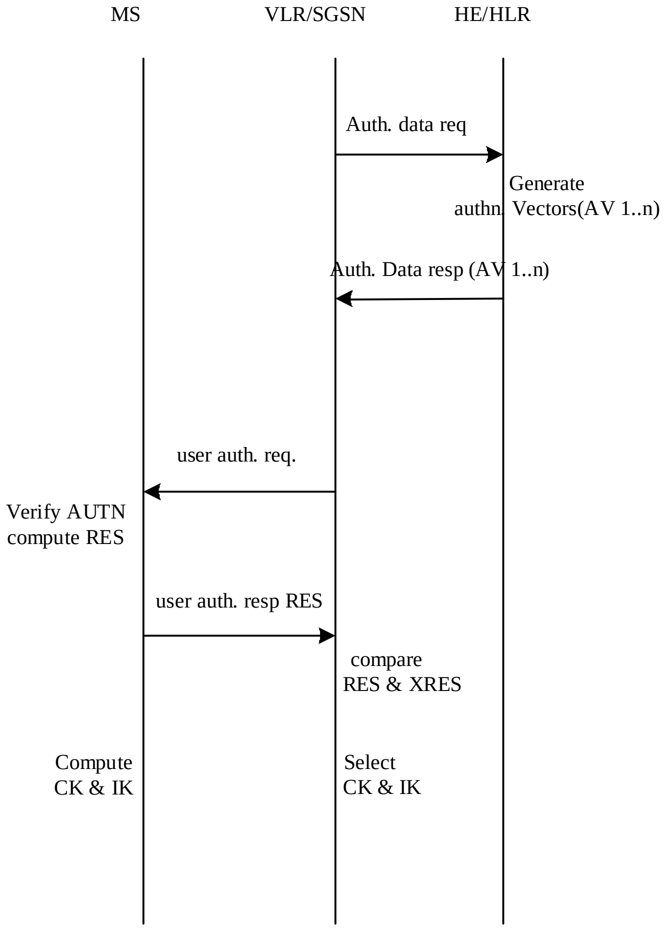

Figure 1: An overview of the AKA procedure

The authenticating parties shall be the AuC of the user's HE (HE/AuC) and the USIM in the user's mobile station. The mechanism consists of the following procedures.

Upon receipt of a request from the VLR/SGSN, the HE/AuC sends an ordered array of *n* authentication vectors to the VLR/SGSN. The authentication vectors are ordered based on sequence number. Each authentication vector (AV) consists of the following five components: a random number RAND, an expected response XRES, a cipher key CK, an integrity key IK and an authentication token AUTN. Each authentication vector is good for one authentication and key agreement between the network's VLR/SGSN and the user mobile's USIM.

When the VLR/SGSN initiates an authentication and key agreement, it selects the next authentication vector from the ordered array and sends the parameters RAND and AUTN to the user. Authentication vectors in a particular node are used on a first in / first-out basis. The USIM checks whether AUTN can be accepted and, if so, produces a response RES that is sent back to the VLR/SGSN. The USIM also computes CK and IK. The VLR/SGSN compares the received RES with XRES.

If the RES and the XRES match the VLR/SGSN considers the authentication and key agreement exchange to be successfully completed. The established keys CK and IK will then be transferred by the USIM and the VLR/SGSN to the entities that perform the ciphering and the integrity functions.

The mechanism for authentication and key agreement requires the following cryptographic functions [7]:

f0 the random challenge generating function;

f1 the network authentication function;

f1* the e-synchronization message authentication function;

f2 the user authentication function;

f3 the cipher key derivation function;

f4 the integrity key derivation function;

f5 the anonymity key derivation function.

f5* the anonymity key derivation function for the e-synchronization message.

For each of the algorithms f1 to f5* there is a general requirement that it shall be computationally infeasible to derive K from knowledge of input(s) and output. 3GPP provides an example set of AKA algorithms called MILENAGE [8] that specifies the above functions.

3.2 Generating Authentication Vectors

When the VLR/SGSN requests for the authentication data the HE may retrieve the pre-computed number of authentication vectors from the HLR database or may compute them on demand.

Figure 2 shows the generation of an authentication vector AV by the HE/AuC. The HE/AuC starts with generating a fresh sequence number SQN and an unpredictable challenge RAND [9]. For each user the HE/AuC keeps track of a counter: $SQN_{HE.}$

The various entries in AV are computed as follows.

