Performance Analysis of Mobile Security Protocols: Encryption and Authentication

Anita Singhrova email: nidhianita@gmail.com
Sr. Lecturer in CSE Department,
DBCR University of Science and Technology, Murthal,
Sonepat, Haryana, 130131 INDIA.

Dr. Nupur Prakash email: nupurprakash@rediffmail.com
Dean, University School of Information Technology,
Guru Gobind Singh Indraprastha University, Kashmere Gate,
Delhi 110006, INDIA.

Abstract

Due to extremely high demand of mobile phones among people, over the years there has been a great demand for the support of various applications and security services. 2G and 3G provide two levels of security through: encryption and authentication. This paper presents performance analysis and comparison between the algorithms in terms of time complexity. The parameters considered for comparison are processing power and input size. Security features may have adverse effect on quality of services offered to the end users and the system capacity. The computational cost overhead that the security protocols and algorithms impose on lightweight end users devices is analyzed. The results of analysis reveal the effect of authentication and encryption algorithms of 2G and 3G on system performance defined in terms of throughput which will further help in quantifying the overhead caused due to security.

Keywords: Encryption, Authentication, GSM (Global System for Mobile communication), UMTS (Universal Mobile Telecommunication System), Time complexity, Performance Analysis, Throughput.

1. INTRODUCTION

The fixed line telephones had revolutionized the concept of voice communication, but with passage of time, lack of mobility was felt seriously. Moreover, delay in new connection, last mile wired connectivity and security hazards were few other problems.

The first generation (1G) of mobile communication system was introduced in 1985 and was driven by analog signal processing technique. It had certain problems, like phone fraud through cloning phones and thus calling at someone else's expense, and the possibility of someone intercepting the phone call over the air and eavesdropping on the discussion.

The second generation (2G) of mobile communication systems popularly known as GSM (Global System for Mobile communication) was one of the first digital mobile phone systems to follow analog era and had started in 1992. The GSM system was supposed to overcome the phone fraud and call interception problems of an analog era by implementing strong authentication between the MS and the MSC, as well as implementing strong data encryption for over the air transmission channel between the MS and BTS [1][2]. The GSM system also suffered some of the shortcomings. The attack against A5, accessing the signaling network, retrieval of key and false base station attack etc.

2.5G is known as GPRS (General Packet Radio Services) came in 1995. This does not implement any new algorithms for authentication or confidentiality, but it uses same algorithm for authentication and encryption as 2G and multiple timeslots in parallel in order to achieve a greater transmission rate i.e. 171 kbps [3].

The third generation (3G) of mobile communication systems known as UMTS (Universal Mobile Telecommunication Systems) was introduced in 2002 and intends to establish a single integrated and secure network. The 3GPP (Third Generation Partnership Project), is a follow up project of GSM which implements UMTS (Universal Mobile Telecommunication Systems) [4][5]. It lays down standards to support broadband data services and mobile multimedia using a wideband radio interface international roaming for circuit switched and packet switched services. Mobile/wireless Internet is becoming available with 3G mobile communication

systems. The complete 3G security architecture consists of five major security classes: (i) network access security, (ii) network domain security, (iii) user domain security, (iv) application domain security and (v) visibility and configurability of security [6].

The fourth generation (4G) of mobile communication systems with its year of inception predicted as 2010-2012[7] is a futuristic approach and is envisioned as a convergence of different wireless access technologies [8].

Wireless networks are as such less secure and mobility further adds to security risk. Therefore, it is desirable that 2G and 3G are atleast as secure as fixed networks if not over secure. Security is achieved at the cost of performance degradation, therefore, it is critical and important to quantitatively measure overheads caused by various security services [9] [10].

The Section 2 presents the various security mechanisms of 2G and 3G in brief. Section 3 deals with the performance Analysis of Authentication and Encryption Algorithms of 2G and 3G both followed by discussion on the performance analysis in terms of throughput. Section 5 is devoted to review the future trends. Finally, summary and conclusion is given in section 6.

2. SECURITY FEATURES

2.1. 2G Security Overview

The security mechanism in 2G mainly consists of subscriber identity authentication and confidentiality i.e. encryption of user traffic.

2.1.1 Authentication

In GSM the authentication algorithm used is A_3. Its function is to generate the 32-bit SRES (Signed Response) to the MSC's random challenge, RAND and the secret key K_i from the SIM as input i.e. SRES= A_3 K_i (RAND). The subscriber identity authentication is used to identify the MS to the PLMN (public land mobile network) operator [11]. Authentication is a one way process. The MS is authenticated but the visited PLMN is not. Therefore, GSM is open to false base station attack.

In GSM A_8 algorithm is used as key generation algorithm. It generates a 64 bit session key, K_c, from the 128 bit random challenge, RAND, received from the MSC and from 128 bit secret key K_i i.e. K_c= A_8 K_i (RAND). The BTS receives the same K_c from the MSC. HLR is able to generate the K_c, because the HLR knows both the RAND (the HLR generated it) and the secret key K_i, which it holds for all the GSM subscribers of this network operator. One session key, K_c, is used until the MSC decides to authenticate the MS again.

The $COMP_{128}$ generates both the SRES response and the session key, K_c on one run [11]. Therefore $COMP_{128}$ is used for both the A_3 and A_8 algorithms.

2.1.2 Encryption

A5 algorithm is the stream cipher and is used to encrypt over-the-air transmissions to protect sensitive information against eavesdropping on the air interface [12].

$K_c = A_8K_i$ (RAND) and Ciphertext = A_5K_c (Plaintext)

Each frame in over-the-air traffic is encrypted with a different key stream. The same K_c is used throughout the call, but the 22-bit frame number changes during the call, thus generating a unique key stream for every frame [12]. The A_5 algorithm consists of three LSFRs of different lengths.

