Analyzing the Security Techniques used in LTE Advanced and their evaluation

Iftikhar Rasheed,Asjad Amin, Mahwish Chaudhary, Sadaf Bukhari, Muhammad Rizwan, Kashif Ali
Department of Telecommunication Engineering
The Islamia University of Bahawalpur
Bahawalpur, Pakistan
iftikhar.rasheed@iub.edu.pk, asjad.amin@iub.edu.pk, mahwish_ch@hotmail.com, Sadafbukhari02@hotmail.com,
ucet45@gmail.com, kashifali.031@gmail.com

Abstract— **In this paper we discuss about security which is the main element in the wireless communication. As the generation changes many steps are used to improve the security so in this we discuss many security techniques choose, implement and compare two of them which provide better security to customers in LTE Advanced. LTE Advanced is evolved and advanced version of LTE (Long Term Evolution) which is developed by 3GPP. We implement the security techniques which we can use in LTE Advanced. To secure our data we use security algorithms (KASUMI & TDES) which have two parts encryption and decryption. In encryption process we convert our original data in cipher text by using keys and then transmit this encrypted data to the receiver. And at the receiving end we decrypt the encrypted data with the same keys to recover the original data. KASUMI Algorithm is a block cipher that produces a 64-bit output from 64-bit input under the control of a 128-key and three functions. It has 8 rounds. TDES Algorithm is a block cipher that produces a 64-bit output from a 64-bit input under the control of three keys of 64-bits with a function. It has 16 rounds. We implement these techniques in Matlab for verifying our results, and then we conclude that both algorithms are efficient for security purposes, so that no one can crack our data.**

Key words: LTE Advanced, Kasumi securitytechnique, Triple DES security Technique

I. Introduction

The evolved version of LTE is LTE advanced which is developed by 3GPP. LTE advanced will fulfill the requirements for 4G radio communication standards. The features of LTE advanced that it has wider bandwidths, enabled by wider aggregation, higher efficiency, enabled by enhanced uplink multiple access and enhanced multiple antenna transmission (advanced MIMO techniques) [1].

To secure our data we use security algorithms which have two parts encryption algorithm and decryption algorithm. In encryption algorithm mathematical formulas or functions are used to transform the unprotected information in protected format [2] while decryption algorithm is used to converts the cipher text into plain text. As the time passes many steps, many security algorithms are used to improve the security in radio communication for example in 2nd generation GSM use the security algorithms A3, A8, A5/2 and A5/3 which is breakable then 3G improves the flaws that we face in GSM and it very much improves the security and then in 4G LTE and LTE Advanced provides good security due to the use of strong and reliable security algorithms. In order to provide the security in LTE-A we briefly discuss the DES algorithm, Blowfish algorithm, Speed algorithm, Threefish algorithm, Chinese ZUC algorithm, A5/1 algorithm, KASUMI algorithm, SNOW3G algorithm and TDES algorithm then we implement two of them KASUMI algorithm and TDES algorithm and compare their results.

The DES (data encryption standard) algorithm is widely used encryption algorithm in the world. It uses the 56 bit key to encrypt and decrypt the 64 bit data in 16 rounds through feistel structure while the remaining 8 bits of key is used in error detection [3] [4] .

SNOW3G algorithm is used in 3GPP. It is word oriented stream algorithm. It uses the 128-bit key to produce a sequence of 32- bit words then these words can be used to protect the plain text [5].

A5/1 is synchronous stream cipher used in GSM and it is the strong algorithm. It uses 64 bit key for ciphering and deciphering. A5/1 consists of three short linear feedback registers of lengths 19, 22, 23 bits which are denoted by R1, R2, and R3 [6].

Chinese ZUC algorithm is a word oriented stream cipher and plays an important role in 3GPP LTE advanced. It uses 128-bit key and 128-bit initial vector to generate the key stream of 32-bit words [7].

SPEED algorithm is a private key block cipher that supports the data length of 64, 128 or 256 bits and key length of 48, 256 or divisible by 16 [8].

Blowfish algorithm is a symmetric block cipher that uses the variable-length key from 32 bits to 448 bits to encrypt and decrypt the 64 bits of data 16 times through feistel structure [9].

Triple DES is based on DES algorithm. It is the strongest version of DES but runs three times slower than DES. It uses three 64 bit keys for encryption and decryption the 64-bit data [10].

Threefish block cipher encrypts and decrypts the data of different sizes 256 bits, 512 bits and 1024 bits. The size of keys used in this algorithm is same as the data size.

978-1-4799-0615-4/13/$31.00 ©2013 IEEE

KASUMI algorithm is a block cipher that plays an important role in 3G UMTS standards, 2G GSM and 2.5 GPRS standards. It uses 128 bit key to encrypt and decrypt the 64 bit data blocks in 8 rounds of feistel structure [11].

