Secure Message System for Mobile Communication Using A5/1 Algorithm

Kone Mar Yi, Tin Zar Zar
Computer University (Dawei)
kmyaei2010@gmail.com

Abstract

The messaging system has become the most popular for mobile communication in the world. This paper is intended to implement secure messaging system for mobile communication. To encrypt / decrypt the message between the Mobile Station (MS) and the Base Transceiver Station (BTS), this system applies A5/1 algorithm. This system can be divided into two parts, uplink communication (MS to BTS) and downlink communication (BTS to MS).In this paper, two personal computers are used for BTS and other two personal computers are used for MS instead of real Mobile Station (MS).This system generates keystream before encryption and decryption process .It produces a unique (different) keystream for every frame throughout the call. Therefore this system can support data confidentiality and provide computationally fast and efficient through the use of the symmetric encryption.

1. Introduction

Nowadays, the messaging systems for mobile communication reached a global scale. Since the digital mobile communication systems are the infrastructure of the future Personal Communication Services (PCS), the security is essential [2]. The cipher key is used as the key to the A5/1 algorithm for subsequent encryption of data between the Mobile Station (MS) and the Base Transceiver (BTS). The Subscriber Identity Module (SIM) generates this cipher key using A5/1 algorithm. The same cipher key is used for the entire session of communication. Each frame in the over-the-air traffic is encrypted with a different key stream because one of the basic requirements for secure cryptographic algorithms is that, the security of the crypto system lies solely on the key [5]. This key stream is generated with the A5/1 algorithm. The A5/1 algorithm is designed to prevent traffic analysis attack for user data confidentiality. The messaging system process is to provide confidentiality of user data because of using the different keystream.

2. Symmetric Algorithms

Symmetric algorithms are algorithms in which the encryption and decryption use the same key [7]. Other terms for symmetric-key encryption are secret-key, single-key, shared-key, one-key, and private-key encryption. If the plaintext is denoted by the variable P, the ciphertext by C, the encryption with key x by the function $E_x( )$, and the decryption with key x by $D_x( )$, then the symmetric algorithms are functionally described as follows.

$C=E_x(P)$

$P=D_x(C)$

$P=D_x(E_x(P))$

The key advantage of symmetric encryption is that it is computationally fast and efficient. This make symmetric encryption the ideal choice for mobile devices. A5/1 algorithm used in mobile communication is symmetric encryption algorithmes. This algorithm can be further divided into two categories, block algorithms or block ciphers and stream algorithms or stream ciphers.

2.1 Block Cipher

Block ciphers take a number of bytes as a single unit. Block ciphers encrypt or decrypt data in blocks or groups of bits. A block cipher encryption algorithm might take (for example) a 128-bit block of plaintext as input, and output a corresponding 128-bit block of ciphertext. The exact transformation is controlled using a second input — the secret key. Decryption is similar: the decryption algorithm takes, in this example, a 128-bit block of ciphertext together with the secret key, and yields the original 128-bit block of plaintext.

2.2 Stream Ciphers

Stream ciphers operate on a bit-by-bit basis, producing a single encrypted bit for a single plaintext bit. Stream ciphers are commonly implemented as the exclusive-or (XOR) of the data stream with the keystream. The security of a stream cipher is determined by the properties of the keystream. Linear Feedback Shift Registers (LFSRs) are a key component of many stream ciphers.

2.2.1 Linear feedback shift register

The linear feedback shift register, most often used in hardware designs, is the basis of the stream ciphers. A string of bits is stored in a string of memory cells, and a clock pulse can advance the bits one space in that string. The XOR of certain positions in the string is used to produce the new bit in the string for each clock pulse. It is possible to choose the positions in the string to XOR so that, as long as the memory cells are not initially loaded with all zero bits. LFSRs are implemented as a shift register where the vacant bit created by the shifting is a function of the previous states. With the correct choice of feedback taps, LFSRs can function as pseudorandom number generators. LFSRs have the additional advantage of being easily implemented in hardware. The maximal length sequence (or m-sequence) is equal to 2^n-1 where n is the degree of the shift register.

