Literature Review of Recent, Practical – Oriented Computer Networks Papers

Hasibul Islam
Student ID: 06110006

Hassan Sameer
Student ID: 06110020

Irtiza Ahmad Farooq
Student ID: 09221140

Department of Electrical and Electronics Engineering
Fall '09

BRAC UNIVERSITY, DHAKA

DECLARATION

We hereby declare that this thesis is based on the results found by ourselves. Materials of work found by other researcher are mentioned by reference. This thesis, neither in whole nor in part, has been previously submitted for any degree.

17 Dec, 2009

Signature of Supervisor

Signature of Author

Hassan Sameer

Habibul Islam

Ittiza Farooq

ACKNOWLEDGMENTS

Special thanks to Nazmus Saquib, Rumana Rahman, Apurba Saha, and to Dr. Al Sakib Khan Pathan and Tarem Ahmed of Electrical and Electronics Department of BRAC University for accepting the difficult task of overseeing this work to completion and to the members of Advisory Committee for taking time out of their busy schedules to consider this work.

ABSTRACT

This thesis will include a literature review of recent practical oriented computer networks papers in premier IEEE conferences. The objective of the thesis is to provide detailed plans for a number of computer network related projects that may be implemented by subsequent BRAC University students. We will do an in-depth study of the selected topics and provide a step by step implementation process.

TABLE OF CONTENTS

LIST OF TABLES

1.0. OBJECTIVE

The objective of our research is to unearth thesis ideas and provide direction to future BRAC University students which will help them in choosing a thesis topic and provide them with guidance on how to finish their practical and theoretical report.

2.0. PROJECT OVERVIEW

In this project we went through different thesis papers which have been published and are related to computer networks. From those papers we sorted the topics that are applicable in Bangladesh and can be implemented in real life.. We faced trouble in choosing our thesis topic. When a student get admitted to the University, he/she attends an orientation program where he learns about the rules & regulation, course outline, grading system and other important things. But regarding thesis, students don't get enough information which makes it difficult for them to choose a practical topic. For that reason, with our supervisor's help we came up with the idea of doing our thesis on selecting do-able topics which are feasible in our country's context. Among these thesis papers, we are suggesting the best topics in the end and we are also providing a detail implementation process which will help the students to work on the topic in future. Computer network offers huge scope of study and we tried to choose the topics with which our fellow students are well aware of. Our suggested topics are stated below:

- A Proposal For Enhancing The Security System Of short Message Service In GSM
- Bluetooth Performance Analysis In Personal Area Network (PAN)
- Cluster Mobile Switching Center For Third Generation Wireless Systems
- Real – Time Monitoring And Filtering System For Mobile SMS
- A Student ID System Using a Cell Phone and Its Evaluation
- Traffic Capacity Performance of a CT2Plus Based Wireless PABX

3.0. CHALLENGES AND SOLUTIONS

Our biggest challenge was to gather thesis papers. We knew that the best place to look for these papers is the IEEE website. However, it is a private organization, not everyone could log on to their website. We have solved this problem by logging in from BRAC University lab as BRAC University is an authorized member of IEEE.

As we know Computer Networking has a huge scope to study, so we found a wide variety of topics to choose from. Thus it was another challenge for us to select the appropriate topics for the students of BRAC University. As a solution, first we categorize few basic sectors of computer network such as wireless communication, short message service, 3G etc, and selected around 50 (fifty) thesis papers under these categories. After that, with the help of our instructor, we have short listed the best possible topics.

4.1.0. A Proposal for Enhancing the Security System of Short Message Service in GSM

4.1.1. INTRODUCTION

At present mobile communication is the top most form of communication in our nation. Each and every citizen of every social class has been using such wireless communication in a personal basis for the last 10 years. However, now wireless communication is becoming the major form of communication in business world as well. Therefore it is time to think about strengthening the security measures of wireless communication.

From the various services that we get from wireless communication, Short Message Service is perhaps used the most. Thus we can deduce that SMS will play a vital role when wireless communication will be an important tool in the business sector of our country. Therefore this paper is presenting a proposal for enhancing the security system of Short Message Service in GSM.

In SMS system, two parties exchange alphanumeric messages via a wireless line. SMS is a part of GSM networks that allows the alphanumeric message up to 160 characters to be sent and received via the network operator's SMS center to the mobile subscribers. If the subscriber is not reachable, then SMS are stored in the GSM operator's SMS center and delivered when it is reachable.

In the existing system plain texts are transferred through a transmission line, therefore it can be easily read by an unwanted third party. This type of action cannot be allowed when people are using SMS for their business transactions. In this paper, the security of SMS in GSM network has been discussed especially for the use of SMS as such business tool.

Here Encryption can be done with the existing GSM encryption algorithm, A8. Then the encrypted message will create hash and finally it will be digitally signed. This signed encrypted will be transmitted. The proposed scheme will give total authenticity, data integrity, confidentiality, authorization and non-repudiation which are the most essential issues in m-commerce or mobile banking and in secure messaging.

4.1.2. STRUCTURE OF SMS IN GSM SERVICE

The basic structure of SMS in GSM network is shown in Fig. 4.1. Here we have considered the communication between the mobile subscriber and the bank which is providing such m-commerce facilities.

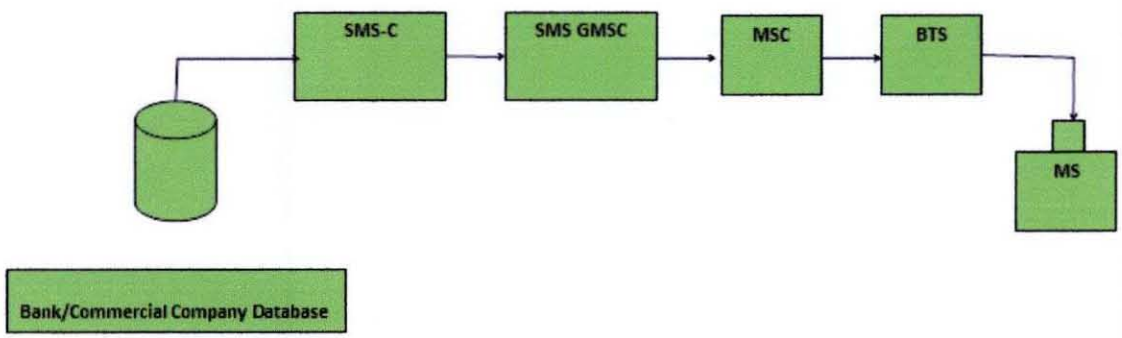


Fig 4.1.1: Existing SMS Architecture in GSM

To explain Fig 4.1.1 completely we can consider two basic services of Short Message Service. They are:

- Mobile Subscriber Originated SMS (MO – SM)
- Mobile Subscriber Terminated SMS (MT – SM)

Mobile subscriber originated SMS means that SMS is sent from MS to a SMS-C. In this process at first the MS is powered on and registered with the

network. Then MS transfers the SM to the MSC. The MSC interrogates the VLR to verify that the message transfer does not violate any supplementary services invoked or the restrictions imposed. Later on the MSC sends the short message to the SMSC using the forward Short Message operation. After that the SMSC delivers the short message to the SME (and optionally receives acknowledgment). The SMSC acknowledges to the MSC about the successful outcome of the forward Short Message operation. Finally the MSC returns the outcome of the MO-SM operation to the MS. Fig. 4.1.2 depicts the successful MO– SM scenario, utilizing the GSM method. The recipient of SMS might be the database system of the bank or any commercial company's database server.

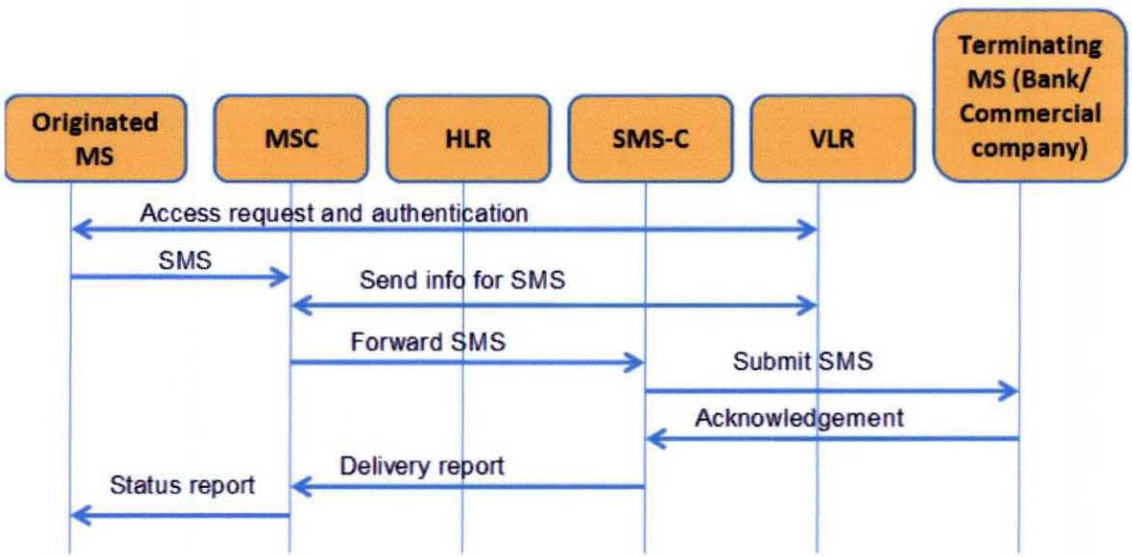


Fig 4.1.2: Mobile Originated SMS (MO – SM)

Mobile Subscriber Terminated SMS means that the SMS communication from SMS-C to an MS. At first the Bank sends the SMS to its SMS-C. SMS-C will then evoke the routing information from the mobile operator's HLR. After knowing the location of the nearest MSC of the MS the SMS-C will forward the SMS to that MSC. MSC after taking the help from its VLR send the SMS to the nearest BSC. BSC will page the MS for telling about the MT-SM. Then authentication procedure will start. After that VLR tells the MSC about the authentication. If the authentication is successful then MSC will forward the SMS to the MS. MS will send an acknowledgment after getting the SMS. The SMS-C will inform the bank about the outcome of the MT-MS operation. Fig. 4.1.3 depicts the successful MT–SM scenario, utilizing the GSM method.

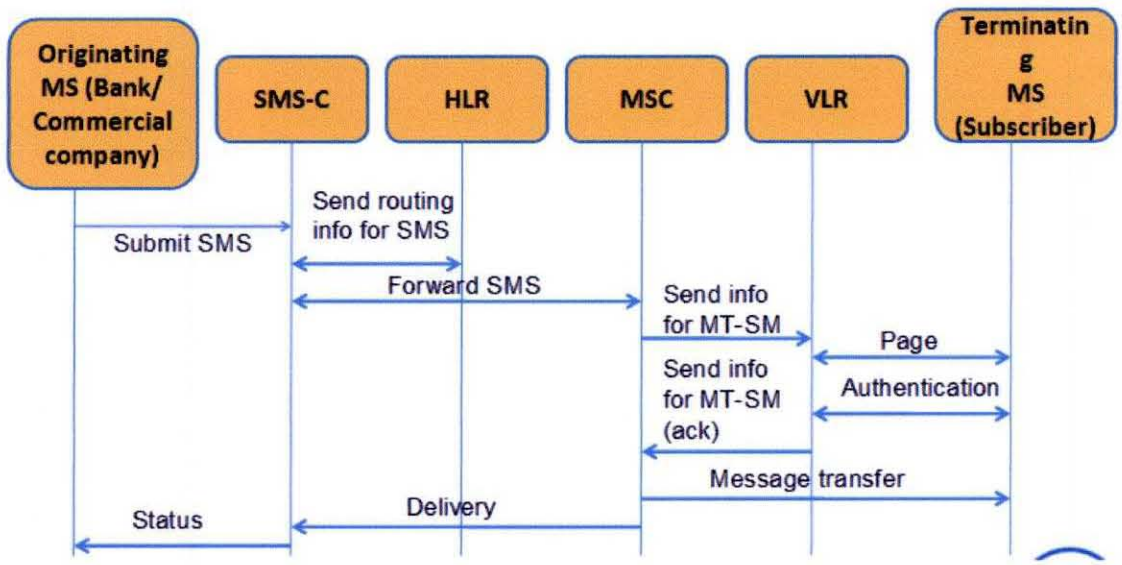


Fig 4.1.3: Mobile Terminated SMS (MT – SM)

The security mechanisms of GSM are implemented in three different system elements; the Subscriber Identity Module (SIM), the GSM handset or MS, and the GSM network. The SIM contains the IMSI, the individual subscriber authentication key (Ki), the ciphering key generating algorithm (A8), the authentication algorithm (A3), as well as a Personal Identification Number (PIN). The GSM handset contains the ciphering algorithm (A5). The encryption algorithms (A3, A5, A8) are present in the GSM network as well. The Authentication Center (AUC), part of the Operation and Maintenance Subsystem (OMS) of the GSM network, consists of a database of identification and authentication information for subscribers. This information consists of the IMSI, the TMSI, the Location Area Identity (LAI), and the individual subscriber authentication key (Ki) for each user. In order for the authentication and security mechanisms to function, all three elements (SIM, handset, and GSM network) are required. This distribution of security credentials and encryption algorithms provides an additional measure of security both in ensuring the privacy of cellular telephone conversations and in the prevention of cellular telephone fraud.

Fig 4.1.4 demonstrates the distribution of security information among the three system elements, the SIM, the MS, and the GSM network. Within the GSM network, the security information is further distributed among the authentication center (AUC), the home location register (HLR) and the visitor location register (VLR). The AUC is responsible for generating the sets of RAND, SRES, and Kc

which are stored in the HLR and VLR for subsequent use in the authentication and encryption processes.

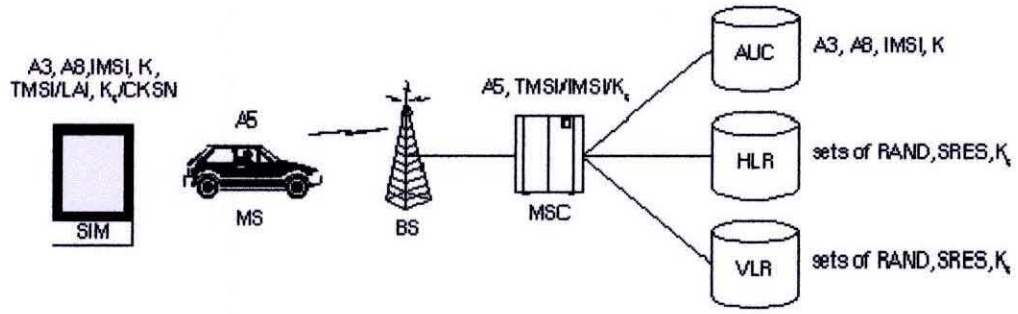


Fig 4.1.4: Distribution of Security Features in the GSM Network

4.1.3. SECURITY BREACH ON SMS FOR M – COMMERCE

When SMS is used for business purposes, there are many threats that can come into account as it will be transmitting confidential information. For Example, sometimes the passwords for a bank account need to be sent. If any intruder read the SMS, he or she can gain the password as it is in plaintext. Encryption technique would be required to solve this problem. The SMS can also be altered or modified. Another problem is repudiation in which case a sender can deny sending his or her SMS. Commercial companies can also deny receiving of the message. Digital signature can provide the solution of these threats. So various threats or attacks can be generalized in 4 ways:

- Interception
- Interruption
- Modification
- Fabrication

4.1.4. PROPOSED SECURITY SCHEME

Our concern is to provide secure end – to – end communication, even keeping the SMS secure from the network operator. For that we will be ciphering the SMS first and then we will impose the digital signature. This signed encrypted SMS will be finally transmitted.