A. KASUMI Algorithm

KASUMI algorithm is a block cipher which was adopted by 3rd generation partnership project program. KASUMI algorithm has a feistel network consisting of eight rounds; apply on 64-bit data by the use of 128-bit key where this key is used to generate a set of round keys (KLi, KOi, KIi) for each round where each round computes the different functions as well as different keys and the same algorithm is used for both encryption and decryption [11].

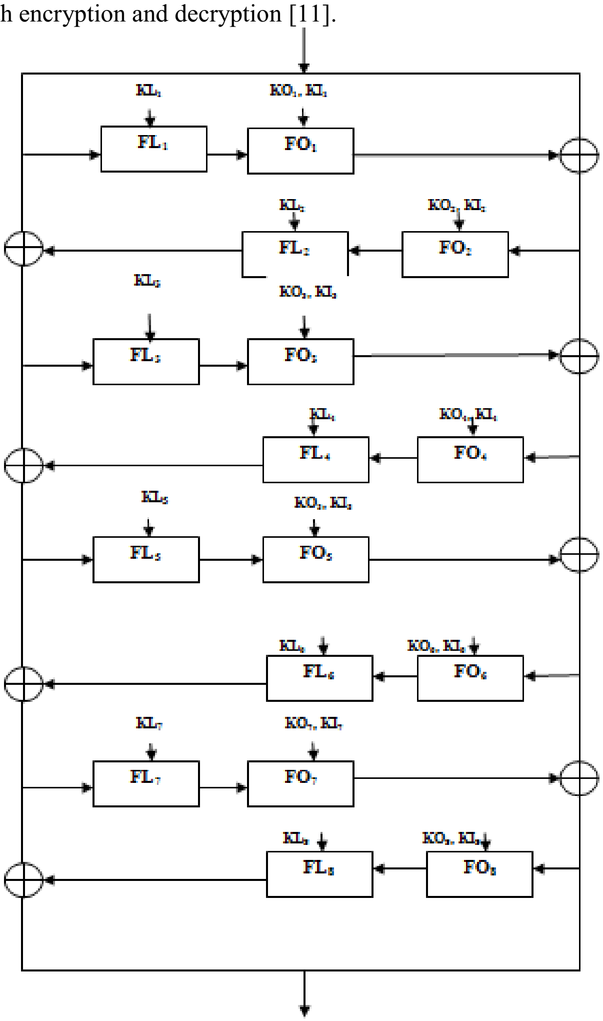

Figure 1: Block Diagram of Kasumi algorithm

B. TDES Algorithm

Triple DES is a mode of DES operation. It uses three 64-bit keys means 192-bit to encrypt and decrypt the data, in each 64-bit key there are 8 parity bits that is not used in encryption or decryption process. The method that is use for both encryption and decryption is similar as DES algorithm but it is repeated in three times. In TDES encryption first the data is encrypted through 56-bit key K1, then decrypted through 56-bit key K2 and then again encrypted with key K3 while in decryption process first the cipher data is decrypted with K3, then encrypted with K2 and then again decrypted through K1[12].

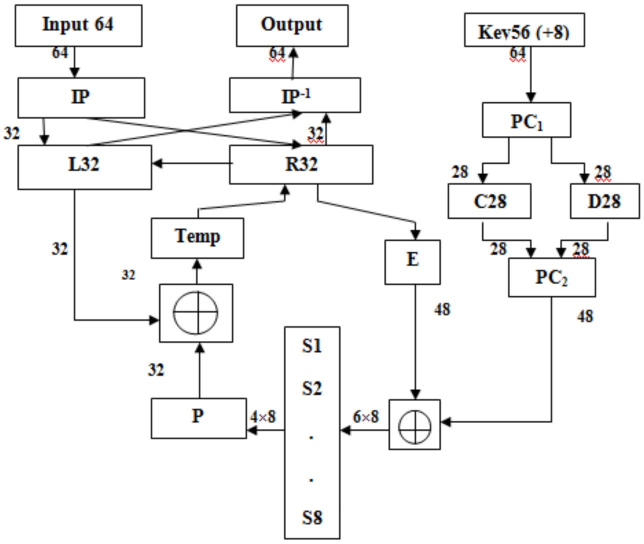

Figure 1: Block Diagram of DES algorithm on which TDES algorithm based

II. IMPLEMENTATION RESULTS OF KASUMI ALGORITHM

In the implementation of KASUMI algorithm in Matlab during encryption we take 128-bit key and the 64-bit of data for example(111111111111111111) which is divided into two 32-bit halves Li (25870071) and Ri (2.2209e+009). These Li and Ri are pass through three functions FOi, FLi and FIi in feistel structure from eight rounds where i represent the round numbers. After eight rounds we get the encrypted data i.e(101111111011111000011011001001011100001010110101011101110111 100100110). And in decryption all functions and subkeys are used in reverse order then we get the (000000011000101010111110111101111100001000110000000111000111000000).