- A message authentication code MAC = $f1_K$ (SQN || RAND || AMF) where f1 is a message authentication function;

- An expected response XRES = $f2_K$ (RAND) where f2 is a (possibly truncated) message authentication function;

- A cipher key $CK = f3_K$ (RAND) where f3 is a key generating function;

- An integrity key $IK = f4_K$ (RAND) where f4 is a key generating function;

- An anonymity key $AK = f5_K$ (RAND) where f5 is a key generating function or f5 = 0.

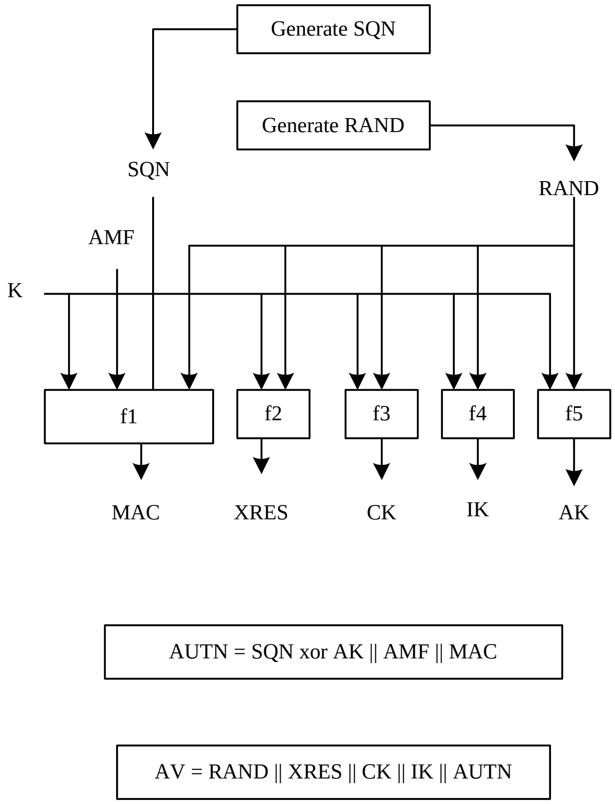
Generate SQN
Generate RAND
SQN
RAND
AMF
K
f1
f2
f3
f4
f5
MAC
XRES
CK
IK
AK
AUTN = SQN xor AK || AMF || MAC
AV = RAND || XRES || CK || IK || AUTN

Figure 2: AV generation function in the AuC.

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

Here, 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. If no concealment is needed then f5 = 0 (AK = 0).

3.3 Challenge - Response

The purpose of this procedure is to authenticate the user and establish a new pair of cipher and integrity keys between the VLR/SGSN and the USIM [9]. During the authentication, the USIM verifies the freshness of the authentication vector that is used.

The VLR/SGSN sends to the USIM the random challenge RAND and an authentication token for network authentication AUTN from the selected authentication vector. Upon receipt the user proceeds as shown in Fig. 3.

Upon receipt of RAND and AUTN the USIM first computes the anonymity key $AK = f5_K$ (RAND) and retrieves the sequence number SQN = (SQN ⊕ AK) ⊕ AK. Next the USIM computes $XMAC = f1_K$ (SQN || RAND || AMF) and compares this with MAC which is included in AUTN. If they are different, the user sends *user authentication reject* back to the VLR/SGSN with an indication of the cause and the user abandons the procedure.