The data is encrypted only between the MS and BTS. After the BTS the traffic is transmitted in the plain text within the operator's network. Therefore, if attacker can access the operators signaling network, then attacker can listen to everything transmitted.

2.2 3G Security Overview

Third generation mobile systems such as UMTS revolutionized telecommunications technology by offering mobile users content rich services, wireless broadband access to internet, and worldwide roaming. However, this introduced serious security vulnerabilities [4]. Encryption and Authentication are the two main security mechanisms in 3G network access securities [5].

2.2.1 Authentication

The UMTS authentication algorithm consists of seven functions f_1,f_1*,f_2,f_3,f_4,f_5 and f_5*. The standardized algorithm set for these seven functions is called MILENAGE. For MILENAGE, a specific kernel has to be chosen, and therefore Rijndael was selected [13] [14]. Rijndael is an iterated block cipher with a 128 bit block length and a 128 bit key length. It is composed of eleven rounds that transform the input into the output.

2.2.2 Encryption

Within the security architecture of the 3GPP system there are two standardized algorithm: a confidentiality algorithm f_8, and an integrity algorithm f_9[4], which are based on the KASUMI algorithm [14] [15].

3. PERFORMANCE ANALYSIS

This section analyses the performance of algorithms used for 2G and 3G authentication and encryption. The time complexity computation has been carried out for this purpose.

3.1 Analytical Analysis of 2G

3.1.1 Authentication

This involves the analysis of authentication and key generation algorithm using A3A8 algorithm for 2G [11]. Authentication initialization needs 48 operations.

OPERATIONS	TIMES	TIME NEEDED	EQUIVALENT TOTAL
Load Rand #	16	2	32
Load Key	16	1	16

Operations needed = 48

TABLE 1: Authentication initialization(load Rand # and key K_i)

OPERATIONS	TIMES	TIME NEEDED	EQUIVALENT TOTAL
Load Rand #	16	2	32
Load K_i	8	16	128
Substitution	8	2080	16640
Form bits	8	768	6144
Permutation	8	1168	9344

Total number of operations = 32 288

TABLE 2: Total operations in 2G authentication

The next step of substitution involves 3 variable j, k, l. Where j can have any value between 0 to 4, k can have value 2^n. For 1st iteration the value is 0 i.e 2^0 for n = 0; for 2nd iteration there are two values 0 and 1 i.e 2^1 for n=1, so on and so forth till n=4. And for l the value is 2^{4-n} . Therefore for n=0, j have values 2^4 i.e j = 0..15 ,if n=1, j have value 2^3 i.e j = 0..7 so on and so forth. Hence, total number of operation required for substitution is 5*16*26 where 26 are the number of operations carried out in 1 iteration. The next step of bit forming requires 32 * 4*6 operations and the permutation requires 72 for outer loop and 1168 for inner loop.

T_{A3A8} is total number of operations for authentication = 32 288.
T_{A3A8} = 32 288.
s_d is the size of original message (in bytes).
N is the message size in bits. $N=8 * S_d$
n is the total number of blocks, n = Ceil (N ÷ 128) where Ceil(x) means the smallest integer ≥ operand
U_{A3A8} is the total number of operations required for A3A8 authentication.
U_{A3A8}= ceil $((8 * S_d) \div 128) * T_{A3A8} = n * T_{A3A8}$
C_p is MIPS performed by the processor.
t_{A3A8} (S_d, C_p) is the time required for encryption (decryption) for processor speed C_p and message size S_d in bytes. $t_{A3A8}(S_d, C_p) = U_{A3A8}(S_d) \div C_p$ or $t_{A3A8}(S_d, C_p) = (\text{ceil}((8 * S_d) \div 128) * T_{A3A8}) \div C_p$
or $t_{A3A8}(S_d, C_p) = (n * T_{A3A8}) \div C_p$

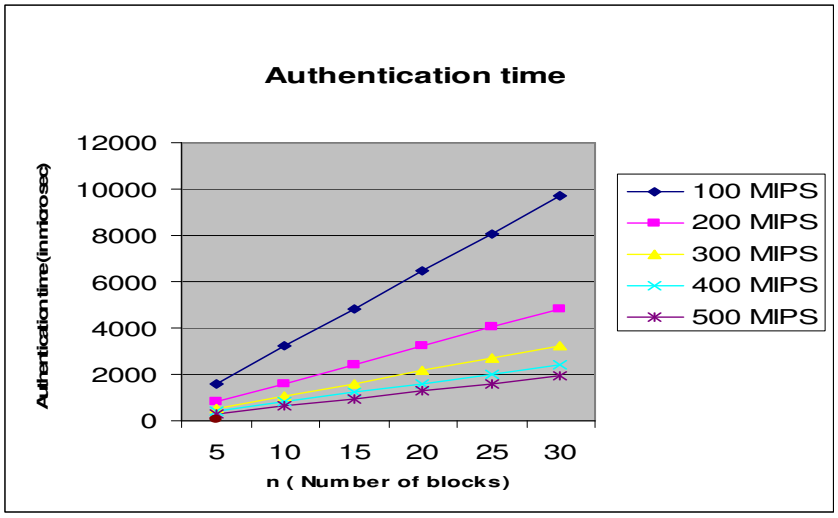

FIGURE 1: Authentication time (in μ sec) Vs n of i/p blocks and processing speed

3.1.2 Encryption

The LSFRs R1, R2, R3 are 19, 22 and 23 bits long respectively defined with the help of MASK 0x07FFFF (0..18 numbers) , 0x3FFFFF (0..21 numbers) and 0x7FFFFF (0..22 numbers). For clocking the feedback registers feedback taps are used[12]. Middle bit of each of the three shift registers, are used for clock

control i.e. R1MID 0x000100, R2MID 0x000400, R3MID 0x000400. The highest bit of LSFRs are taken as output taps. 18th, 21st and 22nd bits respectively for R1, R2 and R3 respectively [12].