3. Background Theory

3.1 A5/1 algorithm

The A5/1 algorithm is the most widely used algorithm for mobile communication system. The A5/1 algorithm uses the session key K_c and the frame number to generate keystream for encryption and decryption .The length of the session key K_c and the frame number are 64 bits and 22 bits. This algorithm uses three Linear Feedback Shift Registers (LFSRs) of different lengths, 19, 22 and 23 bits in Figure 1.Therefore, the maximal length of these LFSRs are 2^{19} -1, 2^{22} - 1, and 2^{23} -1, respectively. The combination length of the three LFSRs is 64 bits. The taps of LFSR 1 are at bit positions 13, 16, 17, 18; the taps of LFSR2 are at bit positions 20, 21; and the taps of LFSR3 are at bit positions 7, 20, 21, 22 as shown in Figure 1. Initially, the registers are set to 0. These registers are then loaded with the session key K_c and the frame number.

The 64 bits K_c is first loaded into the register bit by bit [3]. The least significant bit (LSB) of the key is XORed with the least significant bit of each LFSRs and the result is stored into the least significant bit of each register. According to the schemes: in 64 cycles 0<= i<= 64; R [0] =R [0] ^ K[i] .When a register is clocked, its taps are XORed together, and the result is stored in the least significant of the register. The registers are all clocked (the majority clocking rule is disabled).

The 22 bit frame number is also loaded into the register in the same way except that the majority clocking rule applies from now on. All three registers are clocked, based on the majority clocking rule as shown in Table 1. If the middle bits of the three registers are 1, 1 and 0, the first two registers are clock or if the middle bits are 0, 1 and 0, then the first and third register are clocked. Thus at least two registers are clocked on every round [1]. The outputs of the three registers are XORed together and XOR represents one keystream bit. The three registers are clocked for 100 additional clock cycles with the stop/go clock control but without producing any outputs and the generate keystream bits are discarded [4]. This is done to mix the frame number and keying material together. The 114 bits are used as the keystream for uplink (MS to BTS) communication in the full- duplex mode and the next 100 bits are again discarded .Then the next 114 bits are again used for downlink (BTS to MS) communication. The abandoned bits are used to hide the relation between MS (uplink) keystream to BTS (downlink) keystream.

The three registers are at each step either two or three registers are clocked, and that each register moves with probability 3/4 and stops with probability 1/4. A5/1 can accept at least 228 bits of the input message frame. The input message 228 bits is divided into two 114 bits. The first 114 keystream bits and 114 bits of the input message frame are XORed to encrypt from Mobile Station (MS) to Base Transceiver Station (BTS). The next 114 keystream bits are XORed to encrypt the frame from Base Transceiver Station (BTS) to Mobile Station (MS). After this, the A5/1 algorithm is initialized again with the key and the number of the next frame. Once the frame has been received by the BTS, it decrypts them and sends them in plaintext to the operator's backbone network [6].

3.2 LFSR Polynomial and Majority Function

1. LFSR 1: $f_1(x) = x^{18} + x^{17} + x^{16} + x^{13} + 1$ generates a={a(f)}.
2. LFSR 2: $f_2(x) = x^{21} + x^{20} + 1$ generates b = {b (t)}.
3. LFSR 3: $f_3(x) = x^{22} + x^{21} + x^{20} + x^{7} + 1$ generates c = {c (t)}.
4. Tap positions: $d_1 = 10$, $d_2 = 11$ and $d_3 = 12$.

Majority function $f(x_1, x_2, x_3) = (y_1, y_2, y_3)$ is defined by

Table 1. Majority Function

f (a(t+11),b(t+12), c(t+13))=(y_1,y_2,y_3)	a (t+11) b(t+12) c(t+13)
(1,1,1)	0 0 0 1 1 1
(1,1,0)	0 0 1 1 1 0
(0,1,1)	0 1 1 1 0 0
(1,0,1)	1 0 1 0 1 0

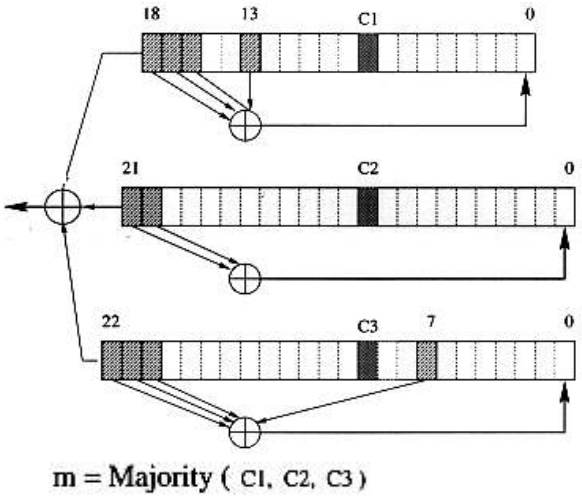

Figure 1. A5/1 stream cipher

4. Mobile Architecture

The main component groups of mobile architecture are [4]:

1. Mobile Stations (MSs)
2. Base Station System (BSS)
3. Network and Switching Subsystem (NSS)

4.1 Mobile Station (MS)

The Mobile Station (MS) consists of two operational parts.