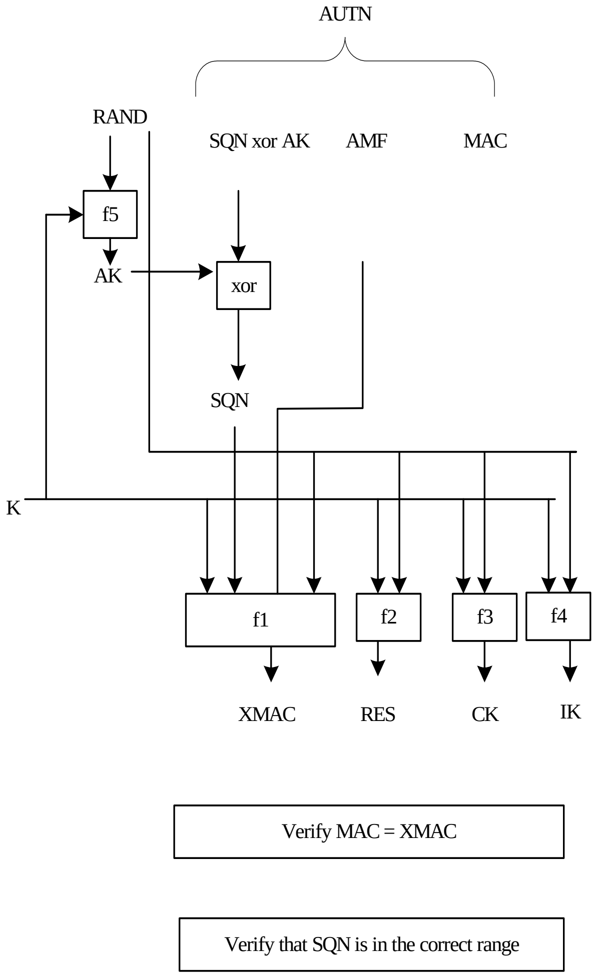

Figure 3: User authentication function in the USIM

Next the USIM verifies that the received sequence number SQN is in the correct range. If the USIM considers the sequence number to be not in the correct range, it sends *synchronization failure* back to the VLR/SGSN including an appropriate parameter, and abandons the procedure.

If the sequence number is considered to be in the correct range however, the USIM computes $RES = f2_K$ (RAND) and includes this parameter in a *user authentication response* back to the VLR/SGSN.

Finally the USIM computes the cipher key CK = $f3_K$ (RAND) and the integrity key IK = $f4_K$ (RAND). CK and IK keys are sent to the MS. USIM shall store original CK, IK until the next successful execution of AKA.

Upon receipt of *user authentication response* the VLR/SGSN compares RES with the expected response XRES from the selected authentication vector. If XRES equals RES then the authentication of the user has passed. The VLR/SGSN also selects the appropriate cipher key CK and integrity key IK from the selected authentication vector. If XRES and RES are different, VLR/SGSN shall initiate an Authentication Failure Report procedure towards the HLR. VLR/SGSN may also decide to initiate a new identification and authentication procedure towards the user.

3.4 Confidentiality and Integrity Protection

Confidentiality protection: Confidentiality protection is applied to all user and signaling data. The CK is always 128 bits long, although its actual strength can be artificially reduced.

Figure 4 illustrates the use of the ciphering algorithm f8 to encrypt plaintext by applying a keystream using a bit per bit binary addition of the plaintext and the keystream. The plaintext may be recovered by generating the same keystream using the same input parameters and applying a bit per bit binary addition with the cipher-text.

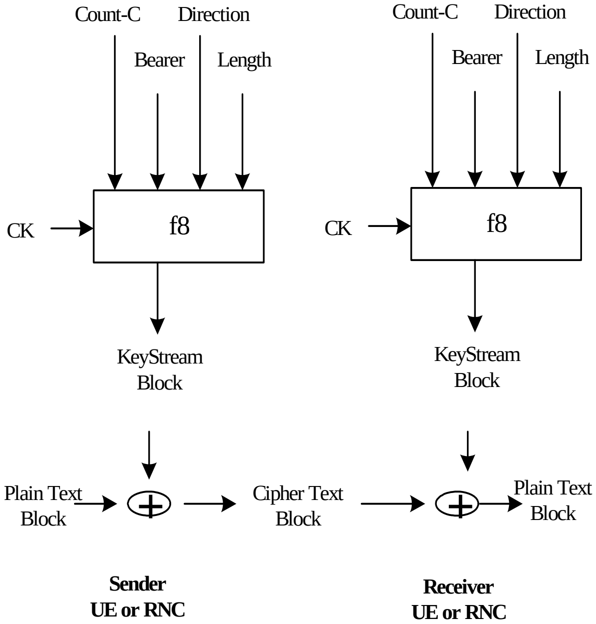

Figure 4: Ciphering of user and signaling data transmitted over the radio access link

The input parameters to the algorithm are

a) CK : the Cipher Key

b) COUNT-C: the cipher sequence number.
COUNT-C is composed of two parts: the physical layer frame number and the hyperframe sequence number. The exact structure of the COUNT-C is specified in [10]. The user equipment at connection set-up sends the initial value of the hyper frame number to the network. The user equipment stores the greatest used hyper frame number from the previous connection and increments it by one to select it for the current connection. This synchronizes the COUNT-C value at both ends.

c) BEARER: the radio bearer identifier.
The same cipher key may be used for different radio bearers simultaneously associated with a single user, which are multiplexed onto a single 10ms physical layer frame. To avoid using the same keystream to encrypt more than one bearer, the algorithm shall generate the keystream based on the identity of the radio bearer.