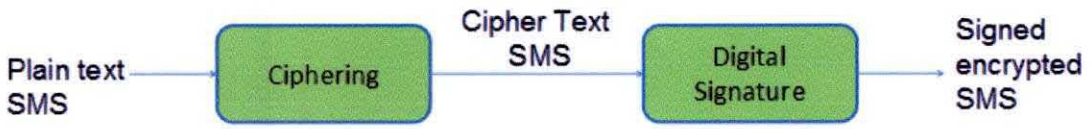


Fig 4.1.5: Proposed Security Scheme for SMS

4.1.4.1 AUTHENTICATION PROCESS

When a MS requests access to the network, the MSC/VLR will normally require the MS to authenticate. The MSC will forward the IMSI to the HLR and request authentication Triplets (Kc, SRES & RAND)

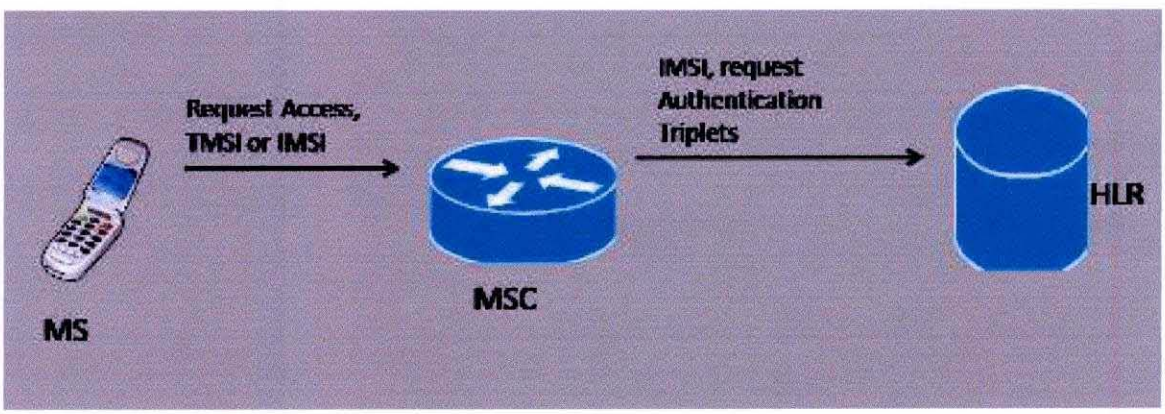


Fig 4.1.6: Request For Authentication

When the HLR receives the IMSI and the authentication request, it first checks its database to make sure the IMSI is valid and belongs to the network. Once it has accomplished this, it will forward the IMSI and authentication request to the Authentication Center (AuC).

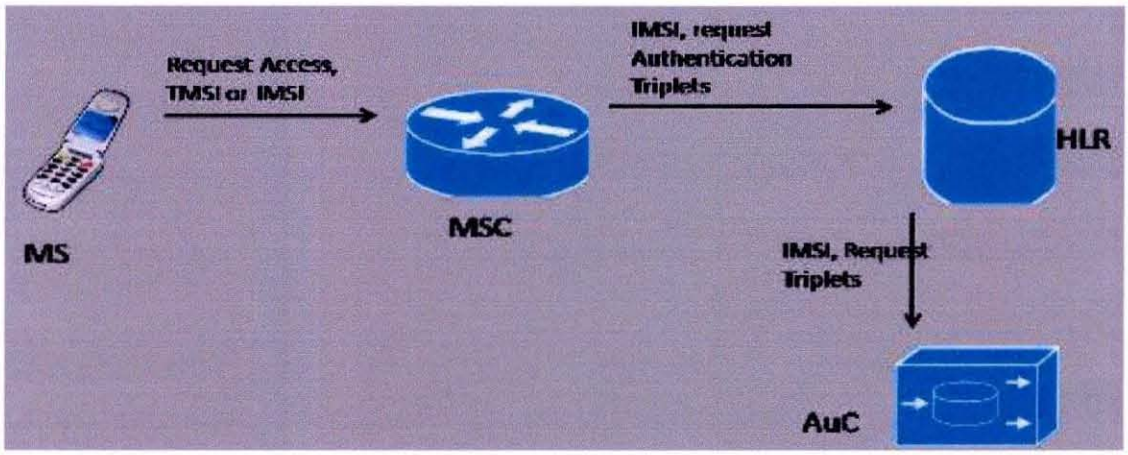


Fig 4.1.7: Checking Validity

The AuC will use the IMSI to look up the K_i associated with that IMSI. The K_i is the individual subscriber authentication key. It is a 128-bit number that is paired with an IMSI when the SIM card is created. The K_i is only stored on the SIM card and at the AuC. The Auc will also generate a 128-bit random number called the RAND.

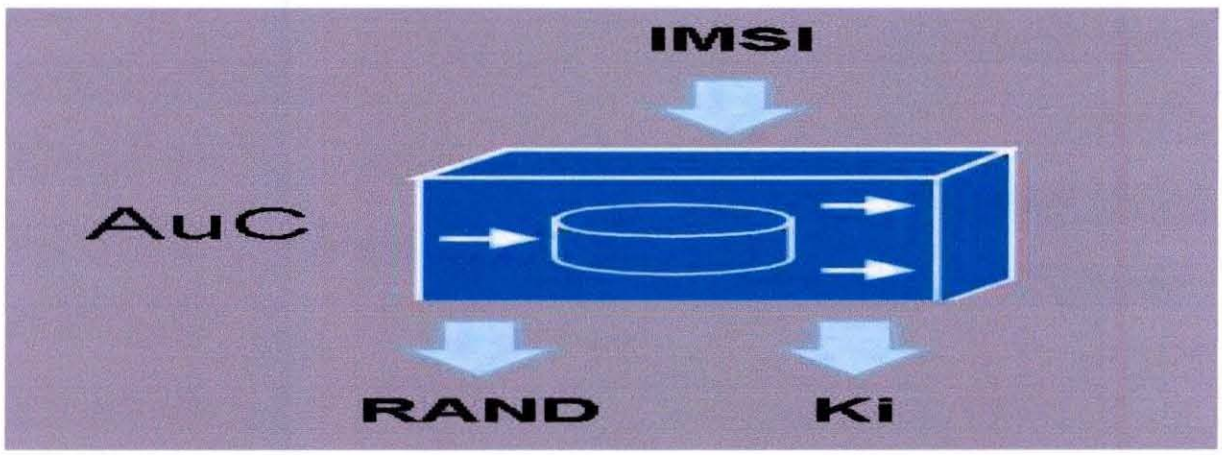


Fig 4.1.8: Generating Random Number

The RAND and the K_i are inputted into the A3 encryption algorithm. The output is the 32-bit Signed Response (SRES). The SRES is essentially the "challenge" sent to the MS when authentication is requested.

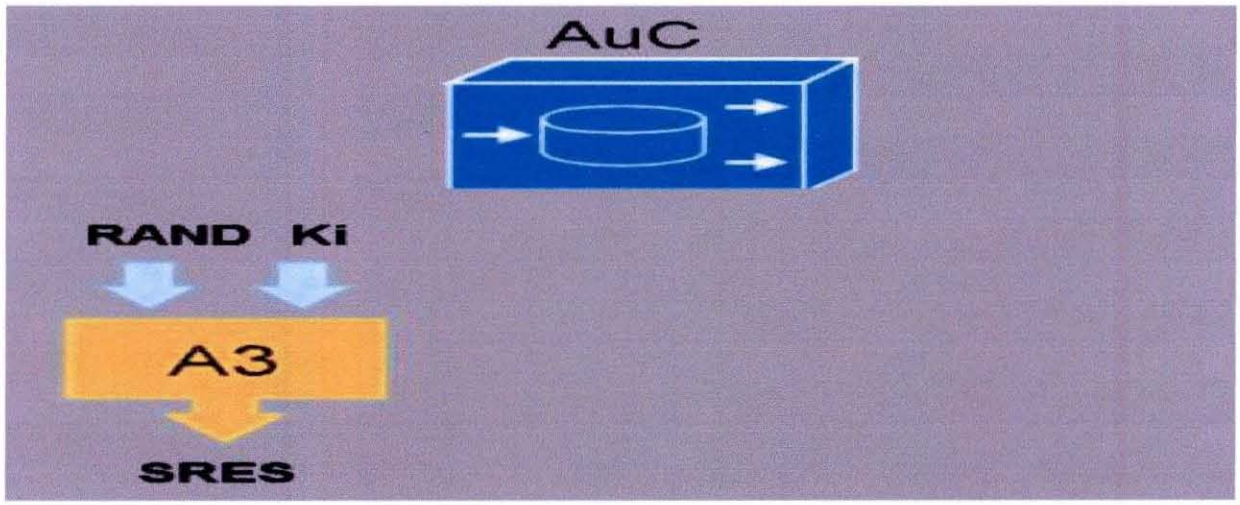


Fig 4.1.9: Generating Signed Response

The RAND and Ki are input into the A8 encryption algorithm. The output is the 64-bit K_c. The K_c is the ciphering key that is used in the A5 encryption algorithm to encipher and decipher the data that is being transmitted on the Um interface.

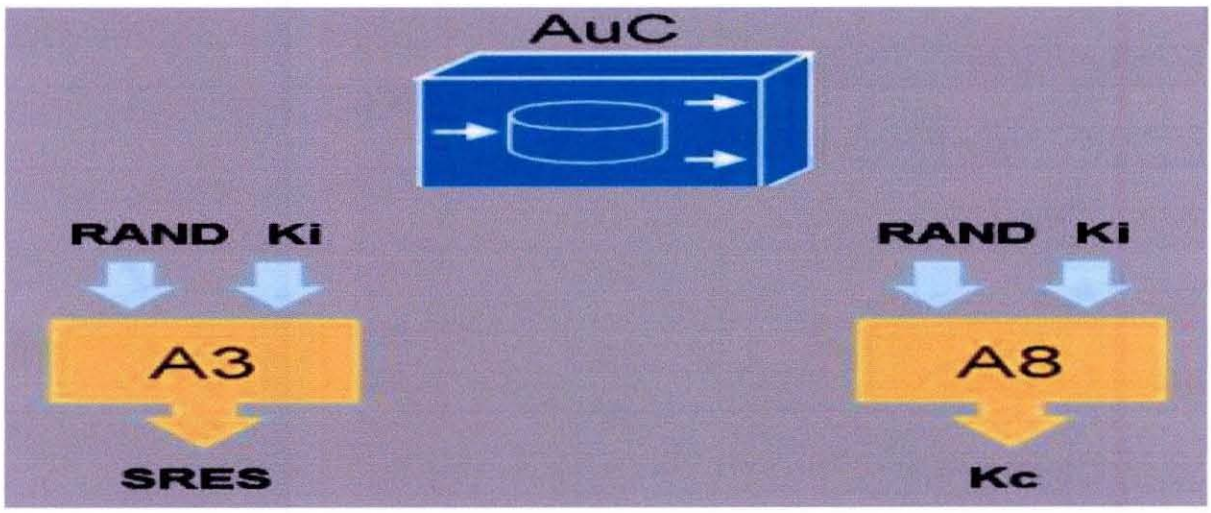


Fig 4.1.10: Generating Ciphering Key

The RAND, SRES, and K_c are collectively known as the Triplets. The AuC may generate many sets of Triplets and send them to the requesting MSC/VLR.

This is in order to reduce the signaling overhead that would result if the MSC/VLR requested one set of triplets every time it wanted to authenticate the. It should be noted that a set of triplets is unique to one IMSI, it can not be used with any other IMSI.

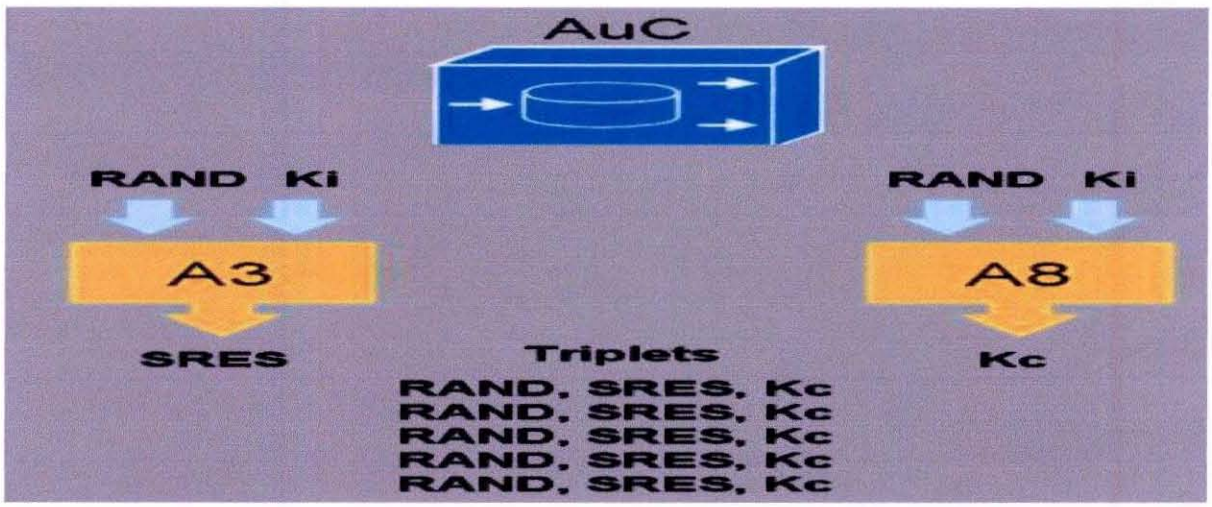


Fig 4.1.11: Triplets

Once the AuC has generated the triplets (or sets of triplets), it forwards them to the HLR. The HLR subsequently sends them to the requesting MSC/VLR.

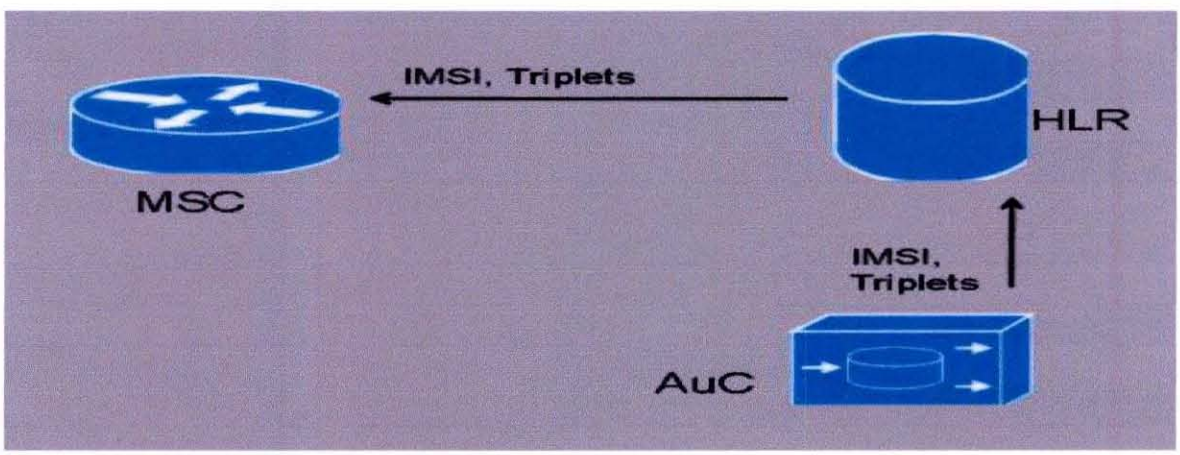


Fig 4.1.12: Forwarding Triplets

The MSC stores the K_c and the SRES but forwards the RAND to the MS and orders it to authenticate.