OPERATIONS	TIMES	TIME NEEDED	EQUIVALENT TOTAL
Right shift by n	5	1	5
XOR	5	1	5
AND	1	1	1

operations needed =11

TABLE 3: Operations in Parity function

OPERATIONS	TIMES	TIME NEEDED	EQUIVALENT TOTAL
AND	2	1	2
Left shift by 1	1	1	1
OR	1	1	1
Parity ( )	1	11	11

operations needed = 15

TABLE 4: Operations in Clockone function

OPERATIONS	TIMES	TIME NEEDED	EQUIVALENT TOTAL
ADD	2	1	2
AND	3	1	3
Parity( )	3	11	33
Comparison	1	1	1

operations needed = 39

TABLE 5: operations in Majority function

OPERATIONS	TIMES	TIME NEEDED	EQUIVALENT TOTAL
Clockone( )	3	15	45

operations needed = 45

TABLE 6: Operations in Clockallthree function

OPERATIONS	TIMES	TIME NEEDED	EQUIVALENT TOTAL
Majority( )	1	39	39
Comparison	6	1	6
Clockone( )	3	15	45

operations needed = 90

TABLE 7: Operations in Clock function

OPERATIONS	TIMES	TIME NEEDED	EQUIVALENT TOTAL
AND	3	1	3
XOR	2	1	2
Parity ( )	3	11	33

operations needed = 38

TABLE 8: Operations in Getbit function

OPERATIONS	TIMES	TIME NEEDED	EQUIVALENT TOTAL
Clockallthree( )	1	45	45
Right shift	1	1	1
AND	2	1	2
Divide	1	1	1
XOR	3	1	3

operations needed = 52

TABLE 9: Operations in Key setup function

OPERATIONS	TIMES	TIME NEEDED	EQUIVALENT TOTAL
clockallthree	1	45	45
Right shift	1	1	1
XOR	3	1	3
AND	1	1	1

operations needed = 50

TABLE 10: Operations in Frame# load function

OPERATIONS	TIMES	TIME NEEDED	EQUIVALENT TOTAL
Clock ( )	1	90	90
Getbit( )	1	38	38
AND	1	1	1
Left shift	1	1	1
OR	1	1	1
Arithmetic operators	2	1	2

operations needed =133

TABLE 11: Operations in Run function

OPERATIONS	TIMES	TIME NEEDED	EQUIVALENT TOTAL
Keysetup	64	52	3328
Frame#Load( )	22	50	1100
Clock	100	90	9000
Run ( )	228	133	30324

Total operations needed=43 752

TABLE 12: Total operations for $A_5/1$

$T_{A5/1}$ is total number of operations in block encryption = 43 752.
$T_{A5/1}$ = 43 752
S_d is size of original message (in bytes)
N is the message size in bits. N=8 *S_d
n is the total number of blocks. n = Ceil (N ÷ 114)
where Ceil(x) means the smallest integer >= operand
$U_{A5/1}$ is the total number of operations required for encryption or decryption of message size Sd.
$U_{A5/1}$ = ceil ((8 * S_d) ÷114) * $T_{A5/1}$ = n * $T_{A5/1}$
C_p is MIPS performed by the processor.
$t_{A5/1}$ (S_d, C_p) is the time required for encryption (decryption) for processor speed C_p and message size S_d in bytes.
$t_{A5/1}$ (S_d , C_p) = $U_{A5/1}$ (S_d) ÷ C_p or $t_{A5/1}$ (S_d , C_p) = (ceil ((8 * S_d) ÷ 64) * $T_{A5/1}$) ÷ C_p
or $t_{A5/1}$ (S_d, C_p) = (n * $T_{A5/1}$) ÷C_p

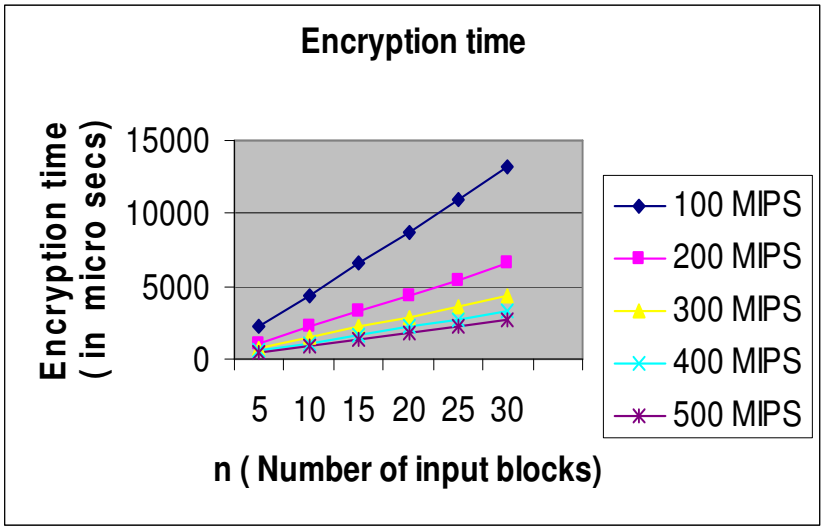

FIGURE 2: Encryption time (in µ sec) as a function of number of packets for different processing speeds (MIPS)

The total number of operations required by a processor to perform A_3A_8 and A_5/1 as a function of the packet size are presented in figure 3. A_5 requires more number of operations as compared to A_3A_8 .