III. IMPLEMENTATION RESULTS OF TDES ALGORITHM

In the implementation of TDES algorithm we take three 64-bit keys and 64-bit input data for example(111111111111111111111111111111111111111111111 1111111111111111111). During encryption the input data is first DES encrypted then DES decrypted and then again DES encrypted with keys K0, K1 and K2 respectively and then we get the 64-bit cipherdata(1100011110000111110100100110111111101101000001 1011011101001000011). In decryption keys are used in reversed order and we get our decrypted data of 64-bit which is equal to the input data.

IV. COMPARISON

For security of data, it must be sent in encrypted form by using special key and decrypted at the receiver side. In order to improve the security in 4G we analyze two algorithms

TDES and KASUMI, both are symmetric block ciphers and give better performance. TDES use three keys for encryption and decryption which makes it stronger while KASUMI use only one key. We use ECB mode of operation in TDES which makes algorithm Simplest method, blocks can be encrypted in parallel, error in transmitting one ciphertext block causes that block to decrypt incorrectly, but other blocks are not affected while in KASUMI algorithm no mode of operation is used. TDES is suitable and efficient to implement in both software and hardware when compared to other encryption algorithms. Triple DES runs three times slower than DES, but is much more secure if used properly. TDES provides good security in PIN enable ATM transaction, commerce and government applications, WiMAX encryption, RFID, password authentication on most Linux and UNIX-like systems at this time, Data Socket as well as TCP and UDP communications, Electronic Funds Transfer, remote control systems and mobile phone communications. Many security-enhanced dynamic routing algorithms based on TDES algorithm widely supported in existing wired and wireless networks. The advantage of TDES is that no practical attack known today as compared to KASUMI algorithm.

A. Time Space Computation

After time space computation we conclude that to recover the complete data bits, TDES security techniques take little more time as compared to kasumi security technique.

Sr. No	Properties	TDES Algorithm	KASUMI Algorithm
1	**Rounds**	16	8
2	**Rounds in encryption**	3×16	1×8
3	**Rounds in decryption**	3×16	1×8
4	**Number of keys**	3	1
5	**Length of key**	64-bit	64-bit
6	**Time space computation**	More time	Less time

V. CONCLUSION

From the results it is concluded that although both algorithms recover accurate data but TDES algorithm is more secure than KASUMI algorithm and stronger against brute force attack, differential cryptanalysis, linear cryptanalysis and any attack due to the use of three different keys and 16 rounds while KASUMI use one key and 8 round. Although TDES take little more time. TDES is suitable and efficient to implement in both software and hardware when compared to other encryption algorithms.

REFERENCES

[1]. Introducing LTE-Advanced Application Note.

[2]. Introduction to Cryptography by Barry K. Shelton.

[3]. Design of Secure Computer Systems CS14138/CEG4394, Notes on DES.

[4]. New Comparative Study Between DES, 3DES and AES within Nine Factors Hamdan.O.Alanazi, B.B.Zaidan, A.A.Zaidan, Hamid A.Jalab, M.Shabbir and Y. Al-Nabhani.

[5]. SNOW 3G Stream Cipher Operation and Complexity Study, Ghizlane ORHANOUghizlane.orhanou@gmail.com , Said EL HAJJI elhajji@fsr.ac.ma , Youssef BENTALEB youssef_bentaleb2003@yahoo.fr Laboratoire Mathematiques, Informatique et Applications,Universite Mohammed V Agdal, Faculté des Sciences BP 1014, Rabat, Maroc.

[6]. Hardware-Based Cryptanalysis of the GSM A5/1 Encryption Algorithm Timo Gendrullis May 29th, 2008.

[7]. Differential Power Analysis on ZUC Algorithm TANG Ming1,2, CHENG PingPan2 ,QIU ZhenLong2 1State Key Lab. of AIS & TC, Ministry of Education, Wuhan University, Wuhan 430072, China; 2School of Computers, Wuhan University, Wuhan 430072, China.

[8]. The SPEED Cipher Yuliang Zheng School of Computing, Monash University McMahons Road, Frankston, Melbourne, VIC 3199, Australia Email: yzheng@fcit.monash.edu.au.

[9]. Blowfish Brent A. Cottom CS 6520 Cryptography 8/18/2004.

[10]. Triple DES – Definition, Mandates and Practical Application by Drago S. Dzerve, Director of Market Development for RBS World Pay.

[11]. Specification of 3GPP and confidential algorithms.

[12]. Triple Data Encryption Standard (Triple-DES) http://www.vocal.com.