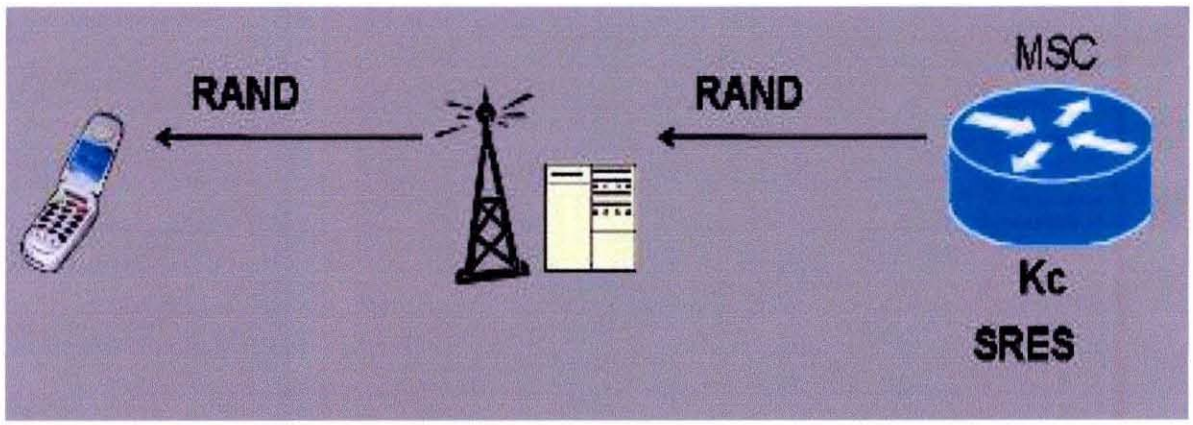


Fig 4.1.13: Request To Authenticate

The MS has the K_i stored on the SIM card. The A3 and A8 algorithms also reside on the SIM card. The RAND and K_i are inputted into the A3 and A8 encryption algorithms to generate the SRES and the K_c respectively.

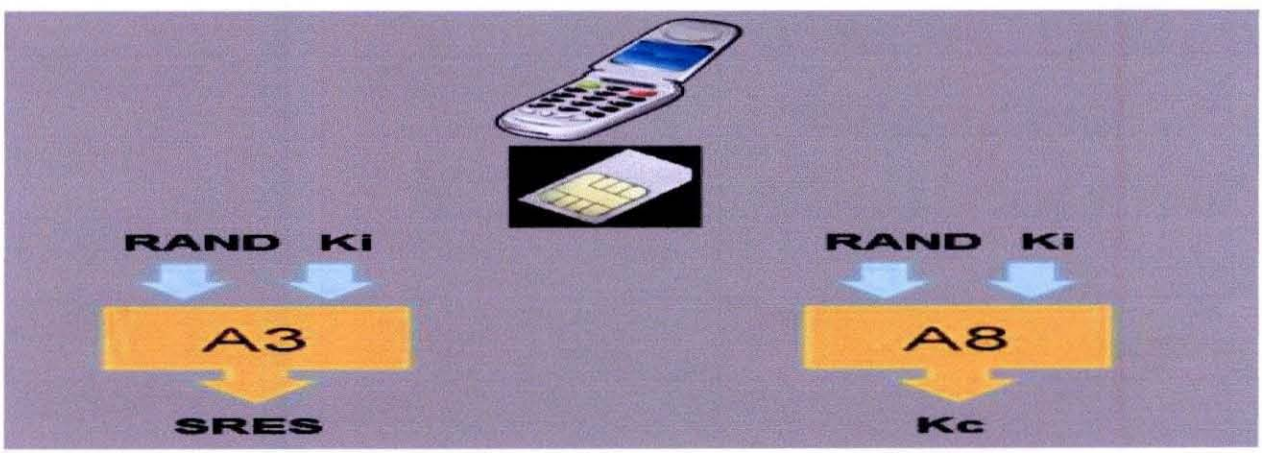


Fig 4.1.14: Generating SRES and K_c in Mobile Equipment

The MS stores the K_c on the SIM card and sends the generated SRES back to the network. The MSC receives the MS generated SRES and compares it to the SRES generated by the AuC. If they match, then the MS is authenticated.

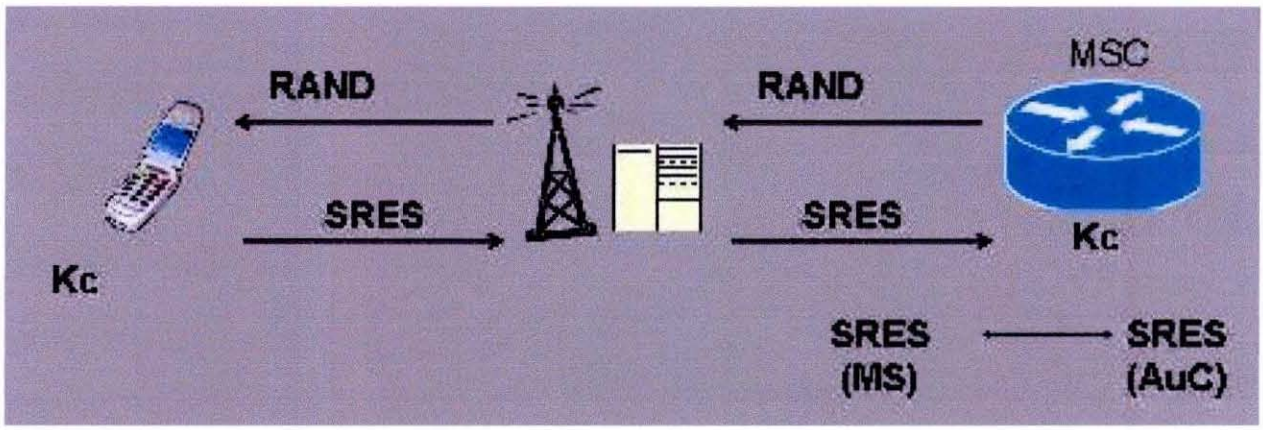


Fig 4.1.15: Matching SRES

4.1.4.2. CIPHERING

The security mechanisms of GSM are implemented in three different system elements. They are:

- Subscriber Identity Module (SIM)
- The GSM handset or MS
- GSM Network

The SIM contains the ciphering key generating algorithm A8 which is used to produce the 64-bit ciphering key (K_c). The ciphering key is computed by applying the same random number (RAND) used in the authentication process to the ciphering key generating algorithm A8 with the individual subscriber authentication key (K_i). The ciphering key (K_c) is used to encrypt and decrypt the data between the MS and BS by the use of the encryption algorithm A5. In our proposal, the first initiate is to make the SMS encrypted by using these existing A8 and A5 algorithm. So no additional algorithm is needed for such encryption. We want to treat the SMS as the voice or data in GSM network.

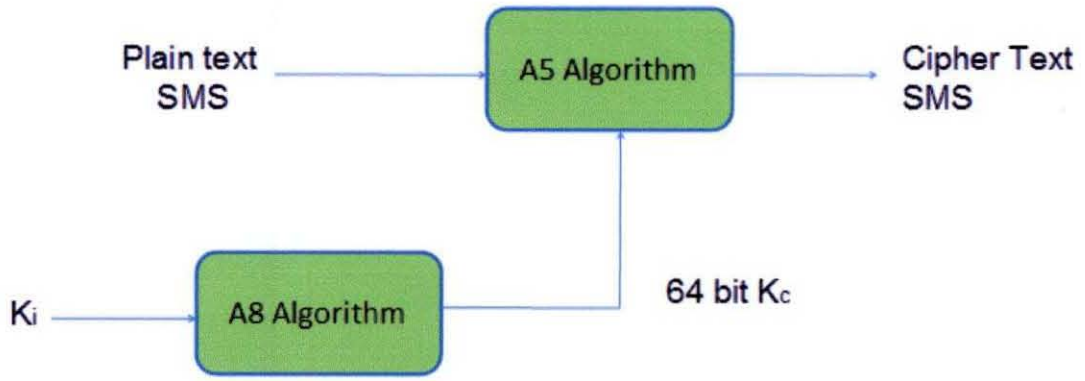


Fig 4.1.16: Ciphering Mechanism for SMS

It is assumed that all the parameters required for this encryption will be provided as per GSM specification. The additional job has to be done by MS. This ciphered SMS will be sent and at the receiver it will be decrypted by the existing procedures. This is the same phenomenon of voice ciphering. This is regularly done in GSM network. So, encryption gives us the data confidentiality, but not the total security solution. Because only cipher can not provide us the data integrity and non-repudiation, we have also proposed the digital signal concept to be incorporated along with this ciphering.

The SIM contains the ciphering key generating algorithm (A8) which is used to produce the 64-bit ciphering key (Kc). The ciphering key is computed by applying the same random number (RAND) used in the authentication process to the ciphering key generating algorithm (A8) with the individual subscriber authentication key (Ki). As will be shown in later sections, the ciphering key (Kc) is used to encrypt and decrypt the data between the MS and BS. An additional level of security is provided by having the means to change the ciphering key, making the system more resistant to eavesdropping. The ciphering key may be changed at regular intervals as required by network design and security considerations. Figure 6 below shows the calculation of the ciphering key (Kc).

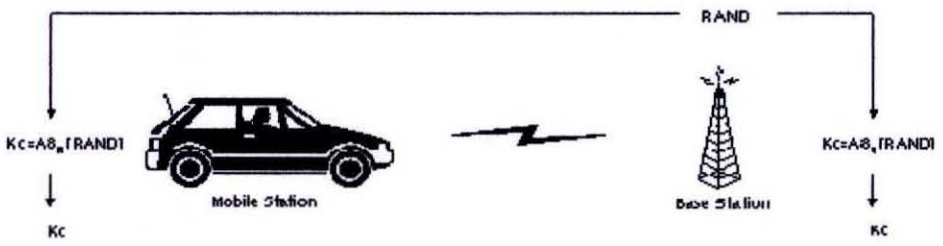


Fig 4.1.17: Ciphering Key Generation Mechanism

In a similar manner to the authentication process, the computation of the ciphering key (Kc) takes place internally within the SIM. Therefore sensitive information such as the individual subscriber authentication key (Ki) is never revealed by the SIM.

Encrypted voice and data communications between the MS and the network is accomplished through use of the ciphering algorithm A5. Encrypted communication is initiated by a ciphering mode request command from the GSM network. Upon receipt of this command, the mobile station begins encryption and decryption of data using the ciphering algorithm (A5) and the ciphering key (Kc). Fig 4.1.18 below demonstrates the encryption mechanism.

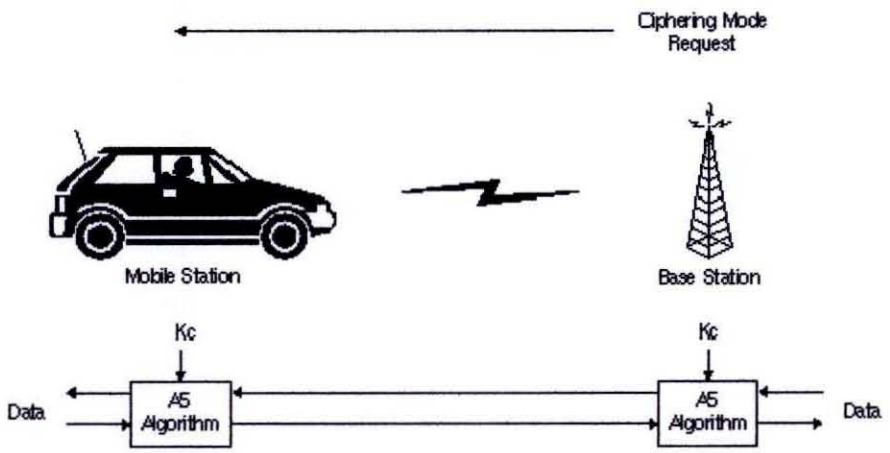


Fig 4.1.18: Ciphering Mode Initiation Mechanism

4.1.4.3 DIGITAL SIGNATURE

Message integrity means that the message has not been altered or destroyed by any attackers. And non-repudiation means that a receiver must be able to prove that a received message came from a specific sender. The sender must not be able to deny sending a message that he or she, in fact, did send. Digital signature will provide us this security service. So we need digital signature after ciphering the plaintext SMS. In this research, Secured Hash Algorithm (SHA-1) has been incorporated as digital signature. For this SHA-1 we need some (mentioned below) additional keys as SHA-1 is known as public key signature.

Ka : private key for signing message

Kb : public key for verifying message

The existing Ki is stored in SIM. The key Ka is also considered to be stored in SIM. And Kb is stored and maintained in a verification key database.

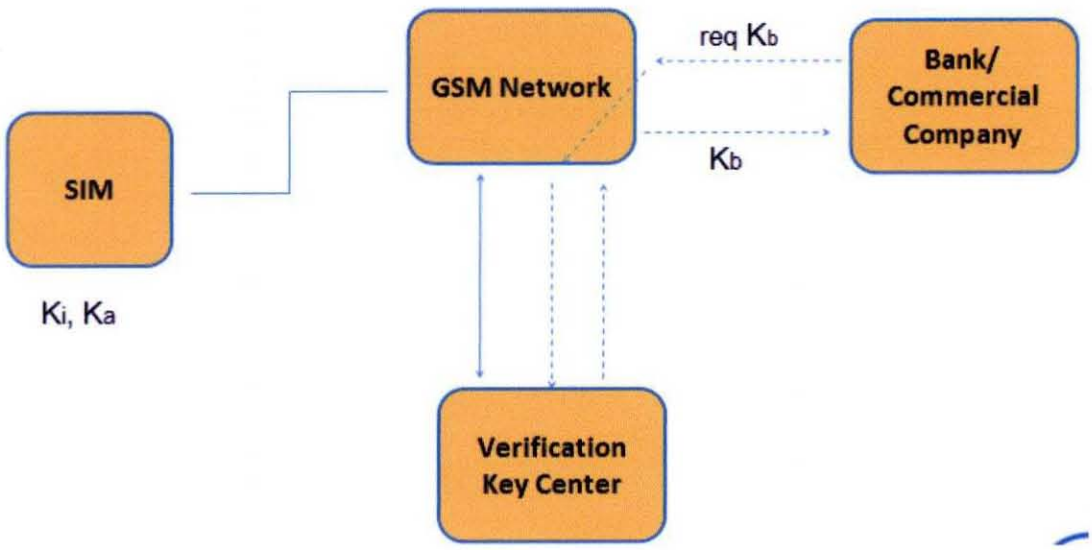


Fig 4.1.19: Keys Needed For Digital Signature

The encrypted SMS will be signed by the Ka. This signed encrypted message along with the encrypted message itself will be sent to the GSM network. In digital signing, at first the encrypted message (E) is fed into the SHA-1 algorithm to get a 160 bit SHA-1 hash (H). Then the RSA (Rivest, Shamir & Adleman) algorithm will sign the hash (DA(H)). The subscriber will send both the signed hash (DA(H)) and the encrypted message (E) to the bank/commercial company via the GSM network. The processes are depicted in Fig.4.1.7.