1. Mobile Equipment (ME)
2. Subscriber Identity Module (SIM)

4.1.1 Mobile Equipment (ME)

It is uniquely identified by the International Mobile Equipment Identity (IMEI), which can be obtained by the network upon request. It is a number, usually unique, to identify_GSM, WCDMA, and IDEN mobile phones, as well as some satellite phones The IMEI number is used by the mobile network to identify valid devices.

4.1.2 Subscriber Identity Module (SIM)

The SIM card contains the International Mobile Subscriber Identity (IMSI) used to identify the subscriber to the system, a secret key for authentication, and other information. The SIM card may be protected against unauthorized use by a password or personal identity number. Without the SIM card calls to and from the mobile station is not allowed. The SIM is implemented as a smart card that can exist in two form; large or small.

4.2 Base Station System (BSS)

BSS is central equipment, which is located at the cell site. It provides the link between MS and NSS. The Base Station Subsystem is composed of two parts.

1. Base Transceiver Station (BTS)
2. Base Station Controller (BSC)

4.2.1 Base Transceiver Station (BTS)

The Base Transceiver Station houses the radio transceivers that define a cell and handles the radio-link protocols with the Mobile Station. BTS communicates with the MS. A single BTS can support one or more cells.

4.2.2 Base Station Controller (BSC)

All switching functions, which are performed in MSC, are controlled by BSC. The Base Station Controller manages the radio resources for one or more BTSs. The BSC is the connection between the mobile station and the Mobile service Switching Center (MSC).

4.3 Network Switching Subsystem (NSS)

It is the main switching center of mobile network. NSS includes the following:

1. Mobile Switching Center (MSC)
2. Home Location Register (HLR)
3. Visitor Location Register (VLR)
4. Equipment Identity Register (EIR)
5. Authentication center (AUC)

4.3.1 Mobile Switching Center (MSC)

It is the basic unit of NSS, which supports call-switching or routing functions. Its purpose is the same as that of telephone exchange but due to advanced wireless technology, its working is much better than that of exchange. Each MSC provides coverage to a defined geographic area only.

4.3.2 Home Location Register (HLR)

For subscriber it is a reference data base. Current location of MS, identification numbers and various addresses are maintained in it. It stores information of all subscribers belonging to an area served by a MSC. The HIR has to provide the MSC with all the

necessary information when the call is coming from a public network.

4.3.3 Visitor Location Register (VLR)

It is also a type of database. When an MS moves from home location to a visited location then its location is registered as a visitor in the VLR of visited system and this information is also updated in HLR of MS, by the VLR.

4.3.4 Equipment Identity Register (EIR)

It's also a type of databases, which contains information about MS equipment and check and identifies its international validity of hardware and software to work properly.

4.3.5 Authentication center (AUC)

It's a processing center and is normally worked together with HLR. Like HLR it's also require to continuously access or update subscriber's data. Its main purpose is to provide data security features to authenticate the subscriber.

5. System Design and Implementation

5.1 System Design

The system is implemented with two portions, for uplink and downlink communication. The block diagrams for uplink and downlink communication are shown in Figure 2 and Figure 3 respectively.