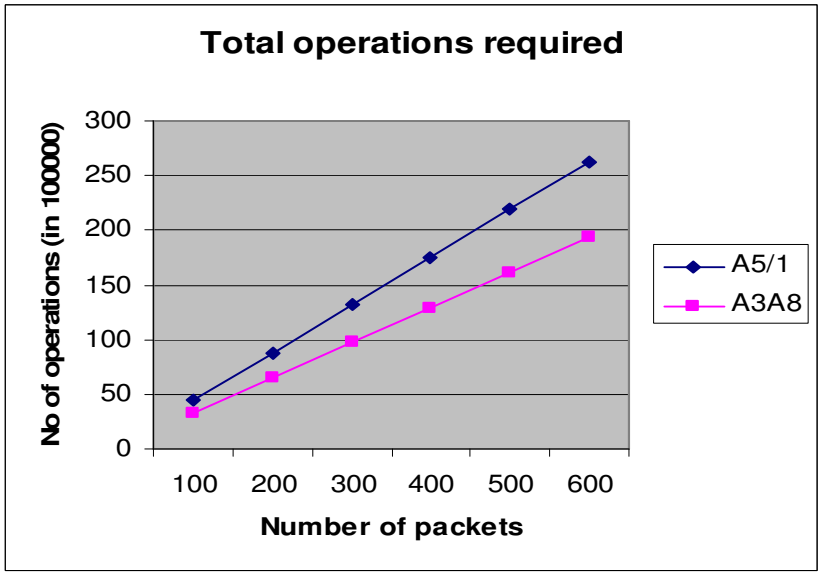

FIGURE 3: 2G, Total number of operations required as a function of number of packets for 2G algorithms

3.2 Analytical Analysis of 3G

3.2.1 Authentication

3G authentication is implemented by Rijndael. Rijndael is an iterated block cipher with a variable block length and variable key length [13]. The block and key length are independently specified as 128 bits for 3GPP and is used in encryption mode. It consists of 9 rounds in addition to an initial and a final round to transform the input into the output. An intermediate result is called state. The state can be a 4 X 4 rectangular array of bytes (128 bits in total).

3.2.1.1. The Byte Substitution Transformation

As described in paper [13] it is a non-linear byte substitution, operating on each of the State bytes independently. The substitution table is stored as S-box. In this transformation, we require 16 1-Dimensional lookup for 16 elements. Therefore, 16 operations are carried for 1 block of input of 128 bits.

3.2.1.2 The Shift Row Transformation

In this transformation[13], the rows of the State are cyclically left shifted by different amounts. Row 0 is not shifted, four states in row 1 are shifted by 1 byte, four states in row 2 by 2 bytes and four states in row 3 by 3 bytes. Therefore, 0 + (4*1) + (4* 2) + (4* 3) = 24 operations.

3.2.1.3. The Mix Column Transformation

The mix column transformation operates on each column of the State independently [13]. For each column there are (4 XOR + 1 multiplication + 1 optional XOR) *4. Since there are 4 columns there will be 80 or 100 operations.

3.2.1.4. The Round Key addition

In this operation, a Round Key is applied to the State by a simple bitwise exclusive-or[13]. The Round Key is derived from the Cipher Key by means of the key schedule. The Round Key length is equal to the block length. There are total of 16 XOR. Therefore, 16 operations are required for this transformation.

3.2.1.5. Key schedule

Rijndael has 11 Round Keys, numbered 0-10, that are each 4x4 rectangular arrays of bytes. Let $rk_{r,i,j}$ be the value of the r^{th} Round Key at position (i, j) in the array and $k_{i,j}$ be the cipher key loaded into a 4x4 array.

BASIC OPERATION	EQUIVALENT OPERATIONS		
	Type	Time needed	Space needed
Round key Addition	8-bit XOR	1	
Byte substitution Transformation	1-D table lookup [B]	1	b
Shift row Transformation	left shift by n bit	1	
Mix column Transformation	XOR	1	
	Multiply	1	
Key schedule	XOR	1	
	MULTIPLY	1	
Key schedule Initialization	8-bit copy	1	
2-D table look up (for i:j bit map)	Multiply	1	
	Add	1	
	1-D table lookup	1	i i rows * j col
2-D table (for 4*4 bit map) into 1-D or vice versa	COPY	1	
	Add	1	
	Right shift by 2 bits	1	4 rows * 4 col

TABLE 13: Rijndael basic operations

Operations	Times	Time needed	Equivalent Total
Round key addition	16	1	16
Byte substitution transformation	16	1	16
Shift row transf(1 for 1st row, 2 for 2nd row And 3 for 3rd row)	4	1+1+1 =3	12
Column transf.(4XOR +1 Multiply +1 XOR optional) * 4 for 1 column.	4	(4+1)*4 =20	80
Key initialization	16	4	16
Key schedule XOR+ 1 Multiply * 10 (for rounds) + 12 XOR for 4 col.)	1	60 + 12 = 72	72

TABLE 14: Rijndael operations

step	operations	Times	Time needed	Equivalent total
0	Key initialization	1	1	1
	Key schedule	1	72	72
0-10	Key (2-D lookup)	11	3	33
1	8-bit round key addition	1	16	16
1-9	Round	9	16+12+80+16 =124	1116
10	Final round	1	16+12+16= 44	56
0	1-D rep. into 2D	16	3	48
10	2-D rep. into 1-D	16	3	48

Total = 1 441 operations

TABLE 15: Total Rijndael operations (1 block Auth.)