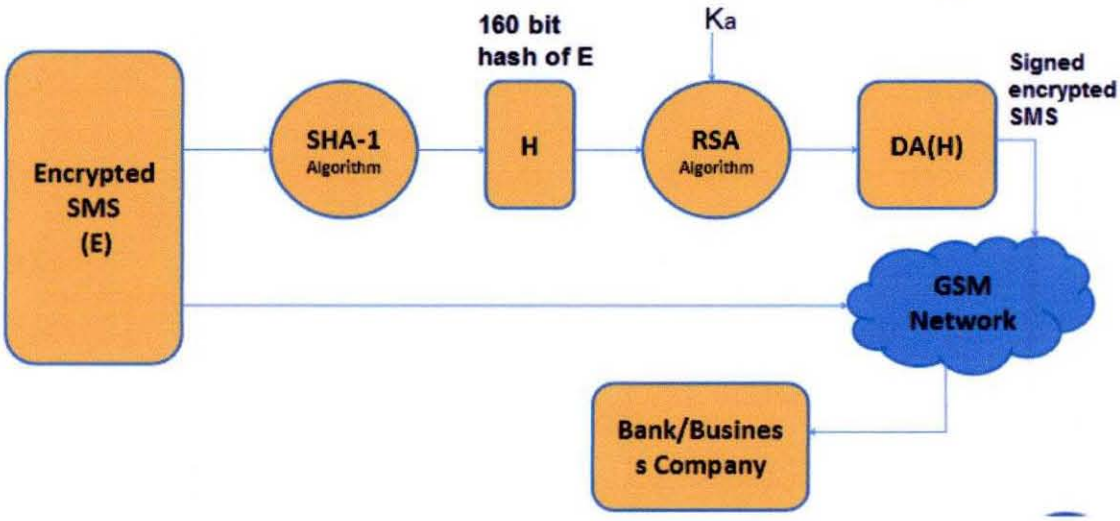


Fig 4.1.20: Digital Signature Mechanism For SMS (Transmitting End)

4.1.4.4. VARIFYING THE DIGITAL SIGNATURE

At the receiver end, bank's server will send a request to get a corresponding Kb from verification key center. Then signed and unsigned E will be separated. Now applying the Kb on the signed message, receiver will decrypt it. It will also make a hash of the unsigned encrypted SMS (E). This operation will give H1. Then H and H1 will be compared (see Fig. 4.1.8). If H and H1 are matched each other it assures that message has been verified as original. That means four measures of security (authenticity, authorization, integrity and non repudiation) are preserved. But if H and H1 are not same, then it can be said that there must be some data modification or alteration. This comparison also gives the guarantee that the transmission of SMS has been done by the true sender and received by the true receiver. The comparison also clarifies that the sender can never deny the SMS sending since he/she can not deny the signature.

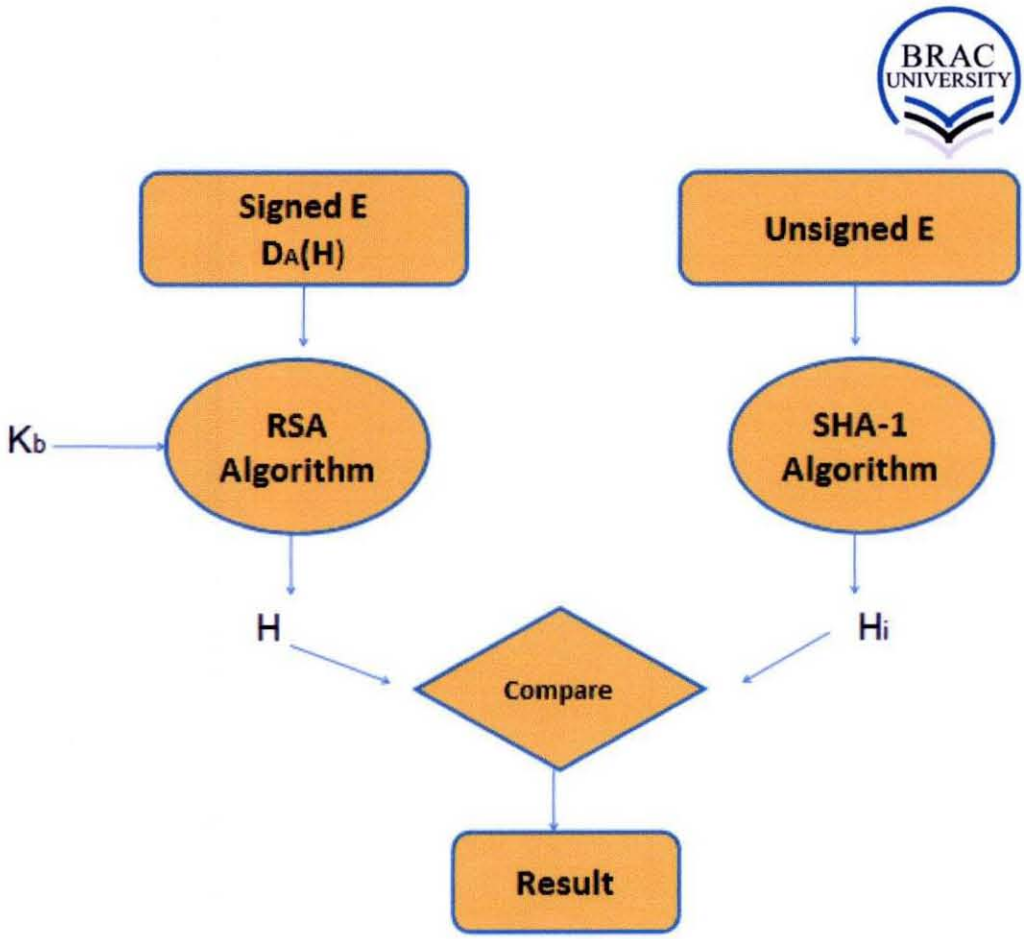


Fig 4.1.21: Verifying The Digital Signature For SMS (Receiving End)

4.1.4.5. Deciphering SMS

After verifying the SMS, the receiver will decrypt it by using the ciphering key Kc by the help of existing GSM decryption algorithm (A5) (that is done for voice communication). Finally, we get the original plain text of SMS.

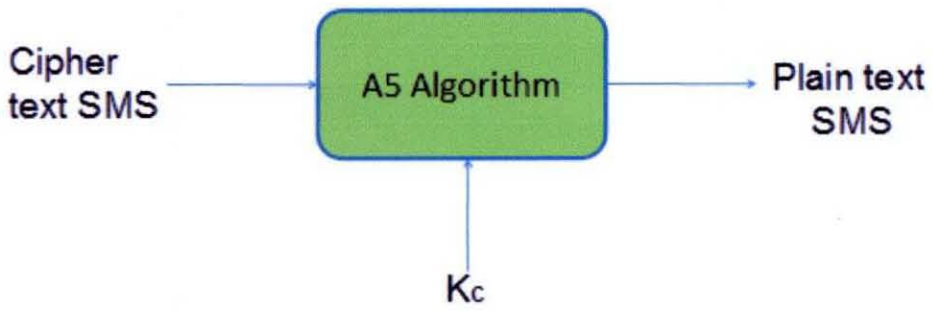


Fig 4.1.22: Decryption Of SMS

So **AT A GLANCE:**

At the Transmitter,

- Kc = A8(Ki)
- E = A5(M)Kc
- H = SHA-1(E)
- DA(H) = RSA (H)Ka
- E and DA(H) will be sent

At the Receiver,

- H = RSA (DA(H))Kb
- H1 = SHA-1(E)

If H & H1 are matched then
- M = A5(E)Kc

If H & H1 are not matched then the message will be rejected

4.1.5. ANALYSIS OF OUR PROPOSED SCHEME

The limited memory capacity of SIM and the slow processing power of MS have to be considered. Another thing we have to consider that the secured SMS communication should be real time or should have a minimal accepted delay. That's why instead of using any new algorithm for ciphering we can use the existing A5 algorithm. For the digital signature, RSA algorithm has been proposed as it's the one of the best public key algorithm. But it takes much for processing. In the key selection, for A5, Kc (which is 64 bit) has been used. Ka and Kb both are 1024 bits because it's the minimum requirement for the RSA to be worked better. In our scheme, some overhead of the SMS will be included while transmitting. This will limit the maximum characters can be sent as 130 instead of 160. Although, for future banking, the 130 characters are sufficient enough. In our proposal, no hardware implementation is needed. All proposals can be served by the software or system modification.

In the future, the use of SMS will have verities of dimensions such as for m-commerce, m-banking etc due to its cheapness and availability. For these feasible future businesses through SMS, we have to provide the total security of it. In this paper, we have proposed a security scheme that will improve the security of SMS. In the proposal, the plain SMS will be encrypted first, and then it

will be digitally signed by the public key infrastructure. So by these themes, we can achieve a total SMS security solution.

4.1.6. IMPORTANT KEYWORDS

Authentication - Whenever a MS requests access to a network, the network must authenticate the MS. Authentication verifies the identity and validity of the SIM card to the network and ensures that the subscriber is authorized access to the network.

Encryption - In GSM, encryption refers to the process of creating authentication and ciphering crypto-variables using a special key and an encryption algorithm.

Ciphering - Ciphering refers to the process of changing plaintext data into encrypted data using a special key and a special encryption algorithm. Transmissions between the MS and the BTS on the Um links, are enciphered.

Ki - The Ki is the individual subscriber authentication key. It is a 128-bit number that is paired with an IMSI when the SIM card is created. The Ki is only stored on the SIM card and at the Authentication Center (AuC). The Ki should never be transmitted across the network on any link.

RAND - The RAND is a random 128-bit number that is generated by the Auc when the network requests to authenticate a subscriber. The RAND is used to generate the Signed Response (SRES) and Kc crypto-variables.

Signed Response - The SRES is a 32-bit crypto-variable used in the authentication process. The MS is challenged by being given the RAND by the network. The SRES is the expected correct response. The SRES is never passed on the Um (Air) interface. It is kept at the MSC/VLR, which performs the authentication check.

A3 Algorithm - The A3 algorithm computes a 32-bit Signed Response (SRES). The Ki and RAND are inputted into the A3 algorithm and the result is the 32-bit SRES. The A3 algorithm resides on the SIM card and at the AuC.

A8 Algorithm - The A8 algorithm computes a 64-bit ciphering key (Kc). The Ki and the RAND are inputted into the A8 algorithm and the result is the 64-bit Kc. The A8 algorithm resides on the ISM card and at the AuC.

Kc - The Kc is the 64-bit ciphering key that is used in the A5 encryption algorithm to encipher and decipher the data that is being transmitted on the Um interface.

A5 - The A5 encryption algorithm is used to encipher and decipher the data that

is being transmitted on the Um interface. The Kc and the plaintext data are inputted into the A5 algorithm and the output is enciphered data. The A5 algorithm is a function of the Mobile Equipment (ME) and not a function of the SIM card. The BTS also makes use of the A5 algorithm.

Triplets - The RAND, SRES, and Kc together are known as the Triplets. The AuC will send these three crypto-variables to the requesting MSC/VLR so it can authenticate and encipher.

4.2.0. Bluetooth Performance Analysis in Personal Area Network (PAN)

4.2.1. INTRODUCTION

One of the fastest methods for file transfer is via wireless communication. We know that at present we have various highly efficient methods of wireless communication. Among them, for a short distance file transfer, using a Bluetooth device is the most renowned system. We can see examples of Bluetooth on tools that we use in our daily life. Some of those devices are:

- Cell Phone
- Laptop
- Personal Digital Assistant (PDA)

Bluetooth is a telecommunications industry specification operating in a frequency band of 2.4 GHz. With the help of this technology different devices can be easily interconnected using a short range wireless connection. Bluetooth devices can form small networks called piconets which can work up to 8 meters. A piconet application which connects several devices that a person carries around in his everyday life creates a network which is called Personal Area Network (PAN).

Bluetooth system provides duplex transmission based on slotted time division duplex (TDD). Time-Division Duplex (TDD) is the application of time-division multiplexing to separate outward and return signals. It emulates full duplex communication over a half duplex communication link. Time division duplex has a strong advantage in the case where the asymmetry of the uplink and downlink data speed is variable. As the amount of uplink data increases, more bandwidth can dynamically be allocated to that and as it shrinks it can be taken away. Another advantage is that the uplink and downlink radio paths are

likely to be very similar in the case of a slow moving system. This means that techniques such as beam forming work well with TDD systems.

Bluetooth operating range of 10 meters or less exceeds the current range of Infrared (IR) technology but falls far short of other wireless networks. Table 5.1 summarizes the comparison between existing wireless technologies in the market nowadays.

Table 4.2.1: Summery of Technology Comparison

	Infrared	Bluetooth	Wireless
Range (m)	1	10	100
Rate (Mbps)	1	1	3
Networked	No	Yes	Yes
Frequency Band	90 nm light	2.4 GHz	2.4 GHz

4.2.2. BASIC OVERVIEW

Bluetooth uses a radio technology called frequency-hopping spread spectrum, which chops up the data being sent and transmits chunks of it on up to 79 frequencies. In its basic mode, the modulation is Gaussian frequency-shift keying (GFSK). It can achieve a gross data rate of 1 Mb/s. Bluetooth provides a way to connect and exchange information between devices such as mobile phones, telephones, laptops, personal computers, printers, Global Positioning System (GPS) receivers, digital cameras, and video game consoles through a secure, globally unlicensed Industrial, Scientific and Medical (ISM) 2.4 GHz short-range radio frequency bandwidth.

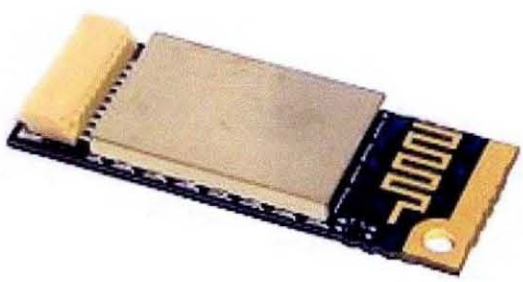


Fig 4.2.1: Bluetooth Card Circuit

A master Bluetooth device can communicate with up to seven devices in a Wireless User Group. This network group of up to eight devices is called a

piconet. A piconet is an ad-hoc computer network, using Bluetooth technology protocols to allow one master device to interconnect with up to seven active devices. Up to 255 further devices can be inactive, or parked, which the master device can bring into active status at any time. At any given time, data can be transferred between the master and one other device, however, the devices can switch roles and the slave can become the master at any time. The master switches rapidly from one device to another in a round-robin fashion. The Bluetooth specification allows connecting two or more piconets together to form a scatternet, with some devices acting as a bridge by simultaneously playing the master role in one piconet and the slave role in another. Any device may perform an inquiry to find other devices to connect to, and any device can be configured to respond to such inquiries.

However, if the device trying to connect knows the address of the device, it always responds to direct connection requests and transmits the information shown in the list above if requested. Use of a device's services may require pairing or acceptance by its owner, but the connection itself can be initiated by any device and held until it goes out of range. Some devices can be connected to only one device at a time, and connecting to them prevents them from connecting to other devices and appearing in inquiries until they disconnect from the other device.

Every device has a unique 48-bit address. However, these addresses are generally not shown in inquiries. Instead, friendly Bluetooth names are used, which can be set by the user. This name appears when another user scans for devices and in lists of paired devices.