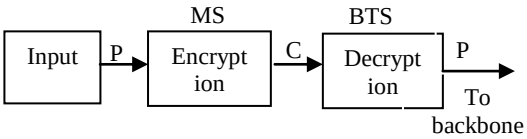

Figure 2. Block diagram for Uplink Communication

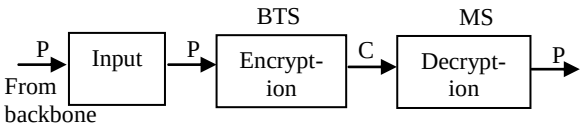

Figure 3. Block diagram for Downlink Communication

5.1.1 Uplink Communication

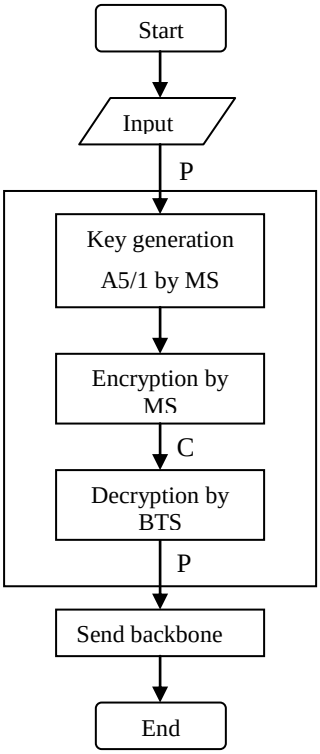

Figure 4. System Design for uplink Communication

The uplink communication system design is shown in Figure 4. It is implemented with the MS Station and BTS Station by using two personal computers. A5/1 algorithm is implemented in MS, which generates a unique keystream for every message frame. The 228 bits of keystream output are generated. The first 114 bits of the keystream is used in MS for encryption the message. In BTS Station, A5/1 algorithm is also implemented for generation the same keystream for this message frame. But the first 114 bits of the keystream is used to decrypt the message. After decryption, the message is sent to the receiver's BTS Station through the backbone network.

5.1.2 Downlink Communication

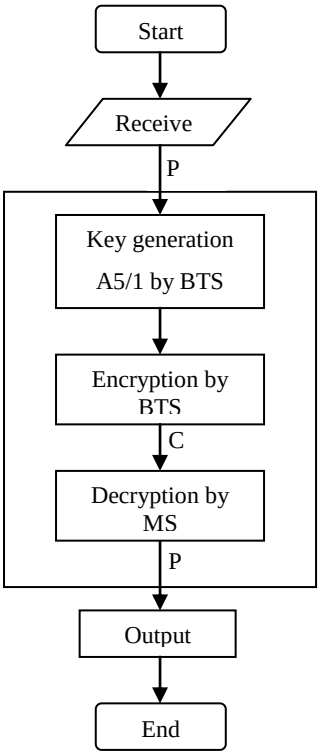

Figure 5. System Design for downlink Communication

The downlink communication system design is shown in Figure 5. The BTS and MS Stations are also implemented by another two personal computers. A5/1 algorithm is used in BTS, which generates a unique keystream for every message frame. The 228 bits of keystream output are also generated. The next 114 bits of the keystream is used in BTS for encryption the message. In MS Station, A5/1 algorithm is also used for generation the same keystream for this message frame. But the next 114 bits of the key is used to decrypt the message. After decryption, the receiver gets the original message in MS Station. The purpose of the implementing system is to provide confidentiality of user data and prevent casual eavesdropping by encrypting communications between MS and BTS. This system encrypts information for security and privacy. Therefore it can protect network against attacks.

5.2 System Implementation

For uplink communication, this system can rank the input message that less than 32 or 32 characters as one frame. The frames are regarded by the incoming input message as shown in Figure 6.

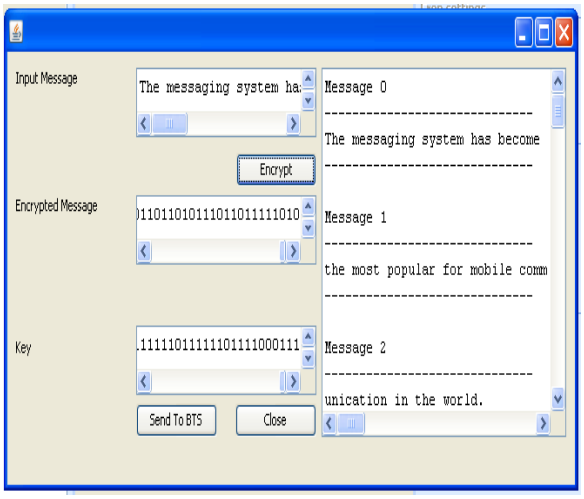

Figure 6. Regarding the frames from the input message

The key generation takes place one time**.** If the input message frames are more than one, another key generation will be needed. The 64 bits session key K_c that initialized in A5/1 algorithm is the same but the 22 bits frame numbers are changed during the call. The first 114 bits are used as the keystream for uplink (MS to BTS) communication in the full-duplex mode and the next 114 bits are again used for downlink (BTS to MS) communication. A5/1 algorithm generates a unique keystream for every message frame. The input message is Xored to encrypt with the first 114 bits of keystream that producing in MS in Figure 7.