d) DIRECTION: the direction of transmission of the bearer to be encrypted.
The same cipher key may be used for uplink and downlink channels simultaneously associated with a UE, which are multiplexed onto a single 10ms physical layer frame. To avoid using the same keystream to encrypt both uplink and downlink transmissions, the algorithm shall generate the keystream based on the direction of transmission. The value of the DIRECTION is 0 for messages from UE to RNC and 1 for messages from RNC to UE.

e) LENGTH: the required length of keystream.
For a given bearer and transmission direction the length of the plaintext block that is transmitted during a single physical layer frame may vary. The algorithm shall generate a keystream block of variable length based on the value of the length parameter. The input parameter LENGTH shall affect only the length of the KEYSTREAM BLOCK, not the actual bits in it. Based on these input parameters the algorithm generates the output keystream block KEYSTREAM that is used to encrypt the input plaintext block PLAINTEXT to produce the output cipher text block CIPHERTEXT. These same input parameters are used to generate the output keystream block KEYSTREAM that is used to decrypt the input cipher text block CIPHERTEXT to produce the output plain text block PLAINTEXT.

Integrity Protection: Most control signaling information elements that are sent between the MS and the network are considered sensitive and are integrity protected. A message authentication function is applied to these signaling information elements transmitted between the MS and the network.

Figure 5 illustrates the use of the integrity algorithm f9 to authenticate the data integrity of a signaling message.

The input parameters to the algorithm are

a) IK: the integrity key

b) COUNT-I: a frame dependent input.

The input parameter COUNT-I protects against replay during a connection. It is a value incremented by one for each integrity-protected message. COUNT-I consists of two parts: the HYPERFRAME NUMBER (HFN) as the most significant part and a RRC Sequence Number as the least significant part. The COUNT-I value is synchronized along with the COUNT-C value as described above. In this way the user is assured that no COUNT-I value is re-used (by the network) with the same integrity key.

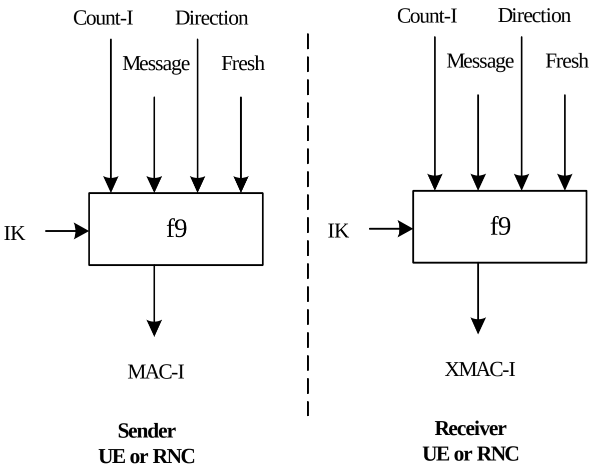

Figure 5: Derivation of MAC-I (or XMAC-I) on a signalling message

c) FRESH: a random number generated by the RNC.

The same integrity key may be used for several consecutive connections. This FRESH value is an input to the algorithm in order to assure the network side that the user is not replaying old MAC-Is.

d) MESSAGE: the signaling data.

e) DIRECTION: the direction of transmission of signaling messages (user to network or network to users).The same integrity key may be used for uplink and downlink channels simultaneously associated with a UE.The value of the DIRECTION is 0 for messages from UE to RNC and 1 for messages from RNC to UE. Based on these input parameters the user computes message authentication code for data integrity MAC-I using the integrity algorithm f9. The MAC-I is then appended to the message when sent over the radio access link. The receiver computes XMAC-I on the message received in the same way as the sender computed MAC-I on the message sent and verifies the data integrity of the message by comparing it to the received MAC-I. If it is a required that the user needs to be authenticated for some billable service, the messages MAC can be further authenticated using the UAK key [6]. Use of UAK is optional. If the home system delivers, and the serving system is prepared to receive, a UAK as part of the AV, the handset must deliver a UMAC on the agreed data packets, not simply the normal MAC. The UMAC procedure relies on UAK, and can only be computed in the UIM.

3.5 Core Cryptographic algorithms

The Diffie-Hellman algorithm [11] is used for the over-the-air service provisioning (OTASP) in CDMA2000 security architecture.