$T_{rijndael}$ is total number of operations in 1 block encryption.
$T_{rijndael}$ = 1 441
S_d is the size of original message (in bytes).
N is the message size in bits. $N=8 * S_d$
n is the total number of blocks. n = Ceil (N ÷ 128)
where Ceil(x) means the smallest integer ≥ operand
$U_{rijndael}$ is the total number of operations required for Rijndael encryption or decryption of message size Sd.

$$U_{rijndael} = \text{ceil}((8 * S_d) \div 128) * \text{Trijndael} = n * T_{rijndael}$$

Cp is MIPS performed by the processor .
$t_{rijndael}$ (S_d, C_p) is the time required for encryption (decryption) for processor speed C_p and message size S_d in bytes.
$t_{rijndael}(Sd, Cp) = U_{rijndael}(Sd) \div Cp$ or $t_{rijndael}(Sd, Cp) = (\text{ceil}((8 * Sd) \div 128) * T_{rijndael}) \div Cp$
or $t_{rijndael}(Sd, C_p) = (n * T_{rijndael}) \div C_p$
The mobile devices are equipped with embedded processors, which can perform 100-500 Million of Instructions per Seconds (MIPS) [16].

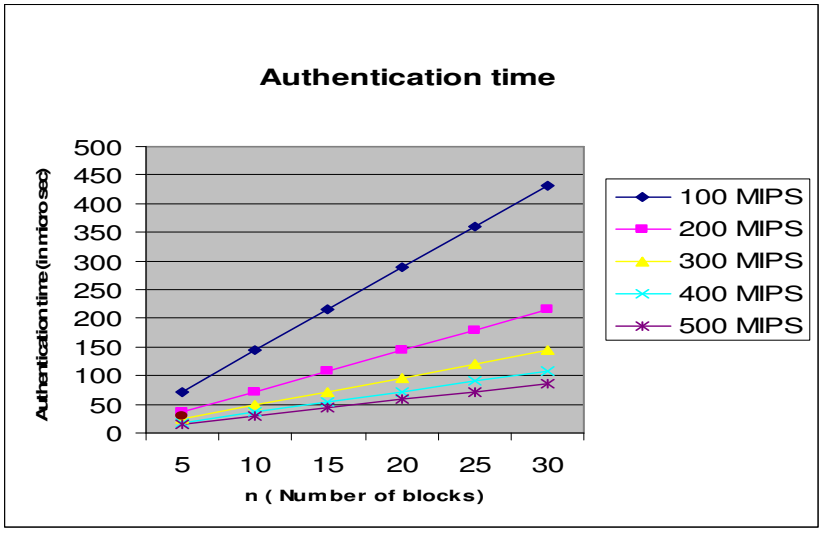

FIGURE 4: Authentication time (in μ sec) Vs n of i/p blocks and processing power

3.2.2 Encryption

3G encryption uses KASUMI algorithm. KASUMI uses a 128 bit key and block size of 64 bits. The algorithm has 8 distinct steps and 8 rounds [15]. Steps 1 to 8 are functionally identical and are dependent on different portions of input key.

3.2.2.1. FL Function

The function FL consists of two XOR (16-bit each), four 16-bit copy, one AND, one OR and two left shifts (cyclic) by one bit each [15]. The input to the function FL comprises a 32-bit data input I, a 32-bit sub key and a 32-bit output.

3.2.2.2. FO Function

The input to the function FO comprises a 32-bit data input I and two sets of sub keys, a 48-bit sub key KOi and 48-bit sub key KIi [15]. The 32-bit data input is split into two halves. The 48-bit sub keys are subdivided into three 16-bit sub keys and we return the 32-bit value (L3 || R3). This function consists of six 16-bit XOR, six 16-bit copy and three FI function call.

3.2.2.3. FI Function

The function FI [15] takes a 16-bit data input I and 16-bit sub key. The input I is split into two unequal components, a 9-bit left half L_0 and a 7-bit right half R_0 where $I = L_0 \| R_0$.Similarly the key KIi,j is split into a 7-bit component KIi,j,1 and a 9-bit component $KI_{i,j,2}$ where $KI_{i,j} = KI_{i,j,1} \| KI_{i,j,2}$. The function uses two S-boxes, S_7 and S9. The function returns the 16-bit value ($L_4 \| R_4$).This function consists of three 9-bit XOR, three 7-bit XOR and six 7-bit copy. Two times S9 and S7 mappings respectively, and invokes ZE( ) and TR( ) functions twice.

3.2.2.4. S-boxes

The two S-boxes [6] have been designed so that they may be easily implemented in combinational logic as well as by a look-up table.

3.2.2.5. Key Schedule

KASUMI has a 128-bit key K. Each round of KASUMI uses 128 bits of key that are derived from K [15]. The 128-bit key K is subdivided into eight 16-bit values and a second array of sub-keys, Kj' is derived from Kj. This function consists of eight 16-bit XOR, eight 1-bit cyclic left shift, eight 5-bit cyclic left shift, eight 8-bit cyclic left shift and eight 13-bit cyclic left shift. The extraction of round sub-keys is a 2-D table lookup.

Basic operation	EQUIVALENT SIMPLE OPERATIONS		
	TYPE	TIMES NEEDED	SPACE NEEDED
ZE	XOR	1	
TR	XOR	1	
2D Table map (i:j bit map)	MULTIPLY	1	
	ADD	1	
	1-D TABLE LOOKUP	1	I ROWS * J COLUMN
Left Shift	LEFT SHIF T BY N BITS	1	
Copy**	N * 32-BITCOPY	N	
XOR**	N * 32-BIT XOR	N	
AND**	N * 32-BIT AND	N	
OR**	N* 32-BIT OR	N	

** for 32-bit processor and up to 32-bits N=1.

TABLE 16: KASUMI basic operations

Operations	Times	Time needed	Equivalent total
16-bit XOR	2	1	2
16-bit COPY	4	1	4
16-bit AND	1	1	1
16-bit OR	1	1	1
16-bit left shift	2	1	2
16-bit split	1	3	3
16-bit combine	1	3	3
2D key lookup	2	3	6