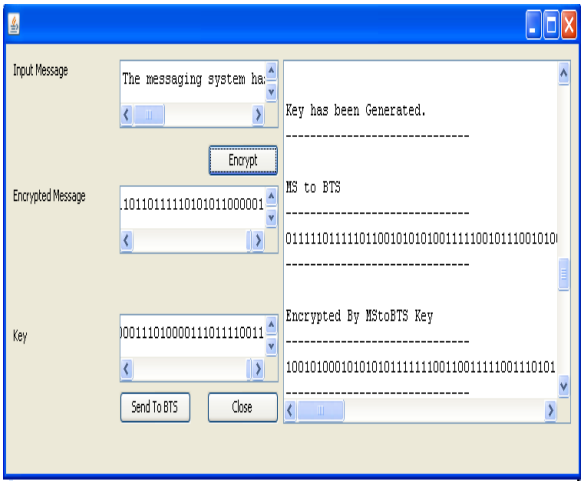

Figure 7. Key generation and message encryption

The encrypted message is sent to the BTS. Once the frame has been received by the BTS, it is Xored to decrypt them with the first 114 bits of the keystream and sends them in plaintext to the operator's backbone network in Figure 8.

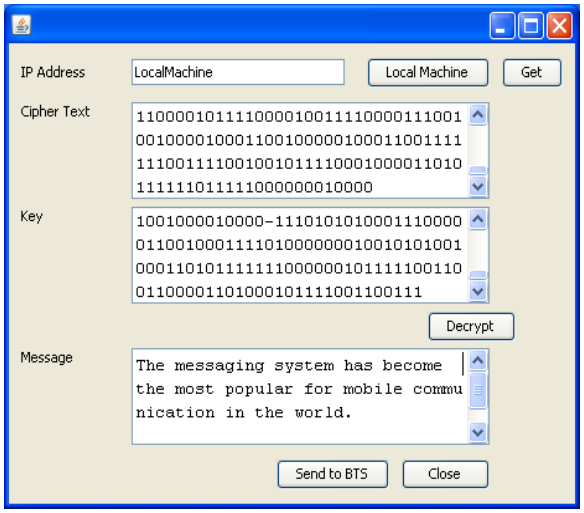

Figure 8. Message decryption

For downlink communication, the message from the backbone network is received by BTS. The key generation takes place in BTS. The receiving message is Xored to encrypt with the next 114 bits of keystream and send them the MS. The encrypted message is Xored to decrypt with the same key and the receiver gets the original (plaintext) message. Therefore this secure system encrypts twice original message to arrive to the receiver. The key advantage of symmetric encryption in the system is computationally fast and efficient because it uses the same key to encrypt and decrypt the message.

6. Conclusion

The system uses A5/1 algorithm to secure data transmissions.The A5/1 algorithm is used to prevent casual eavesdropping by encrypting communications between Mobile Station and BSS. This system uses the cipher key(session key) K_c as the key to the A5/1 algorithm for subsequent encryption of data between the Mobile Station (MS) and the Base Transceiver Station(BTS).The use of a rekeyed cipher is a good way of obtaining a guaranteed huge period . The security mechanisms make it to secure mobile communication standard currently available. The system provides confidentiality of user data.

7. References

[1] Anderson Ross, A5 - The GSM Encryption Algorithm, 17.6.1994,[referred 30.9.1999] <http://chem.leeds.ac.uk/ICAMS/people/jon/a5.html >

[2] Cooke, J.C.; Brewster, R.L., "Cryptographic Security Techniques for Digital Mobile Telephones," Proceedings of the IEEE International Conference on Selected Topics in Wireless Communications, Vancouver, B.C., Canada, 1992.

[3] D. Margrave, "GSM Security and Encryption," [Online document], Available HTTP: http://www3.l0pht.com/~oblivion/blkcrwl/cell/gsm/gsm-secur/gsm-secur.html

[4] Friedhelm Hillebrand, GSM and UMTS : the creation of global mobile communication, 2002

[5] J. Dj. Golic, "On the security of shift register based keystream generators," Fast Software Encryption - Cambridge '93, *Lecture Notes in Computer Science*, vol. 809, R. J. Anderson ed., Springer-Verlag, pp. 90-100, 1994.

[6] A5 cryptanalysis by Ross Anderson, Michael Roe, Bruce Schneier and Simon Shepherd: http://jya.com/crack-a5.htm

[7] Van der Arend, P. J. C., "Security Aspects and the Implementation in the GSM System Proceedings of the Digital Cellular Radio Conference, Hagen, Westphalia, Germany, October, 1988.