The algorithm used for calculating the MAC for a data packet for Integrity Protection in CDMA2000 is the EHMAC [12]. It is a more efficient and secure variant of HMAC-SHA-1. HMAC is the internet standard for message authentication. HMAC is efficient for long messages, however, for short messages the nested constructions results in a significant inefficiency. For example to MAC a message shorter than a block, HMAC requires at least two calls to the compression function rather than one. This inefficiency may be particularly high for some applications, like message authentication of signaling messages, where the individual messages may all fit within one or two blocks. EHMAC is an enhancement that allows both short and long messages to be message authenticated more efficiently than HMAC. In particular, for a message smaller than a block EHMAC only requires one call to the compression function. In this algorithm, there are two cases differentiated based on the length of the input packet to be authenticated:

- If the input is less than 511 bits in length, a single outer compression function is performed on the input, padded with a single 1 bit and at least one 0 bit.

- If the input is 511 bits or more in length, an inner hash (in the same sense as HMAC) is calculated on all but the last 351 bits of the message. Then an outer compression function is performed on the 160-bit result of the inner hash, the remaining 351 input bits, and a single 1 bit.

The Advanced Encryption Standard (AES) (also known as Rijndael) [13] is the encryption algorithm used in CDMA2000. It is a block cipher encrypting 128-bit blocks under the control of a 128-bit key. CDMA2000 uses ESP_AES mode of AES, essentially a straightforward counter mode as specified in [14].

4 Conclusions

The security mechanisms in CDMA2000 are a major improvement over the 2G mechanisms. It provides a very efficient one-pass challenge-response mechanism that provides mutual authentication of both the User and the Network thus eliminating the false base stations attacks. The confidentiality algorithm used in CDMA2000 is much stronger than the one in 2G and is also better than the one used in the other 3G architecture UMTS. 2G algorithms use only 64-bit key and UMTS uses 128-bit key but uses only a 64-bit input block, where as CDMA2000 uses both 128-bit key and 128-bit input block. While CDMA2000 uses the same AKA mechanisms as in UMTS it actually builds additional features on top of it like the f11 function to ensure that the USIM is present and is an authenticated one. Unlike UMTS, CDMA2000 requires that the AKA functions are standardized so that they are of high quality and not left to individual operators to design. So CDMA2000 is far superior to that of its predecessors and better than most of its peer in recent times. It is developed by a public partnership project and is open for analysis and can consequently become a much more superior technology. Security is the fundamental and most import requirement of any communication medium and wireless communication media has long suffered because of poor security mechanisms. CDMA2000 is a great innovation that is going to change this perception about wireless networks and appease the general public to accept the wireless technology whole-heartedly into their lives.

5 References

[1] 3GPP2 C.S0002-C, "Physical Layer Standard for cdma2000 Spread Spectrum Systems," Rel. C v1.0, May 2002.

[2] IEEE Wireless Communications, "An introduction to access security in UMTS", February 2004

[3] 3GPP TS 33.105, "Cryptographic Algorithm requirements," v. 6.0, June. 2004.

[4] 3GPP2 N.S0011, OTASP and OTAPA v1.0, Jan. 1999.

[5] 3GPP2 C.S0016-B, "Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Standards," v. 1.0, Oct. 2002.

[6] IEEE Wireless Communications, "Access security in CDMA2000,

[7] 3GPP2 S.R0032, "Enhanced Subscriber Authentication and Enhanced Subscriber Privacy," v. 1.0, Dec. 2000.

[8] 3GPP TS 35.206, "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*," Doc. 2: Algorithm Specification.

[9] S. Patel, Z. Ramzan, and G. Sundaram, *Efficient Pseudo-do-Random Generators Based on Collision Intractable Hash Function*s, 1998.

[10] 3G TS 33.102, 3rd generation partnership project; Technical specification group services and system aspects; 3G Security; Security architecture; September 2004.

[11] W.Diffie and M.E.Hellman, "New directions in cryptography," IEEE Trans. Inform. Theory, IT-22, 6, 1976, pp.644-654.

[12] S. Patel, "An Efficient MAC for Short Messages," *Sel.Areas in Cryptography 200*2, Springer Verlag, 2002

[13] National Institute of Standards and Technology (NIST) FIPS-197, Advanced Encryption Standard (AES) (FIPS PUB 197), Nov. 26, 2001.

[14] 3GPP2 S.S0078,"Common Security Algorithms," v. 1.0, Dec. 2002.