GSM NETWORKS: A REVIEW OF SECURITY THREATS AND MITIGATI0N MEASURES

BY

WAMYIL, MAGDALENE TURAN

And

***MU'AZU, MUHAMMED BASHIR**

Department of Electrical Engineering, A. B. U. Zaria

ABSTRACT

The Global System for Mobile communication network, popularly called GSM, is a worldwide standard for mobile communication offering varied services like voice calls, short and multimedia messaging (text) services (SMS and MMS) and Global Packet Radio Service (GPRS) which allows internet connectivity. Some of these services have possible security vulnerabilities. This paper investigates the security measures used in GSM networks which include Authentication, Encryption, Equipment Identification and Subscriber Identity Confidentiality, as well as the manifestation of network vulnerabilities including SIM, SMS attacks, encryption and signaling attacks. Suggestions on mitigative measness are also discussed.

GSM NETWORKS: SECURITY

THREATS AND MITIGATI0N

MEASURES

Introduction

Communication is an essential part of the economy of every nation. In about ten years after the launching of the first Global System for Mobile communication network, popularly called GSM, it became the worlds leading and fastest growing mobile standard, spanning over 200 countries as of then. Presently, it is used by more than one-sixth of the world's population, hence, over 1 billion GSM subscribers across the world (**www.gsmworld.com**).

Nigeria, being a part of the world trend, launched its first network in August 2001 and has since being having various network expansion projects by all four network operators (MTN, Vmobile, Glo and MTel) in the country, attesting to the growth of subscribers (**Wetten: 2003)**. The growth of this particular form of wireless technology is due to the various services it offers which could be applied in various sectors of any economy. Apart from the basic telephony (voice calls) service, it has other services like Short Message Service (SMS), Multimedia Messaging Service (MMS), Global Packet Radio Service (GPRS) which allows internet connectivity. As a result, it could be applied in Banking for checking of account balance, sales and in commerce; amongst many other fields (**www.gsmworld.com**).

GSM Network Architecture

The GSM network is divided in to several functional entities that have specific applications (**Wetten: 2003)**. Figure 1 shows the major components of the GSM network. The GSM Network can be divided in to three major parts: The Mobile Station (MS), the Base Station Subsystem (BSS) and the Network Subsystem (NSS)

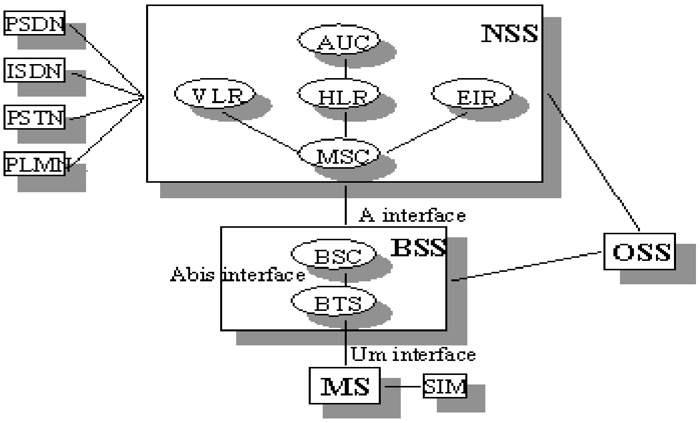

Figure 1: The GSM Network Architecture

The Geographical Areas Of The GSM Network

The different areas that form a GSM network are as shown in Figure 2.

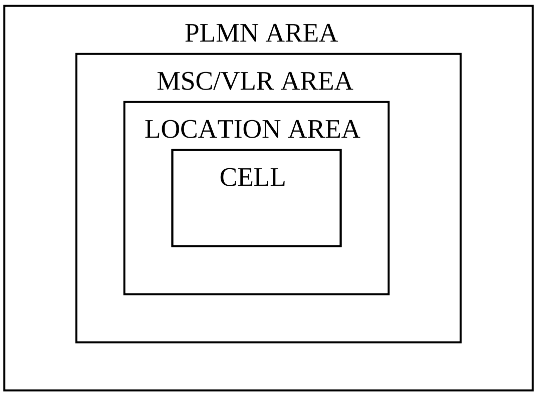

Figure 2: The GSM Network Areas

A cell is the basic geographic unit of a cellular system. The term *cellular* comes from the honeycomb appearance or cell-like structure of the areas in which a coverage region is divided. Cells are base stations transmitting over small geographical areas that are represented as hexagons as in Figure 3. Each cell size varies depending on the landscape. Because of constraints imposed by natural terrain and man-made structures, the true shape of cells is not a perfect hexagon.