Most phones have the Bluetooth name set to the manufacturer and model of the phone by default. Most phones and laptops show only the Bluetooth names and special programs are required to get additional information about remote devices. This can be confusing as, for example, there could be several phones in range named T610.

More prevalent applications of Bluetooth include:

- Wireless control of and communication between a mobile phone and a hands-free headset.
- Wireless communication with PC input and output devices.
- Transfer of files, contact details, calendar appointments, and reminders.
- Replacement of traditional wired serial communications in test equipment, GPS receivers, medical equipment, bar code scanners and traffic control devices.
- For controls where Infrared were traditionally used.

- For low bandwidth applications where higher bandwidth is not required and cable free connection desired.
- Wireless bridge between two industrial Ethernet.
- Dial up internet access on personal computers or PDAs using a capable mobile phone as a wireless modem.

4.2.3. PROJECT METHODOLOGY

The scope of this study is to observe the behavior of file transfer from one device to another in PAN via Bluetooth technology. This system can use Visual Basic programming to create a graphical user interface (GUI) for network performance monitoring of Bluetooth file transfer delay due to types and sizes of file versus distance of transmission. The data will be sent from the master to the Bluetooth device (slave) as asynchronous serial data. Transmission and reception are half duplex, which means that it will either transmit or receive but not simultaneously.

The system should also put to other tests like varying the files' sizes and transmission distances. Both devices should be placed at different distances and each respective device can then transmit several files. The result would show:

- Delay
- Throughput
- Error Rate

At first, both prototypes must be placed very closely together and then gradually apart. The longest testing distance for file transfer is approximately 8 meter in a room (indoor). It can be observed that error increases over longer separation of the said devices. The major advantage of using Bluetooth technology as a medium of transmission is Line of Sight (LOS) characteristic. This means that this prototype does not have problem if it is placed separately in different rooms. Device (as receiver) can receive the entire signal transmitted by the transmitter even if there are walls in between. This proves that the Bluetooth technology, which uses microwave propagation, is able to penetrate through walls.

As stated before, for the purpose of analyzing the performance of this Bluetooth system, data in the form of different sizes of files, types of files and separation distance are measured against the transmission delay. Three types of files that can be used are text (*.txt) format, winamp (*.mid) format and picture (*.jpeg, *.png, *.gif) format. Data tabulated will be for a distance of up to 6 meters only because our research has shown that a transmission of 8 meters is possible but not stable. Hence, the readings at that distance were not taken under consideration. All data in Table 4.2.2 were analyzed and plotted as shown in

Figure 2. It can be seen that the transmission delay is directly proportional to the size of files. Meaning, as the size of the file increases, the delay for transmission will increase too. Figure 4.2.2 shows the system throughput by plotting the delay of file transfer versus the transmission distance. Throughput is the number of bits, characters, or blocks passing through a data communication system, or portion of that system. Throughput may vary greatly from its theoretical maximum and it is expressed in data units per period of time.

Table 4.2.2: File transfer delay due to distance and size of file (Time format in seconds)

Text File (Kb)	2m	4m	6m	2 walls
200	4.3	5.0	5.4	6.0
400	9.3	10.1	9.7	12.3
600	13.8	12.1	14.9	19.5
800	21.3	21.1	19.0	28.6
1000	23.4	28.3	25.7	29.2
2000	45.5	45.2	58.0	57.8
4000	89.1	94.7	104.3	118.9
5000	117.9	128.4	124.6	154.5

Throughput is also defined as the maximum capacity of a communications channel or system and a measure of the amount of work performed by a system over a period of time. The analyzed data in Table 4.2.2 shows the capacity of the setup of Bluetooth based PAN can handle a file size up to 5000 Kilobyte. It is also observed that with obstacles, the propagation of signal transmitted will have more delay regardless of the different sizes of file. It is proved that with two walls in between, the delay is higher for all file sizes as noted in Table 4.2.2.

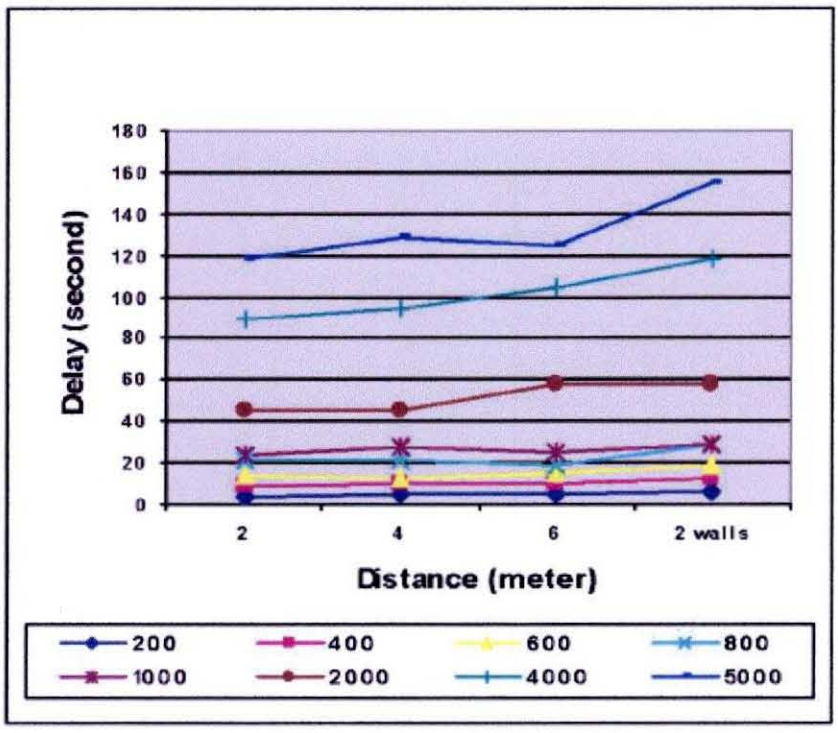


Fig 4.2.2: Estimated Graph of System Throughput

An analysis was also carried out on the performance of file transfer between a Bluetooth mobile phone and a PC. The traffic behavior was investigated using two different types of file, picture file (*.jpeg, *.png, *.gif) and winamp file (*.mid). The findings indicate that the transmission delay also varies exponentially with both types of file.

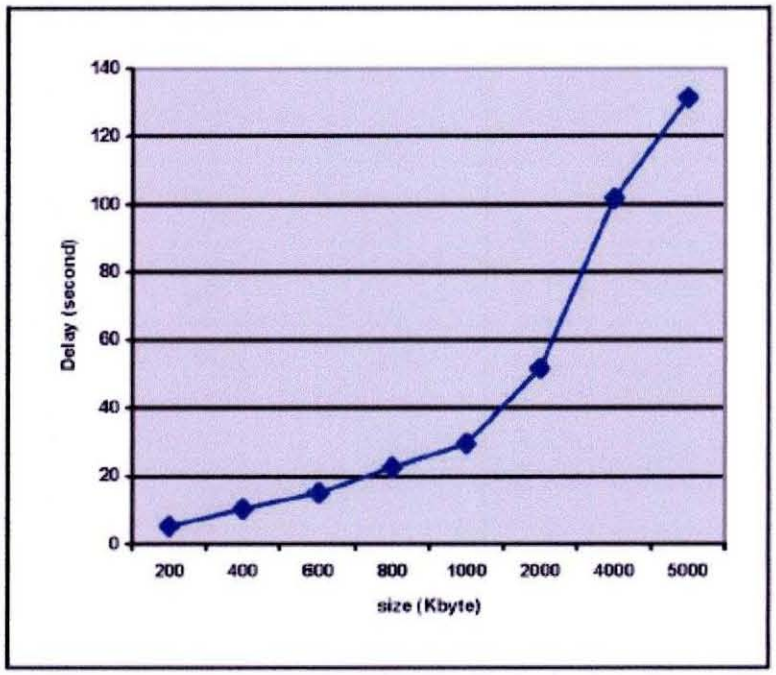


Fig 4.2.3: Different File Sizes versus Average Delay

Quality of service is an important issue when dealing with any communication link. The Bluetooth specification provides Quality of Service (QoS) configuration to allow the properties of links to be configured according to the requirements of higher layer applications or protocols. The properties that can be configured depend on the application QoS requirements, data rate, buffer storage, peak bandwidth, delay requirements and delay variations. For example, an application transferring compressed video streams may want a link that is not 'bursty', and may be able to miss a few packets as long as the delay on the link is not too high.

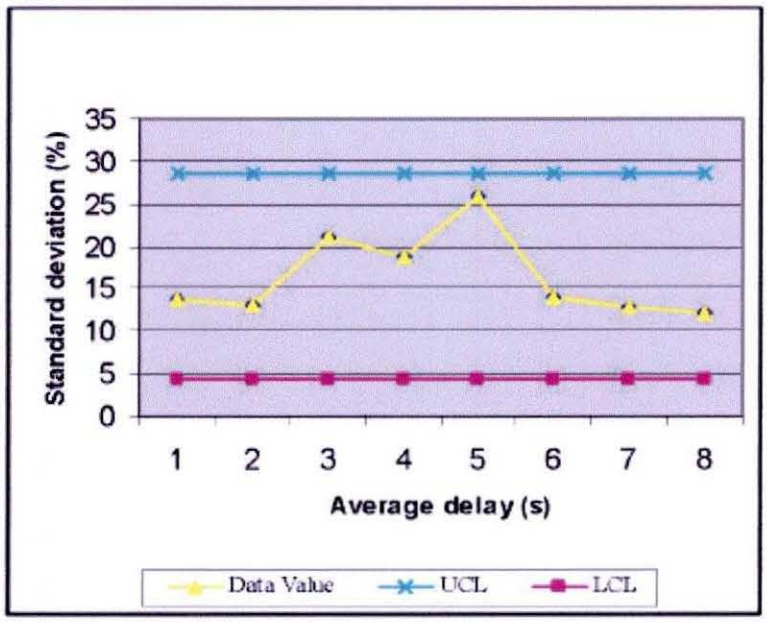


Fig 4.2.4: Standard Deviation (%) versus Average Delay (s)

Upper Control Limit (UCL) and Lower Control Limit (LCL) calculations help to examine whether the performance of the set-up Bluetooth-based PAN is within acceptable QoS. It can be observed from Figure 4.2.4 that the variation of standard deviation with the average delay is within the defined statistical control.

4.3.0. Cluster Mobile Switching Center for Third Generation Wireless Systems

4.3.1. INTRODUCTION

We can see technology is being updated every day. Therefore we must build systems that can cope up with the ever changing technology that we use at present. One such major change in the mobile communication system of our country is from 2G to 3G.

Our mobile communication system use to follow 2G technology, however since its being evolved into 3G technology we must design a system that will support this transformation. Third generation wireless systems will support multimedia services and provide access to ISDN and Intelligent Network value-added services such as call forwarding. In this paper we have examined three

different steps of a new structure called Cluster Mobile Switching Center (cMSC). These steps are:

- Design
- Implementation
- Performance

We will use distributed call processing so that the system will have a high rate of call handling capacity and we will also use modular design so that there might be various feature additions and load balancing can be done too in a network of processors.

Third generation systems will require increased capacity because the number of users and bandwidth required for advanced services will greatly increase. For this system will use

1) Digital air interfaces

2) Use smaller cell sizes to increase frequency re-use

Third generation networks will also provide an expansive set of services, including telephone services available on modern ISDNs, location-based services, data services, and multimedia communication. Signaling protocols and control procedures must be added to existing systems to support these new services while inter working with existing services.

Summarizing, the next generation of wireless infrastructure requires a switching arrangement that is scalable to support inexpensive small installations, and flexible to support the easy introduction of new services and inter work with emerging systems without major software modifications.

One approach to a third generation cellular wireless telecommunications switching system that has been tried in the past is called Wireless Distributed Call Processing Architecture (W-DCPA). The W-DCPA approach has several drawbacks. First, it does not allow for graceful evolution from existing systems to a third generation approach, but rather requires a "flash cut" from existing to new equipment. Second, components internal to W-DCPA had various interfaces to other entities in the telecommunications network, which were non-standard. Therefore, W-DCPA was not arranged or able to use existing call processing and mobility management application layer protocols.

Our extensive research has shown the results that after running various tests and experiments we saw that three Ultra 2s can support over 300000 calls per hour with average call setup latency 300 milliseconds which is acceptable because it meets the requirements of third generation systems. Thus, we

conclude that the software design, CORBA-based platform, and commodity processors are suitable for call processing applications in a wireless environment. Given that the performance-to-price ratio of processors will continue to improve dramatically, we expect solutions based on these principles to have long life cycles.

4.3.2. EXISTING SYSTEM

Due to the large investment in second generation wireless systems, third generation systems will likely evolve from second generation systems and inter work with them. The following figure shows the network architecture.

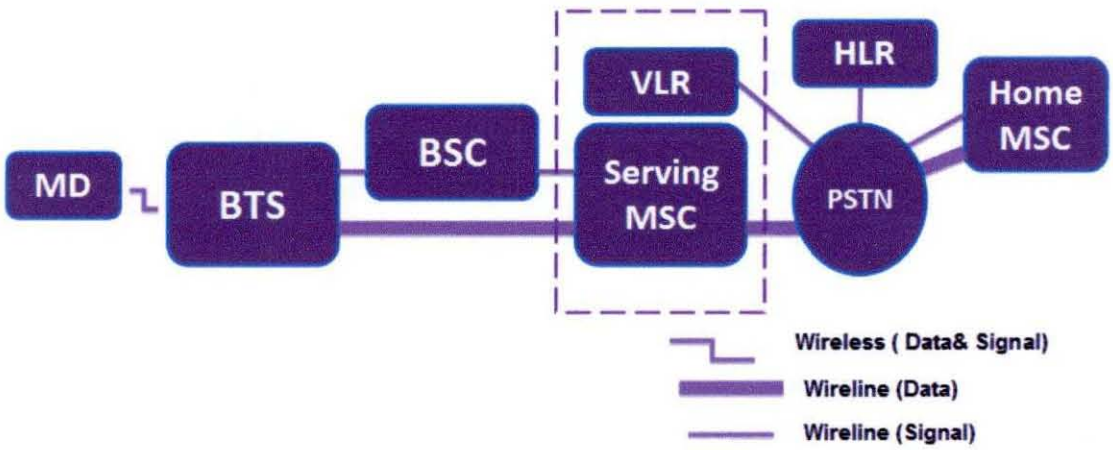


Fig 4.3.1: Cellular Telecommunication Network Architecture

A Base Terminal Station (BTS) terminates the air interface protocol to the Mobile Device (MD). It forwards user traffic to the Mobile Switching Center (MSC), and control traffic for example, signaling messages, to the Base Station Controller (BSC). The home MSC serves as a bridge for incoming calls to a mobile device. Calls for a mobile device are routed to its home MSC which, through interaction with the HLR, determines the serving MSC at which the mobile device is located, and then sets up a connection to the mobile device through the Public Switched Telephone Network (PSTN). A Home Location Register (HLR) contains a permanent service profile for each user and mobile device in the network, and tracks the approximate location of the mobile devices.

The serving MSC performs tasks related to both transport of user information and signaling. There are three types of user information. They are:

- Switching
- Voice Coding
- Frame Selection

Signaling contains the following tasks:

- Mobility Management – Registration, Paging and Handoff
- Connection Control – Routing
- Call Control – Providing Access to Processing Logic for Value Added Service

The VLR functions as a database for location and service profile information. In current systems, VLR and Serving MSC co-located as shown by the dashed box in Fig 4.3.1.