Total=22 operations

TABLE 17: KASUMI - FL function

Operations	Times	Time needed	Equivalent Total
Endian correct	8	5	40
K prime	8	2	16
construct subkeys	8	34	272

Total = 328 operations

TABLE 18: KASUMI – Keys

Operations	Times	Time needed	Equivalent total
Key XOR (KIi,j,1 and KIi,j,2)	2	1	2
9-bit XOR	2	1	2
7-bit XOR	2	1	2
7-bit copy	3	1	3
9-bit copy	3	1	3
S9 mapping (1-D table map)	2	1	2
S7 mapping (1-D table map)	2	1	2
ZE	2	1	2
TR	2	1	2
7-9 bit split	1	4	4
7-9 bit combine	1	3	3
Key split in seven	1	2	2
Key split in nine	1	2	2

Total = 31 operations

TABLE 19: KASUMI - FI function

Operations	Times	Time needed	Equivalent total
16-bit XOR	6	1	6
16-bit COPY	6	1	6
FI ( )*	3	31	93
16 bit split	1	3	3
16 bit combine	1	3	3
2D key lookup	6	3	18

Total = 129 operations

*in one FO( ), FI ( ) is called three time

TABLE 20: KASUMI -- FO function

step	Operations	times	Time needed	Equivalent total
1-8	32-bit COPY	16	1	16
1-8	32-bit XOR	8	1	8
1-8	FL ( )	8	22	176
1-8	FO ( )	8	129	1032
	key setup	1	328	328
1	32 bit split	1	22	22
8	32 bit combine	1	14	14

Total = 1596 operations

TABLE 21: KASUMI operations (1 block encry.)

T_{kasumi} is total number of operations in block (encryption) = 1596.
T_{kasumi} = 1596
S_d is the size of original message (in bytes).
N is the message size in bits. N=8 *S_d
n is the total number of blocks. n = Ceil (N ÷ 64)
where Ceil(x) means the smallest integer >= operand
U_{kasumi} is the total number of operations required for KASUMI encryption or decryption of message size Sd.

$$U_{kasumi} = \text{ceil}((8 * S_d) \div 64) * \text{Tkasumi} = n * T_{kasumi}$$

C_p is MIPS performed by the processor.
t_{kasumi} (S_d, C_p) is the time required for encryption (decryption) for processor speed Cp and message size S_d in bytes.

$$t_{kasumi}(S_d, C_p) = U_{kasumi}(S_d) \div C_p \text{ or } t_{kasumi}(S_d, C_p) = (\text{ceil}((8 * S_d) \div 64) * T_{kasumi}) \div C_p$$

or $t_{kasumi}(S_d, C_p) = (n * T_{kasumi}) \div C_p$

The mobile devices are equipped with embedded processors, which can perform 100-500 Million of Instructions per Seconds (MIPS) [16].

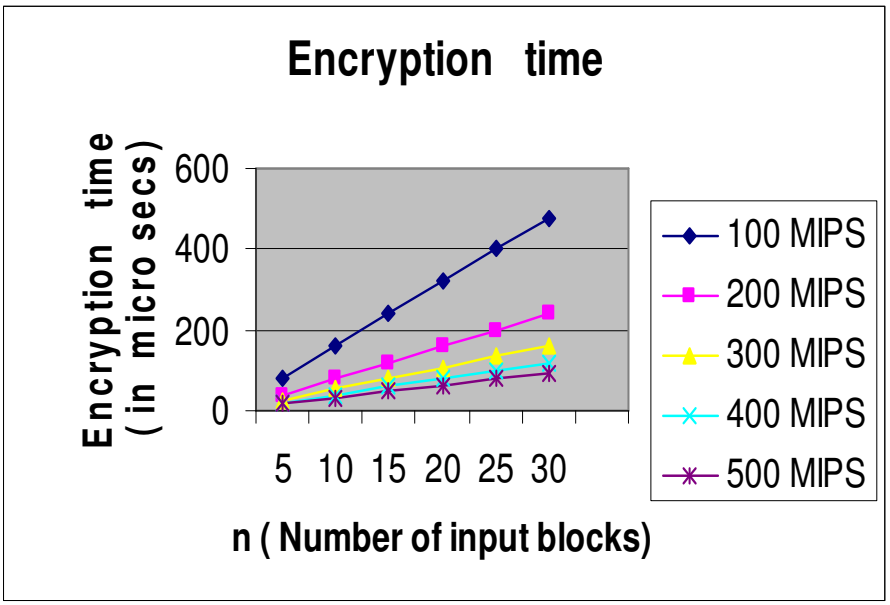

Figure 5: Encryption time (in μ sec) as a function of number of packets for different processing speeds (MIPS).

To draw comparison between the computational cost of encryption and authentication, a graph is drawn with number of operations and number of packets as inputs.

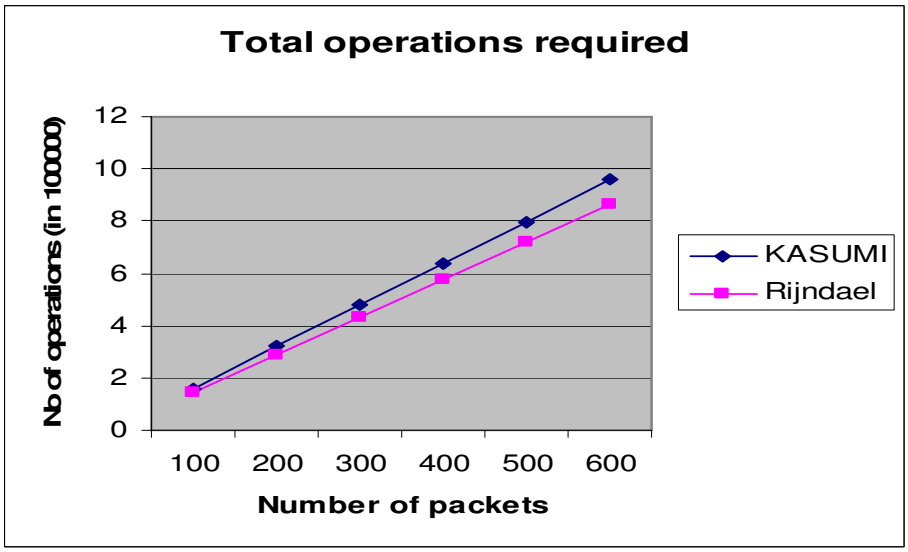

Figure 6: Number of operations required as a function of packet size

The above graph clearly shows that number of operations in case of encryption is more as compared to authentication.