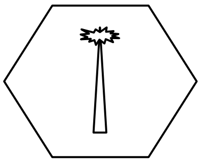

Figure 3: The Diagram of A Cell

A cell is identified by its Cell Global Identity number (CGI), corresponding to the radio coverage area of a base transceiver station. A Location Area (LA), identified by its Location Area Identity (LAI) number, is a group of cells served by a single MSC/VLR. A group of location areas under the control of the same MSC/VLR defines the MSC/VLR area. A Public Land Mobile Network (PLMN) is the area served by one network operator (**Ericsson Telecoms: 1998)**.

Security In Telecommunication Networks

The security protocols used in various communication networks vary in procedure and deployment, but they have similar underlying motivations. All communication networks, though technologically based still have a fundamental goal of profit making for the operators. A bridge in security could lead to substantial financial loss to the operators due to loss of credibility.

Existing Security Measures

1) Authentication

When a new subscriber is registered in the GSM network, the mobile system is given a 128 bit subscriber authentication key K_i , and the telephone number or international Mobile Subscriber identity (IMSI) which are used in the network to identify the Mobile System. The Authentication algorithm used in GSM system is known as the A3 algorithm. Most GSM network operators utilize a version of the COMP 128 algorithm as the implementation of the A3 algorithm. Although this wasn't actually intended as an algorithm but a placeholder, as it was designed as a reference model for GSM implementation, it was, however, adopted by most GSM providers worldwide (**www.ericsson.com/support/telecom/part-d/d-6-4.shtml**).

The K_i and the IMSI are stored in both the mobile and Authentication Center (AUC). This uses the K_i and IMSI, which are inputs to the A3 algorithm to calculate the 32-bit identification parameter called the Signal Response (SRES). In actual sense, A3 generates 128-bit output but only the first 32-bit form the SRES. SRES is calculated as a function of K and a 128-bit random number (RAND) generated by AUC (**www.nettwerked.net**) as shown in Figure 4 and then stored in the HLR for use in set-up procedures.

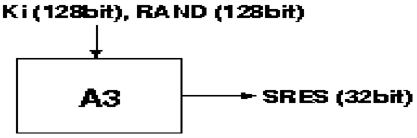

Figure 4: **The A3 Authentication Mechanism**

Set-up or registration will not be accepted until authentication, as in Figure 5, has been performed. Using the mobile system's IMSI, the MSC fetches the corresponding RAND and SRES from the HLR. RAND is sent to the mobile system, which uses its stored K value to calculate SRES. It then returns the calculated SRES to the MSC, where it is compared with the SRES value received from the HLR.[13] If the values tally, the set up is accepted, if not, it is rejected.

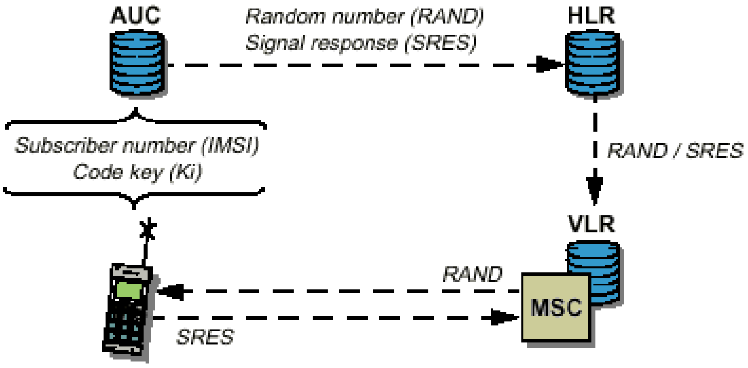

Figure 5: **Authentication in GSM**

Along side authentication, the key generation algorithm known as A8 algorithm, generates the 64-bit Session Key (K) from the RAND and K as in Figure 6. The session key K is used by the encryption algorithm A5 (**www.ericsson.com/support/telecom/part-d/d-6-4.shtml**).

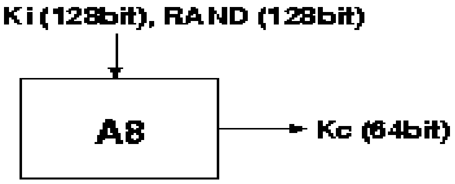

Figure 6: **The Key Generation Mechanism.**

2) Encryption.

GSM, which is a form of radio communication, can be intercepted by practically anyone in the immediate surroundings. Therefore, protection against eaves dropping is an important service in a mobile network. This is done by using an encrypted air interface both for traffic and control channels. Since encryption of voice requires digital coding, it cannot be used in analog mobile networks (**www.ericsson.com/support/telecom/part-d/d-6-4.shtml**).

The encryption algorithm used in GSM voice ciphering is a stream cipher known as the A5 algorithm. Multiple versions of A5 exists which implement various levels of encryption. They are

i) A5/0 which utilizes no encryption
ii) A5/1 which is the original A5 algorithm used in Europe
iii) A5/2 which is a weaker encryption algorithm created for export and used in the United States.
iv) A5/3 which is a stronger encryption algorithm created as part of the Third Generation Partnership Project (3GPP) (**www.gsmsecurity.com/faq.shtml**).