4.3.3. PROPOSED SYSTEM

Cluster MSC (cMSC) is an integrated control function of current MSCs and VLRs which provides support for third generation services. It is called Cluster MSC because it is made up of a cluster of processors. The reason to design this software in different modules is because it supports flexible deployment of the system. We are using distributed processing to provide scalability with respect to capacity. Different commodity software and hardware platforms are used to decrease the cost. For running the workstation UNIX operating system and for communication middleware Common Object Request Broker Architecture (CORBA) is used. Many current research projects in control software for broadband and third generation wireless networks also stress flexibility, either through layered software or object-oriented design. Distributed processing techniques are also widely used in these systems to achieve scalability and allow for increased flexibility to incorporate algorithms which may improve overall system performance. To reduce the time required to develop distributed systems, several efforts propose using CORBA as a communications middleware. In the cMSC, the focus is to build a single network element that is compatible with second generation wireless standards and is evolvable to support advanced services such as third generation.

Many of the concepts of the cMSC originate from earlier work on the Wireless Distributed Call Processing Architecture (W-DCPA). W-DCPA was designed and prototyped to support third generation services such as high bit-rate voice and multimedia communication whereas the cMSC is designed to evolve from a second generation system to a third generation system.

4.3.4. SOFTWARE ARCHITECTURE

To reduce the cost of designing the cMSC and increase the portability, widely available commercial software and hardware platforms are used instead of custom-built counterparts. In the current implementation, the cMSC executes on both HP-UX and Solaris operating systems using CORBA as communications middleware. The software is written in C++.

Software objects are defined to perform specific tasks and manage particular resources where these objects interact to provide end-to-end services. Objects that perform strongly-related functions are grouped together into a server. Each object has a well-defined interface through which others may access its services. As long as its interface is kept unchanged, a single object may be modified to change its behavior or upgrade its functionality without affecting other existing objects which makes the system scalable in the functional dimension and helps in the evolution from second to third generation systems. C++ coded objects are used as the basic objects for each server. However, each servers are implemented as CORBA objects were every server has Interface Definition Language (IDL). This IDL is defined in the CORBA which is only interface to the server.

Each of the servers run as a single UNIX process which can be duplicated and distributed to various processors so that the system can be scalable in the capacity dimension.

Figure 4.3.2 shows the complete architecture of the cMSC. Each box represents a CORBA server within the cMSC. The interconnection of servers may be over a high speed LAN or over a backplane depending on whether or not the servers are collocated on the same processor.

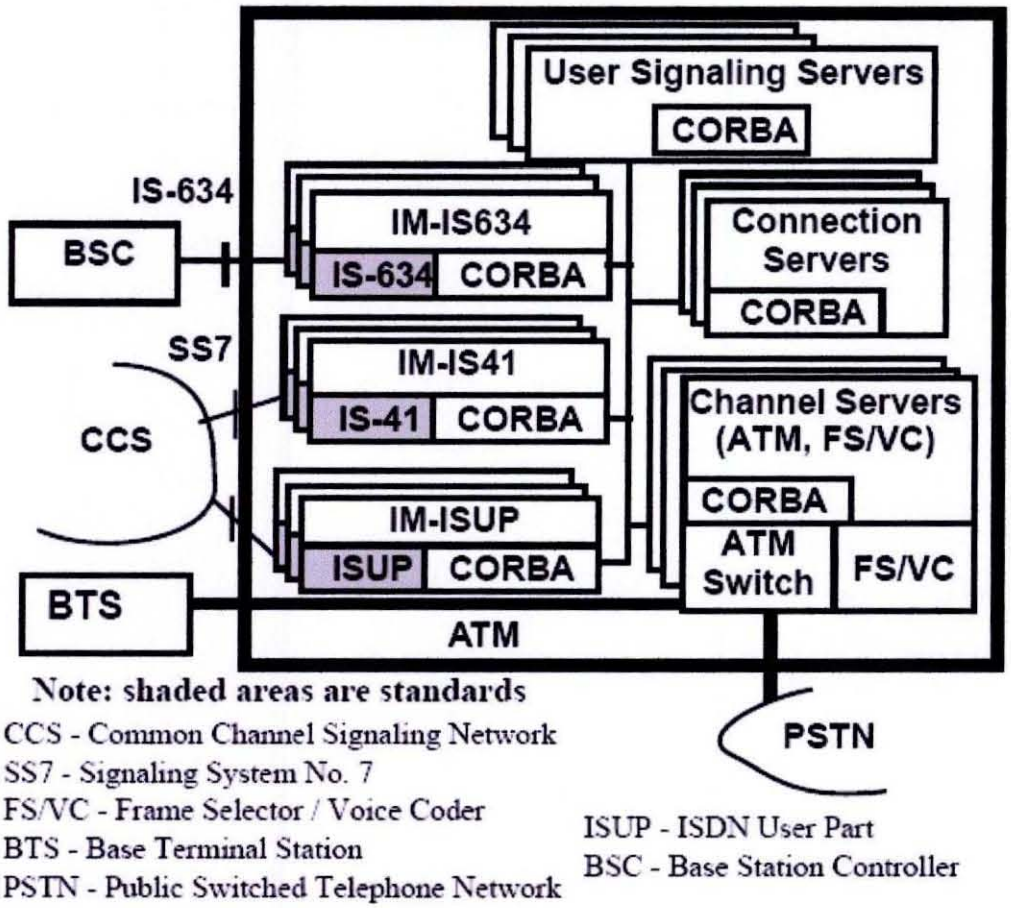


Figure 2. cMSC Software Architecture

The cMSC has two classes of servers:

1. Inter working managers (IMs): IMs act as gateways and provide interfaces to external network elements. IMs terminate standard protocols with the external elements and use CORBA to communicate with the core servers.

2. Core servers: These perform call processing functions and communicate with each other using CORBA.

The IMs allow the call processing in the core servers to be designed independently of the external signaling protocols. As new protocols are standardized, the cMSC could deploy new IMs to support the new protocols without modifying the core servers. This is important as networks evolve from second to third generation systems and as new protocols emerge. The current cMSC has three inter working managers. An IMIS634 terminates the IS-634A

protocol with the BSC across the standard IS634 A1-interface. The IM-ISUP terminates the SS7 protocol suite for call/connection control with the common channel signaling network across the Network Node Interface (NNI). The IM-IS41 terminates the IS-41 protocol stack which is used for mobility management.

There are four core servers in the cMSC. They are:

1. The frame selector/voice coder channel server
2. ATM channel server
3. User signaling server
4. Connection server.

The servers each provide a specific service to the other servers, and may in turn, request services from the other servers.

The frame selector/voice coder channel server:

The FS/VC channel servers manage the assignments of frame selectors and voice coders.

ATM channel server:

The ATM channel server manages VCI space and bandwidth in the ATM switch.

User signaling server:

The user signaling server performs mobility management functions of a VLR and provides access to IN-type services consistent with second and third generation systems. It also maintains call and connection state from the user's perspective. Mobility management functions include coordinating mobile device registration with the home network, managing paging, and assigning temporary routing numbers which are used by other network elements to route incoming calls to a mobile device. To provide access to IN services, the user signaling server maintains a temporary copy of a user's service profile which is obtained during registration procedures. It also checks service triggers to determine if value-added services should be activated.

Connection server:

The connection server determines a route between the BTS serving the mobile device and a circuit to the next hop switch at the edge of the PSTN. This includes choosing a frame selector/voice coder. The connection server interacts

with the FS/VC channel server, the BSC (through the IM-IS634), and the PSTN (through the IM-ISUP) to reserve resources for this portion of the connection.

In case of external elements, we use cMSC as a standard integrator between MSC and VLR. During registration procedures, the cMSC receives registration and location updates from the mobile devices through a BSC, registers the mobile device with the HLR, and populates the user's service profile. During outgoing calls from a mobile device, the cMSC receives the service request from the mobile device through the BSC and routes the connection to the proper switch in the PSTN. During incoming calls to a mobile device, the cMSC performs both call/connection control and mobility management functions. During these procedures it responds to routing requests from the HLR by assigning a temporary routing number, paging the mobile device, and routing the connection to the proper base station.

In cMSC of the present invention, objects that perform closely related functions are grouped together into particular servers. In this fashion, the servers may be distributed across processors to more easily allow the system to be scalable in the capacity dimension. That is, by allowing different instances of the same software server to exist on different processors, it is possible to balance the processing load of the system. It is also easier to achieve higher reliability through networked redundancy. The modular software structure thus allows servers, and the components within the servers, to be reused to implement networks that support different applications and use different protocols.

4.4.0. Real-time Monitoring and Filtering System for Mobile SMS

4.4.1. INTRODUCTION

People of our country now a days use SMS transactions as much as voice call transactions. We are realizing that SMS is playing a vital role in our life and as time goes by, importance of SMS is increasing day by day. Therefore we ought to take some steps so that in the future, we will not face much trouble or interference in the system of sending and receiving SMS.

Just like junk E – Mails people may start to send junk SMS. Although it is not yet a problem of our country but we might soon face it, so we should start taking some necessary steps accordingly. This paper is on reducing junk SMS in the future, keeping in mind that if such actions are not taken then we will face some major problems like other countries, for example China.

Junk message is a kind of illegal or advertising message violating the receivers' will, hiding the senders' real information and can't be rejected by the receivers. According to our research, from the year 2000 to 2006, SMS sending load in China was 1 billion, 18.9 billion, 90 billion, 137.1 billion, 217.7 billion and 429.6 respectively. Among these almost 30% of the SMS were junk messages. Junk message not only occupies the limited network resource, results in the internet congestion, degrades the mobile company's reputation, but also seriously influences the customers' normal work and daily life.

Research on filtering junk SMS is rare recently. While junk email, which is the counterpart of junk SMS, has been researched deeply and the technology of filtering junk email has become mature. Bayesian algorithm can be used to filter spam. Real-time filtering of the monitoring center impacts the processing speed of the SMSC and there are no corresponding technical measures to resolve it. Comparing the misjudgment of legal SMS and junk SMS, the former brings more loss to the customers and more trouble to the operators, however, the corresponding processing technology and strategy giving consideration to both issues is absent. The auto-generating technology of the keyword dictionary is absent, too. In this paper, the above problems during the SMS filtering are well resolved. In special, the mobile SMS real-time monitoring and filtering is implemented by combining the Pinyin Fuzzed Keyword Matching Technology with dynamical adjustment of the users' credit-grade by MD5 HASH algorithm.

A method of implementing real-time monitoring and filtering for SMS has been presented in this paper. For the implementation, the system should use a multi-core software platform for it.

4.4.2. SMS MONITORING AND FILTERING SYSTEM

Mobile Communication Network has two kinds: the GSM Network and the CDMA Network. Fig.4.4.1 shows the Network Topology Graph of SMS.

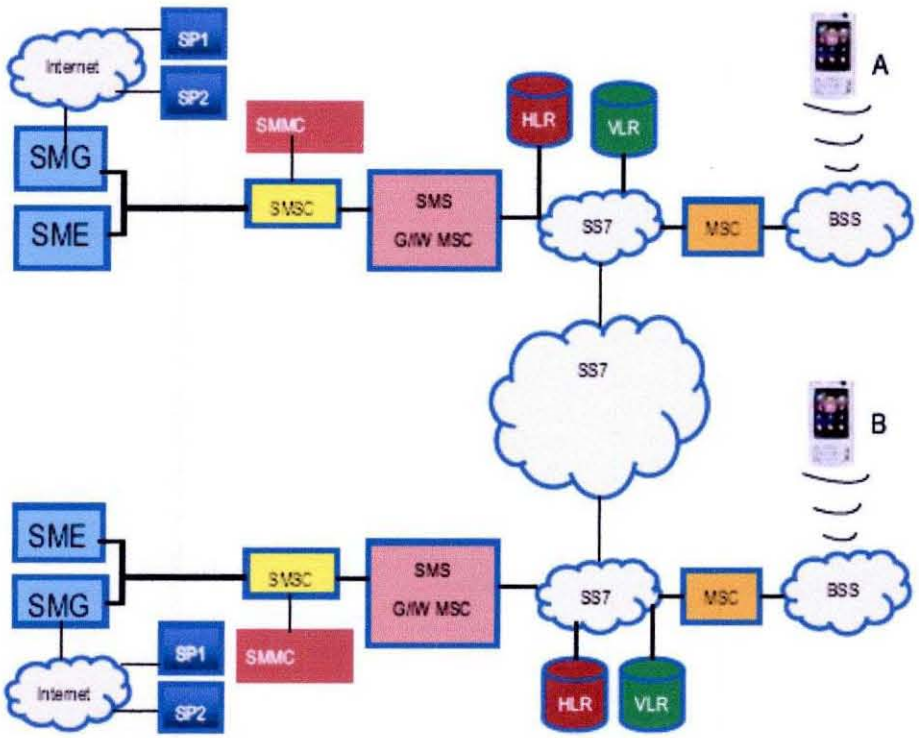


Fig 4.4.1: The Network Topology of SMS

For the above two networks, although the implementation mechanisms of SMS are different, the SMSC and SMMC are included in both of the two networks. So we can implement the SMS monitoring and filtering. Fig. 4.4.2 shows the block diagram of the SMSC and the SMMC.

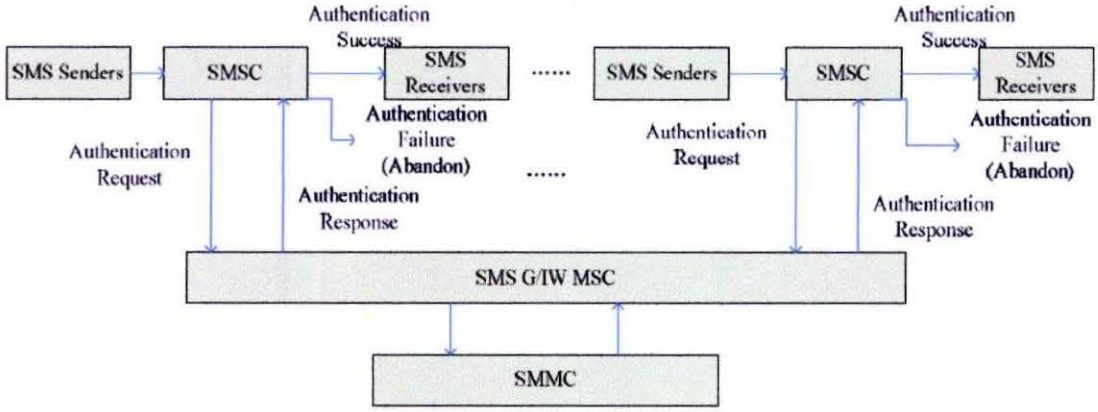


Fig 4.4.2: Block Diagram of SMSC and SMMC

Each SMSC receives the SMS sent by general users or submitted by the entity, sends an authentication request to the SMS Gateway/ Interworking Mobile Switching Center (SMS G/IW MSC), and then SMS G/IW MSC retransmits the request to the SMMC. The SMMC makes a judgment about the SMS's content and the behavior character, and then sends the authentication response to the SMSC through the SMS G/IW MSC. If the SMS is legal, the SMMC returns an authentication success message, and the SMSC sends the SMS to the receiver. If the SMS is doubtful, the SMMC returns an authentication acceptance message, the SMSC will send the message to the receiver by adding operators' signal message. If the message is illegal, the authentication failure message will be returned and the SMS will be abandoned by the SMSC. According to Interface Standard between the SMSC and the SMMC promulgated by information industry department, the communication between the SMSC and the SMMC adopts the standard SMPP Protocol. The SMSC calls for MO (Mobile Original) and submits it to the SMMC, the SMMC extracts the content of the "short_ message_ test", processes it according to the appointed rules and returns an authentication response message "short_ message_ test". If the time for waiting the response is more than 5 seconds, the SMSC will record the log and send the SMS directly.