4. THROUGHPUT

Throughput is defined as the number of bits in one time unit and is measured in Mbps [10].

4.1 Throughput of 2G

4.1.1 ThroughputA3A8

n blocks require tA3A8 (in μ sec) time period for authentication for a given Cp.

Therefore, in 1sec = (n*128 bits) ÷ tA3A8 (in μ sec)

4.1.2 ThroughputA5/1

n blocks require tA5/1 (in μ sec) time period for encryption for a given Cp.

Therefore, in 1sec = (n*114 bits) ÷ tA5/1 (in μ sec)

4.2 Throughput of 3G

4.2.1 Throughput$_{kasumi}$

n blocks require t_{kasumi} (in μ sec) time period for encryption for a given Cp.
Therefore, in 1sec = (n*64 bits) ÷ t_{kasumi} (in μ sec)

4.2.2 Throughput$_{rijndael}$

n blocks require $t_{rijndael}$ (in μ sec) time period for authentication for a given Cp.
Therefore, in 1sec = (n*128 bits) ÷ $t_{rijndael}$ (in μ sec)

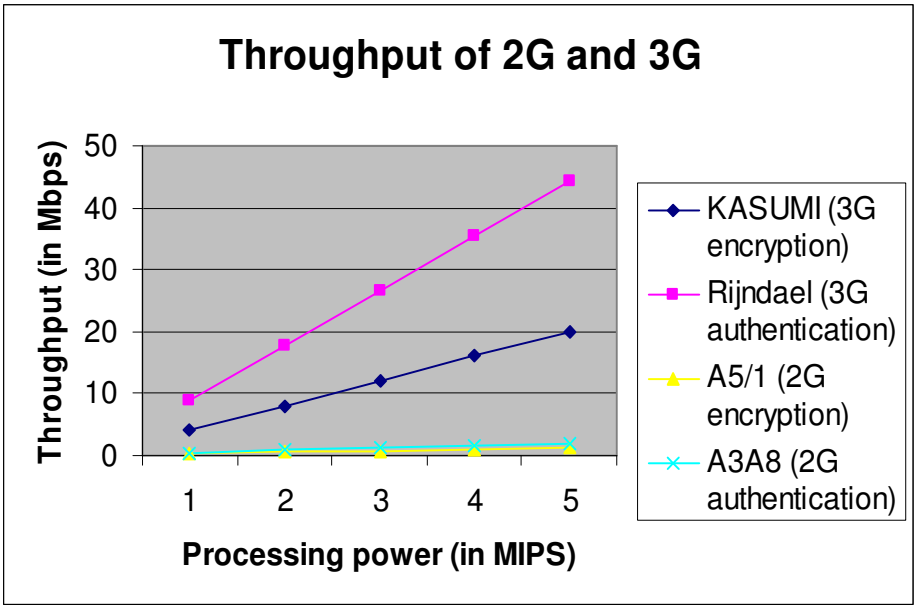

Figure 7: Throughput (in Mbps) of 2G and 3G (authentication and encryption algorithm) as a function of processing speed (in MIPS)

The number of operations for 2G authentication and encryption are 32,288 and 43,752 respectively. The encryption requires more number of operations as compared to authentication for same number of input blocks and same processing speed in MIPS. This is very obvious from the figure1, 2 and 3. Similarly in 3G, from figure 6, it is clear that the number of operations for authentication is less as compared to encryption. For one block of authentication 1441 operations are required and for one block of encryption 1596 operations are required. Therefore, time taken for authentication is less as compared to encryption for the same number of input blocks and same processing speed.

The throughput is the number of bits in one time unit. So, more are the number of operations, more is the processing time required, lesser is the bits in one time unit and hence lower throughput. Figure 7 shows authentication and encryption algorithms of 3G provides higher throughput as compared to 2G authentication and encryption algorithms. Even though 3G algorithms are more complex and provides certain enhanced features like two way authentication and integration key based more secure encryption, throughput of 3G is still high as the algorithm is more efficient as compared to 2G.

5. FUTURE TRENDS

This work can be further extended to 4G in near future. Though, 4G algorithms (as the predicted date for 4G [7] is given as 2010) will be available after 4G standardized documentation is made available. In 4G, heterogeneity will be the rule instead of exception and it would be of paramount importance to identify and explore the different issues and challenges related to mobility management in 4G. A seamless handoff should be supported between different interfaces like WMAN (using WiMax standard), WPAN (using Bluetooth), WLAN (using WiFi). A study of 802.11, 802.16 and 802.15 standards would be required for ensuring seamless mobility [19, 20].

While shifting from 2G to 3G, to acquire high speed transmission, improved voice quality, global roaming and service flexibility(which means both services – circuit and packet switching), first and the foremost challenge is, interoperation between 2G and 3G. Both the systems use different key lengths. After 3G authentication, the USIM and the SN/HE uses 128 bit cipher and integrity keys CK and IK whereas 2G uses 64 bit cipher key Kc. Therefore, certain conversion functions are needed, that convert the 3G keys to 2G length and vice versa [17].