Keyword filtering is the most frequently utilized anti-spamming technique. Using the achievement in the area of Spam Email Filtering for reference, keyword dictionary is generated automatically through Bayesian Off-line Learning for SMS sample. The spam immune system has the potential to do automated weighting of much more complex detectors, which may make it more robust to attacks designed to disrupt the Bayesian systems (for example, it would be possible for spam senders to begin appending large unrelated pieces of text to

the spam message so that the Bayesian System must weight more tokens and the final scoring will be thrown off by the unrelated text). Fig.4.4.3 shows the flow diagram of SMS keyword dictionary using Bayesian Learning. During the idle time of SMMC, Bayesian Learning Module makes Bayesian Learning for the sample screened from the SMS automatically/manually; the formed junk SMS keywords are supplied to the Pinyin Fuzzed Keyword Matching Module for SMS real-time filtering.

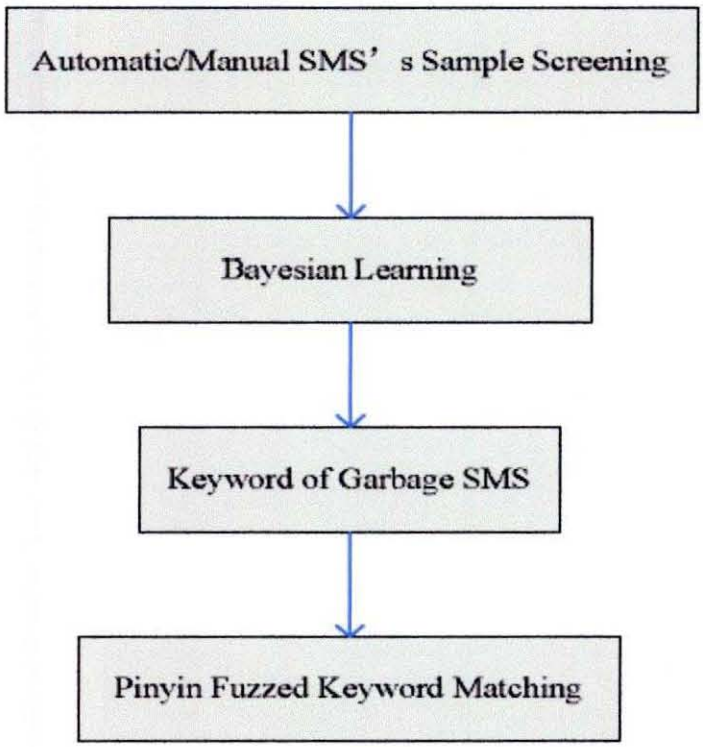
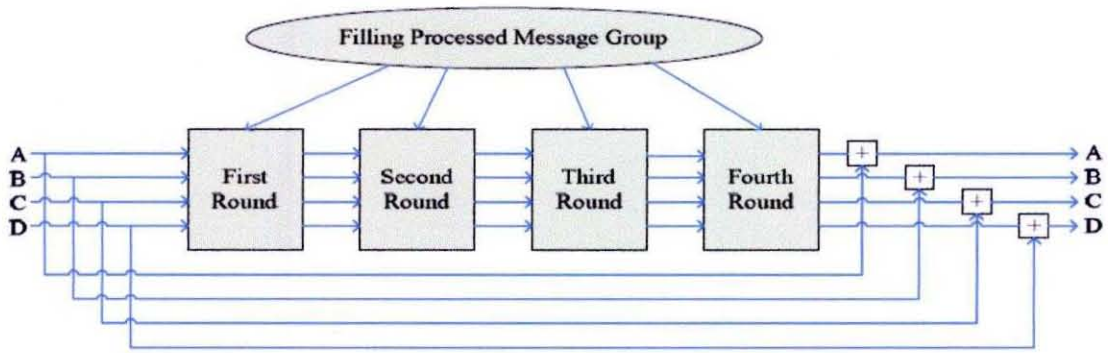


Fig 4.4.3: Flow Chart of SMS Keyword Dictionary Using Bayesian Learning

Existing research and test shows that the operation of SMMC will reduce the process speed of SMSC by 30%.The reason is that the SMS real-time filtering and Pinyin Fuzzed Keyword Matching Algorithm needs a lot of software and hardware resources. This question is also thorny for the operators. The technical measure to solve this problem is to adopt multi-core hardware platform and run parallel real-time filtering program. The difficult point for multi-core application is the software, fortunately, SMS real-time filtering has natural parallelism, and so the difficulty for running the parallel filtering program is greatly reduced.

4.4.3. ANALYSIS MECHANISM

MD5 is a hash algorithm introduced in 1992 by Professor Ronald Rivest. It is an enhanced version of its predecessor MD4. MD5 is widely used in several public key cryptographic algorithm and Internet communication in general. MD5 calculates a 128-bit digest for an arbitrary b-bit message and it consists of the following steps [9]: appending Padding Bits, appending Length, buffer Initialization, processing of the message and output. Here MD5 HASH algorithm is used to discriminate the consistency of SMS, which is shown in Fig.4. MD5 is short for "Message-Digest Algorithm 5"; its typical application is creating the message-digest for one message. MD5 takes the total document as a text, changes algorithm through irreversible character and produces a unique message-digest. In the transmition of the document, no matter however the content changes, we can decide it's a false document by calculating MD5 renewedly. Simply speaking, the function of MD5 is to compress the SMS into a secure format which means to change a character string having arbitrary length into a large integer having certain length.



(a)

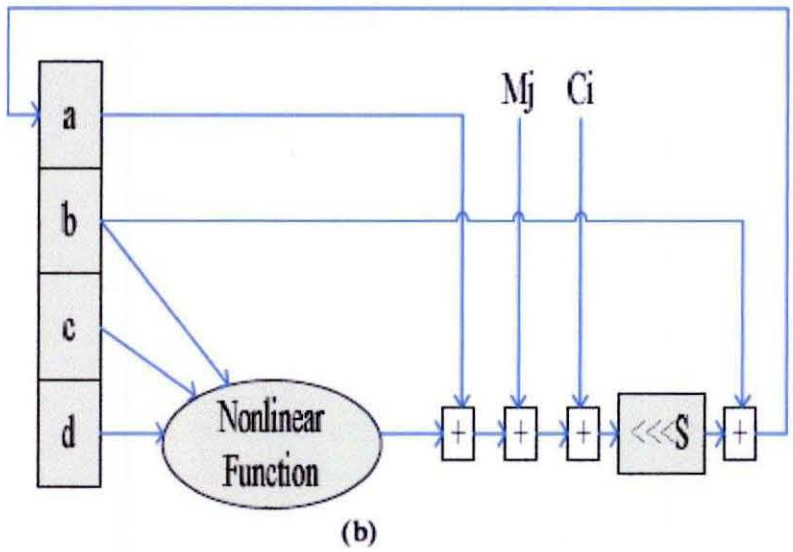


Fig 4.4.4: The MD 5 Hash Algorithm for the Consistency of the SMS's Content

4.4.4. REAL TIME FILTERING MECHANISM

There are many methods for the real-time filtering of SMS theoretically, but the method based on keyword matching is most widely used. Searching data for specific keywords or signatures is an important operation in a wide variety of applications including full-text-search, database queries, search engines, and natural language processing. As the junk SMS senders can make monitoring interference to the SMMC by adding some interference information, here we brings forward the Pinyin Fuzzed keyword matching technology for real-time filtering in order to eliminate interference effectively and achieve the goal of SMS filtering. The flow diagram of Pinyin Fuzzed Keyword Matching Algorithm is shown in the following figure. An example is given to discuss the Pinyin Fuzzed keyword matching technology for real-time filtering. Through Bayesian Learning for garbage keywords of thirty thousand SMS, we obtain the keyword of junk SMS "drug trade" whose pinyin form is "dupin jiaoyi" and the garbage-degree "M". When the system receives the illegal SMS "We will have drug trade at..." after making the pinyin fuzzed matching for the SMS, the system will get the keyword "dupin jiaoyi" and its corresponding garbage-degree.

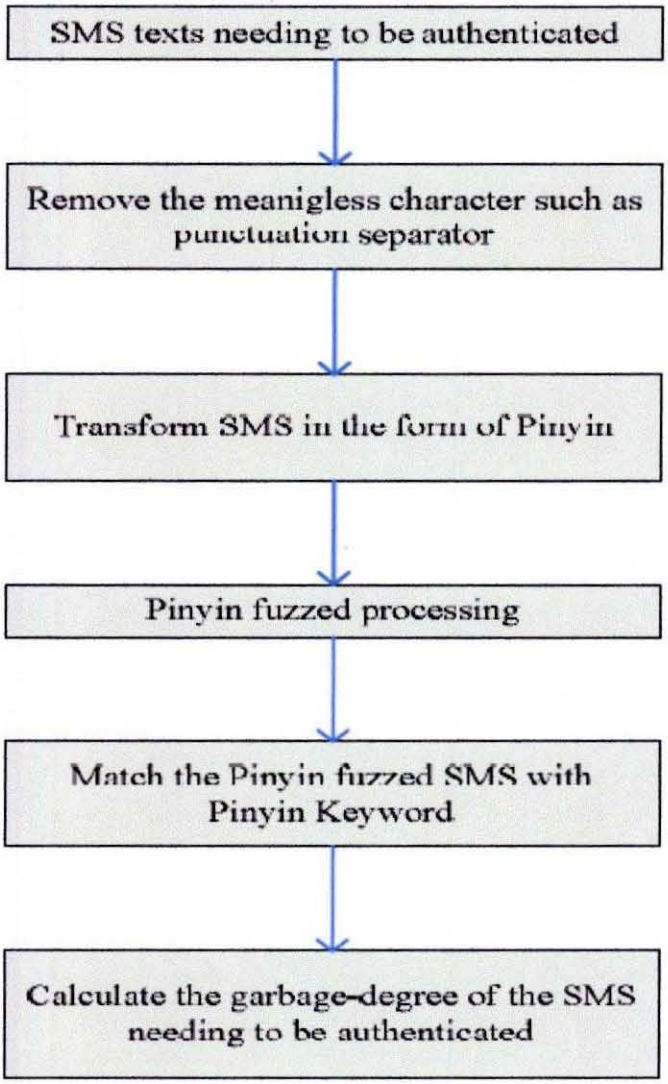


Fig 4.4.5: Flow Chart of Pinyin Fuzzed Keyword Matching Algorithm

Considering the facts that the misjudgment of legal SMS has more negative impact than illegal SMS, so many interceptions will reduce the operators' profit and the constraints to operators made by the relative law, we divide the SMS into three kinds: legal SMS, doubtful SMS and junk SMS. We release the legal SMS, intercept the junk SMS and add operator's signal language to doubtful SMS. Through the method above, the users can avoid the loss of important information being intercepted; the operators also have performed their obligation from the angle of legal science by adding signal language to doubtful SMS. Furthermore, whether the SMS is junk SMS has different answers to different customers. In sum, by considering the junk SMS's obvious behavior character and running the real-time monitoring and filtering on

the multi-core hardware platform, the strategy above gives consideration to both of the users and the operators, reduces the misjudgment rate of junk SMS and improves the processing speed.

4.4.5. OVERVIEW

The use of the Pinyin Fuzzed Keyword Matching Technology to get the pinyin keywords and the junk-degree of SMS, can eliminate the interference information of junk SMS effectively.

That adjusting the users' credit-grade dynamically according to the behavior character of junk SMS and then combining it with the junk-degree gotten above to give a comprehensive evaluation of SMS-class, enhances the interception rate and classification right rate

That running the parallel real-time filtering program on the multi-core hardware platform, reduces the impact of SMMC to SMSC processing speed

Proposing a new strategy for SMS classification and process which divides SMS into legal SMS, doubtful SMS and junk SMS, gives consideration to both interests of the customers and Telecom Company by setting legal SMS free, intercepting junk SMS and adding signal language to doubtful SMS

Adopting the Bayesian offline learning for SMS sample to create the keyword dictionary for SMS. The problems in the area of SMS service appear gradually as the telecom service quality improves. In the future, it could be expected the junk SMS senders could produce more new attack methods. Consequently, the monitoring and filtering technology tends to be more intelligent. Considering the different clients will give different definitions on what is "junk SMS", it will be more efficient to resist the overflow of the junk SMS by using the centralized filtration in the comprehensive server and meanwhile personalized filtration in the users' terminal.

4.5.0 A Student ID System Using a Cell Phone and Its Evaluation

4.5.1. INTRODUCTION

There are various ways one can carry his or her ID card. The can pin it on their shirts or they can hang it on their neck. No matter how they carry their ID card there is always a chance that they might forget and leave it at home. In

addition to this problem we can also say that another drawback is that we cannot put much information in plastic ID cards since there is not much space. However we always carry our cell phone with us. No matter what we remember to take our cell phone with us when we leave the house. We can also add as much information as we want if the ID is digitized.

A method to construct a student ID (identification) system using a cell phone has been proposed. The student ID data are stored in the server. Each student receives the student ID data in each cell phone. The cell phone displays the character data (name, affiliation, etc.), the face image and the two dimensional symbol. As the face image displayed on the cell phone is large enough in comparison with the photograph size of the conventional ID card, the precision is improved when the examiner compares the displayed face image to the live face. The student ID can be used not only when the examiner's terminal can communicate with the server, but also when it cannot communicate with the server. The cost for issuing or reissuing a student ID by using the proposed method is very low in comparison with the conventional student ID card.

The student ID (identification) card is used to identify each student in a university or a college. The purpose of a student ID card is to identify each student, improve the services for each student, and improve the efficiency of the staff in a university. Plastic cards and smart cards are used as student ID cards. As for the functional elements for the computerization of student ID cards, there exists an IC card, a cell phone, a barcode, a two-dimensional symbol, a database, a personal computer, a server, and a network system. A two-dimensional symbol has characteristics such as large recording capacity and error correction capability. By adding the two-dimensional symbol in the student ID system using a cell phone, the ID data can be quickly read by the two-dimensional symbol scanner attached to the examiner's terminal computer. The encryption and authentication techniques can be used for improving the security of the two-dimensional symbol for the cell phone. This paper proposes a method to construct a student ID system using a cell phone for improving the function of student ID cards and decreasing the cost. The prototype is constructed and the evaluation is executed.

4.5.2.1 THE FUNDAMENTAL CONCEPT

The fundamental concept of the proposed student ID system using a cell phone is described as follows.

The student ID data are stored in the database of a Web server.

Each student receives the student ID data from the Web server in each cell phone. The time when the student receives the student ID data depends on the application. It is possible for the student to equest the student ID data to the Web server. It is also possible that the Web server automatically sends he student ID data to the cell phone at the appropriate time decided by the application.

(3) The cell phone displays the student ID data such as the character data (name, address, etc.) and he face image. The examiner checks the displayed data.

(4) The cell phone additionally displays the two dimensional symbol including the student ID data. The purpose of the two-dimensional symbol is to read the data from the two-dimensional symbol scanner and automatically processes the data at the terminal computer of the examiner.

(5) The encryption and authentication techniques are used for the security of the two-dimensional symbol in the cell phone. Additionally, the two-dimensional symbol includes the timestamp to decide the expiring date and time for the student ID.

(6) The verification check for the student ID is performed not only when the examiner's terminal can communicate with the server (i.e., on-line identification), but also when the examiner's terminal cannot communicate with the server on account of its failure (i.e., off-line identification).

The elements of the proposed student ID system using a cell phone are described in Fig. 4.5.1.

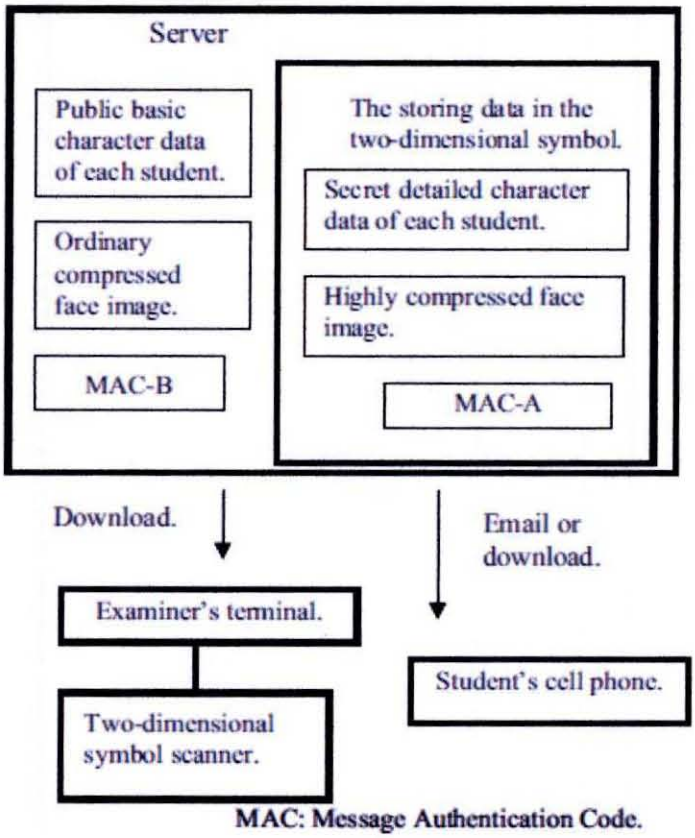


Fig 4.5.1: The elements of the proposed student ID system using a cell phone

4.5.2.2. THE SERVER

The examiner produces an ordinary compressed face image and a highly compressed face image from the face image of each student. The difference between these compressed face images is the compression rate for the face image.

The server obtains the basic character data (name, student ID number, and affiliation) of each student, the ordinary compressed face image, and the data for the two-dimensional symbol. The data for -the twodimensional symbol consists of the following data. The highly compressed face image and the detailed character data (name, student ID number, affiliation, birth date, a phone number, address, reation date, expiration date, and other additional information) of each student.

(3) The server creates MAC-A as the message authentication code (or digital signature) for the data of the two-dimensional symbol such as the highly compressed face image and the detailed character data of each student.

(4) The server creates MAC-B as the message authentication code (or digital signature) for the transmission data to the cell phone and the examiner's terminal such as the basic character data (name, student ID number, and affiliation) of each student, the ordinary compressed face image, and the data for the two-dimensional symbol.

(5) The server encrypts the detailed character data of each student, the highly compressed face image and MAC-A. The server stores the encrypted data in the two-dimensional symbol.

(6) The server transmits the ordinary compressed face image, the basic character data of each student and the two-dimensional symbol, to the cell phone. These data are transmitted by email from the server, or are downloaded by the student from the Web browser of the cell phone.

(7) Both of the encryption key and the authentication key are shared between the server and the examiner's terminal.

4.5.2.3 THE CELL PHONE OF THE STUDENT

(1) The cell phone of each student receives the ordinary compressed face image, the basic character data of each student and the two-dimensional symbol from the server.

(2) The student displays and shows the basic character data of each student, the ordinary compressed face image, and the two-dimensional symbol on the cell phone according to the instruction of the examiner.

4.5.2.4 THE IDENTIFICATION PROCESS BY THE TERMINAL COMPUTER OF THE EXAMINER

The system can execute both of the on-line identification and the off-line identification. The online identification is used when the examiner's terminal computer can communicate with the server. The off-line identification is used when the examiner's terminal computer cannot communicate with the server on account of the failure of the server or the communication line.

4.5.2.2.5 THE MERITS OF THE PROPOSED METHOD

The proposed method of a student ID system using a cell phone has the following merits.

(1) As the student ID data can be downloaded from the Web server anytime, it is unnecessary for each student to worry about losing the student ID card. Even when the student loses the cell phone, the student ID is protected by the security function of each cell phone such as the password to use the cell phone.

(2) As the face image displayed on the cell phone is large enough in comparison with the photograph size of the ordinary plastic ID card, the precision increases when the examiner checks the similarity between the displayed face image and the live face.

(3) After the two-dimensional symbol scanner directly reads the student ID data, the examiner's terminal computer can automatically process the data.

(4) By using the two-dimensional symbol for the ID system using a cell phone, the forgery becomes more difficult and the time for checking the student ID data is reduced.

(5) The cost for issuing or reissuing the student ID is very low, because there is no printing cost.

4.5.3. THE PROTOTYPE

We have constructed the prototype based on the proposed method. The Web server consists of the Web server software and the script program. The administrator inputs the student ID data in the Web server. The QR code is used for the two-dimensional symbol of the prototype system. The student ID data including the two dimensional symbol is transmitted to the student's cell phone at the pre-specified time by email. The examiner's terminal is a notebook computer with a two-dimensional symbol scanner connected by the USB interface.

Traffic Capacity Performance of a CT2Plus Based Wireless PABX

INTRODUCTION

Almost 90% of organizations in our country use internal PABX line. Even our very own BRAC University uses a PABX line to stay connected with each department. A PABX line is used because it is the cheapest communication technology. Therefore, if we can transform a regular PABX line into a wireless PABX line then it would be both cheap and fast. This section presents the traffic capacity performance of a CT2Plus Based Wireless PABX.

Adoption of new standards for Digital Cordless Telephone Services (DCTS), such as CT2Plus, determining the impact on the Network Gateway portfolio (i.e. PABX, Centrex, LAN) has become very important. Defining the technical requirements is also necessary that will address the business applications for wireless access. One major concern is the impact of the traffic capacity of a digital cordless system on the Network Gateway solution. As a consequence, the investigation of the traffic capacity performance of a digital cordless system in different application environments is required. A comprehensive traffic capacity simulator, based on the CT2Plus Common Air Interface Specifications (CAI) has been developed. The impacts of multiple in-building systems in both synchronized and unsynchronized environments on traffic carrying capabilities has to be investigated and extensive simulations on the traffic capacity of an indoor wireless system needs to be run under different environments and system configurations from which results in terms of *GOS* can be presented.

4.6.2. SYSTEM OVERVIEW

Here we explain all the important terms related to this topic as under:

4.6.2.1. CT2Plus CAI

CT2Plus CAI is an enhanced version of CT2 CAI and has a few major enhanced features. One of them is that CT2Plus CAI has Common Signaling Channels (CSCs). The CT2Plus will operate at frequency band 944 - 948.5 MHz, and has 40 communications channels and an additional 5 CSCs. The channels are 100 KHz wide. Each of the 5 CSCs supports 8 common signalling data streams in TDMA mode.

4.6.2.2. INTERFERENCE MODEL

In implementing the traffic capacity simulator, three kinds of interference sources: co-channel, adjacent-channel and unsynchronized interference, were considered. The consideration of unsynchronized interference depends on the simulation scenarios of interests. The inter modulation distortion in both a portable and base station is not considered.

4.6.2.3. TRAFIC MODEL

It is supposed that the service area is partitioned into a finite number of equal size square areas. This kind of equal size square area is called a cell. A fixed station or base station is placed at the center of each cell. All base stations can be synchronized or not synchronized, depending on the simulation scenarios. A portable is randomly positioned within the service area prior to a call set up attempt. Over the duration of the call, the portable remains quasi-stationary, i.e. the shadowing and distance dependent variables associated with the call remain constant. Call originations from each portable follow a Poisson process with an average call arrival rate which is determined by offered traffic in the service area. The duration of a call (set-up time and talk time) has an exponential distribution with a mean of 100 seconds in this Paper.

4.6.2.4. CT2Plus CALL SET-UP PROCEDURE

When a randomly located handset (or portable) in the service area initiates an outgoing call, this handset will measure the signal strengths from all base stations in the service area on CSCs, rank them, and finally lock on to the strongest. Then the handset will have to check if the strongest base station has free transceivers for use. An attempt will be made to set up the call to another base station in the service area if this base station is busy. If none of a given number, for example 5, base stations is available, this call set-up attempt will be dropped as a blocked call. Upon the reception of a call set-up request from the handset and if a free single-channel transceiver is available, the base station will send a list of all its free channels to that handset, where free channels mean those that are not being used at this base station (in CnPlus, both the portable and base station are able to scan all available frequency channels. In this paper, it is assumed that there are only 36 frequency channels available instead of 40). The handset will measure the interference level on all of these free channels and rank them in terms of the interference level once it has received the response. Then the handset will pick up the best channel in terms of the interference level to check if the received Signal to Interference Power ratio(S1R) on this selected channel is larger than the threshold of SIR (i.e. 21dB). If yes, the handset will

inform the base station of the chosen (preferred) channel and let the base station check it too. If the received SIRS at both ends of the link are acceptable, then the link between the handset and the base station is set up on the selected channel.

Otherwise, the handset and base station try the next best channel selected from the list of best channels maintained by the handset. If none of five best channels in either the base station or the handset is appropriate for link set-up due to high interference level, the handset will turn to the next best station to search for appropriate channels. The maximum number of base stations that will be tried by a handset depends on the application and requirements, and is assumed to be 5 in this paper.

4.6.2.5. HANDOVER ALGORITHM

A check for handover for all calls on a traffic channel (TC) is made when the interference on that channel increases. This will happen either when a new call is set-up on a channel that interferes with TC, (co-channel or adjacent channel) or when an existing call is handed off to a channel that interferes with TC. If the average measured signal to interference power ratio, S/(I+N), at either the base station or the portable falls below the call handover threshold, a search for a new channel begins immediately (zero second time-out). The search will first start from the current base station to which the portable is locked-on (intra-cell handover) and then in case of failure, from any of the adjacent base stations (intercell handover). A call is dropped if the average S/(I+N) at either the portable or the base station drops below the call threshold for more than 10 seconds.

4.6.3. SIMULATION SCENARIOS

In this paper, various scenarios are postulated in order to assess the capacity of a business customer's wireless system, employing CT2Plus under various environments of interest. For a multi-floor building, two scenarios are postulated. Scenario A envisages a multi-tenant facility involving several small or medium sized businesses employing wireless Key Sets or wireless PABXs. The Scenario A takes the form of a 3 floor building with 3 synchronized systems (one on each floor). Scenario B is defined as 3 unsynchronized systems (one on each floor of the same 3 floor building).

Fig 4.6.1 shows the simulated building for the evaluation of traffic capacity of a multi-service provider wireless system under scenarios A & B.

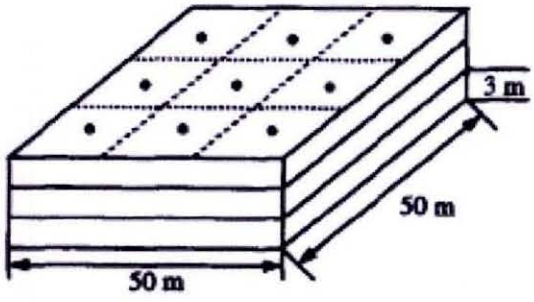


Fig 4.6.1: The simulated building for the evaluation of traffic capacity of a multi-service provider wireless system under scenarios A and B

Building: 50m x *5Om,* 3 floors.

Operation: one service provider on each floor, calls set-up and hand off only to base stations on their floor. For scenario A, all base stations in *this* building are synchronized, but for scenario B, the base stations for each service provider are synchronized among themselves, while not synchronized to the base stations of any other service provider.

Traffic: 0.1 Erlangs of traffic (average) per portable and 100 seconds call holding time (exponentially distributed) are assumed in this paper.

5.0. CONCLUSION

Senior students of BRAC University always face their biggest problem in their last year about their thesis. The concept of thesis is very vague. A student needs to choose a thesis topic which is very confusing for them because usually they don't have much idea on this field. If a student does not have good background information then he will be totally lost since none of the courses teach them anything on how to choose a thesis topic and then implement it. Therefore we, along with our supervisor came up with the idea of doing a thesis that will help solve such problems. We have made a documentation that provides a selection of thesis topics and also provide guidance on how to complete a thesis on those topics. After all thesis is not only about gaining more knowledge or how it helps us but a thesis is about how it helps the community around us.

Keeping this in mind we went through an extensive research and sorted around 30 topics. From these topics we selected 6 topics which can be done by students of BRAC University and after implementation of these projects or study they will help our nation as well.

LIST OF REFERENCE

[1] Behrouz A. Forouzan, "**Data Communications and Networking**", 3rd Ed, Tata McGraw-Hill, 2004.

[2] Hossain, A. Jahan, S. Hussain, M.M. Amin, M.R. Shah Newaz, S.H, **"A proposal for enhancing the security system of short message service in GSM"** in Anti-counterfeiting, Security and Identification, 2008. ASID 2008. 2nd International Conference on 20-23 Aug. 2008

On page(s): 235 - 240

Location: Guiyang

[3] www.gsmfordummies.com/encryption/encryption.shtml

[4] Rashid, R.A. Yusoff, R., **"Bluetooth Performance Analysis in Personal Area Network (PAN)"** in: RF and Microwave Conference, 2006. RFM 2006. International on 12-14 Sept. 2006

On page(s): 393 - 397

Location: Putra Jaya

[5] http://en.wikipedia.org/wiki/bluetooth

[6] La Porta, T.F. Ramjee, R. Murakami, R. Buskens, R. Lin, Y., **"Cluster mobile switching center for third generation wireless systems"** in: Personal, Indoor and Mobile Radio Communications, 1998. The Ninth IEEE International Symposium on 8-11 Sept. 1998

On page(s): 121 - 125 vol.1

Location: Boston, MA

[7]. Ningning Wu ,Mingguang Wu, Siguo Chen, **"Real-time monitoring and filtering system for mobile SMS"** in Industrial Electronics and Applications, 2008. ICIEA 2008. 3rd IEEE Conference on 3-5 June 2008.

On page(s): 1319 – 1324

Location: Singapore

[8] Kobayashi, T. Jaewook Kim Machida, N., **"A student ID system using a cell phone"** in: Wireless and Mobile Technologies in Education, 2005. WMTE 2005. IEEE International Workshop on 28-30 Nov. 2005

On page(s): 45 – 47

[9] . Zhang, H. McGladdery, B. Chung, J., **"Traffic capacity performance of a CT2Plus based wireless PABX"** in: Vehicular Technology Conference, 1994 IEEE 44th on 8-10 June 1994

On page(s): 1581 - 1585 vol.3

Location: Stockholm.

[10] Kitchener, D. Smith, M.S, **"Low cost antennas for mobile communications"** in: Low Cost Antenna Technology (Ref. No. 1998/206), IEE Colloquium on 24 Feb. 1998

On page(s): 5/1 - 5/2

Location: London