Except for the transformation complexity and the processor capabilities, the real time required for a packet to be protected may depend on the overall system load as well. Security services not only have significant impact on the system throughput, but security services may further delay data transfer. The mean end to end delay values can be found out as a function of mean data rate for various security scenarios and MS processing capabilities. The mean packet delay is least for unprotected data flow and may vary differently for different algorithms.
Security services also affect mean buffer size. One of the main reason that causes system performance degradation is the packet congestion at the MS because of the computational complexity of the security tasks executed as well as its limited processing capabilities [18]. The mean buffer size at the MS may be calculated as the function of mean data rate for data protection algorithms.

6. SUMMARY AND CONCLUSION

The evolution of the security in mobile systems signifies a shift towards open and easily accessible network architecture, which raises major security concerns. The main thrust of research is to develop security which is secure and efficient (in terms of time overhead and space overhead). The time required for security transformation increases proportionally with the required number of operations, but it also involves the processor capabilities. Since the numbers of operations are greater for encryption than authentication both in 2G and 3G, throughput for encryption is low compared to authentication as encryption consumes significantly more processing resources compared to authentication.
The time required for authentication is less as compared to encryption in both 2G and 3G respectively. However, throughput of 3G for both authentication and encryption is higher than that of 2G. 2G requires more number of processing resources as compared to 3G.The mobile companies are shifting from 2G to 3G for the following reasons:

i. Higher throughput of 3G as compared to 2G
ii. 3G is more secure than 2G. 3G offers two-way authentication i.e. not only network authenticates mobile equipment, mobile equipment also authenticates network, so as to overcome fraud base station attack.
iii. Higher data transfer bandwidth incase of 3G.

To reduce computational overheads encryption should be used in critical user information only and not for regular traffic flow. Encryption if needed should be combined with authentication. In this case if the message fails authentication, decryption process is saved (not performed).
Further the performance analysis determines the cost (in terms of time complexity and throughput). Quantifying the security overhead makes mobile users and mobile network operators aware of the price of added security features and further helps in making optimized security policy configurations.
Finally, except for the transformation complexity and the processor capabilities, the real time required for a packet to be protected depends on the overall system load and traffic conditions as well.

7. REFERENCES

1. Lauri Pesonen "*GSM Interception*", lecture notes, Helsinki University of technology, Lauri.Pesonen@iki.fi, 1999.

2. Paulo S. Pagliusi "*A contemporary foreword on GSM Security*", Lecture notes, Royal Holloway, University of London, UK, http://www.isg.rhul.ac.uk

3. Chengyuan Peng, "GSM and GPRS Security", Helsinki university of technology, IIUT TML 2000, TIK 110.501 Seminar on network security.

4. Stefan Pitz, Roland Schmitz, Tobias Martin,"*Security mechanisms in UMTS*", Datenschutz und Datensicherheit (DUD), vol. 25, pp 1-10. 2001.

5. Christos Xenakis, Lazaros Merakos, "*Security in 3G Mobile network*", Computer communications, vol. 27, pp 638-650, 2004.

6. 3GPP TS 33.102 (v3.12.0), " *3G Security: Security Architecture*", Release '99, June 2002.

7. Jun- Zhao Sun, Jaakko Sauvola, Douglas Howie " *Features in Future: 4G visions from a technical perspective* " , IEEE, 0-7803-7206-9/01, pp 3533-3537, 2001.

8. Suk Yu Hui and Kai Hau Yeung " *Challenges in the Migration to 4G Mobile Systems*", IEEE Communications Magazine, Dec 2003.

9. Christos Xenakis, Lazaros Merakos, "IPsec *based end_to_end VPN deployment over UMTS*", Computer Communications vol. 27, pp.1693-1708, May 2004.

10. O. Elkeelany, M. Matalgah, K. Sheikh, M. Thaker, G. Chaudhry, D. Medhi, J. Qaddouri, "*Performance analysis of IPSec protocol: encryption and authentication*", Proc. IEEE Int'l Conf. Communications, New York, NY, pp. 1164-1168, April-May 2002.

11. Marc Briceno, Ian Goldberg, David Wagner, "*An implementation of GSM A_3, A_8 algorithm*", http://www.scard.org/gsm/a3a8, 1999.

12. Ross Anderson, " *A_5 The GSM Encryption Algorithm*", sci.crypt, 1994.

13. 3GPP TS 35.205 (v.1.0), " *Specification of Milenage algorithm for the 3GPP authentication and key generation functions*", Nov 2000.

14. 3GPP TS 33.105 (v4.1.0), "3G *security: cryptographic algorithm requirements*", release 4, 2001.

15. 3GPP TS 35.201 (v.1.0), "*Specification of 3GPP confidentiality and integrity algorithm*", Document 1: f_8, f_9 specification, Dec 1999.

16. ARM microprocessor solutions from ARM Ltd, http://www.arm.com/products/CPUs.

17. 3GPP, [TR 31.900] . "*Interworking between 2G and 3G*" , V 5.1.0 , 2002.

18. Qingyang song and Abbas Jamalipour, " *A network selection mechanism for next generation networks*", IEEE-0-7803-8938-7/05, pp1418-1422, July 2005.

19. Pablo Vidales, Javier Baliosian, Joan Serrat, "*Autonomic system for mobility support in 4G networks*", IEEE Journal on selected areas in communications volume 23, No.12, IEEE 0733-8716, pp. 2288-2303, Dec 2005.

20. Chang Wei Lee, Li Ming Chen, Meng Chang Chen, Yeali Sunny Sun, "*A framework of handoffs in wireless overlay networks based on mobile IPV6*", IEEE journal on selected areas in communications, vol 23 No 11, pp 2118-2128, Nov 2005.