In A5/1 and A5/2, voice encryption is done using the calculated session key K_c, based on K_i and RAND by the AuC, in addition to the SRES it generates as shown in Figure 7. This key is stored in the HLR together with the RAND and SRES (**Isomaki: 1999**).

The mobile system also calculates a K_c values based on both the RAND value received from the MSC and on the K_i value stored in the mobile system. If the result of the authentication is approved, the MSC will also store the encryption key in the base station (via the BSC) for use in encryption/ decryption operations. The BSC then sends a “test signal” (encryption mode command) to the mobile system. In response, the mobile system should generate an encrypted signal (encryption mode complete) which if the BSC can interpret it, permits continued signaling and communication. This process is shown in Figure 8 (**www.ericsson.com/support/telecom/part-d/d-6-4.shtml**).

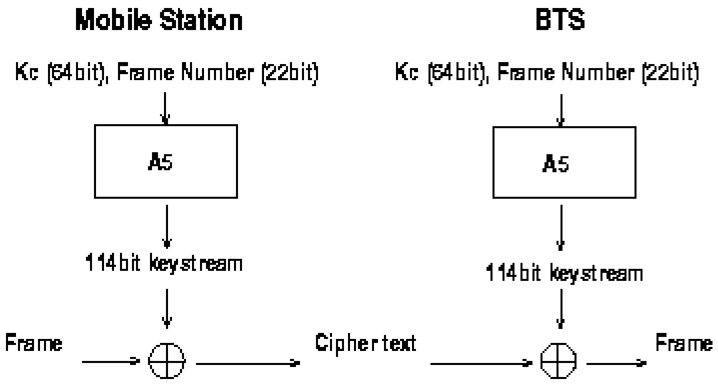

Figure 7: **A5 Ciphering Initiation**

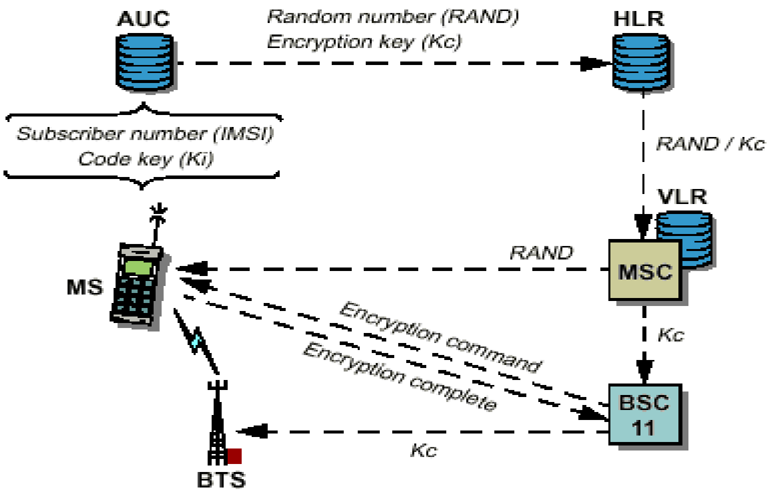

Figure 8: **Encryption in GSM**

A GSM conversation is sent as a sequence of frames every 4.6 milliseconds. Each frame contains 114 bits representing the digitized sender to receiver communication and 114 bits representing the digitized receiver to sender communication. For each frame, K_c is mixed with a publicly known frame counter Fn and the result serves as the initial state of a generator which produces 228 pseudo random bits. These bits are XOR'ed (using an exclusive-OR gate) by the two parties with the 114+114 bits of plaintext to produce the 114+114 bits of cypertext (**www.cryptome.org/a51-bsw.htm**).

For A5/1 algorithm, the 228 pseudo random bits are generated by three short linear feedback registers and the clocking is being controlled by a majority function of bits from the three registers. For A5/2 algorithm, four registers are used instead of three and this alters the control of the registers hence producing a non-linear function as output (**www.cryptome.org/a51-bsw.htm**).

3) Equipment Identification.

Equipment identification is a form of checking the mobile systems used within in the network. This is to ensure that no stolen or otherwise unauthorized mobile systems are used in the network. To this end, every mobile system in the network is provided with a tamper proof equipment number in the manufacturing process, called International Mobile Equipment Identity (IMEI). During the set-up phase, the MSC can request this number from the mobile system and then send it on for checking in the EIR (**www.ericsson.com/support/telecom/part-d/d-6-4.shtml**). If the number is barred or unknown, the set-up attempt is rejected.

4) Subscriber Identity Confidentiality

Subscriber identity confidentiality means that the operator tries to protect the users telephone number (the IMSI) from unauthorized tapping. A temporary mobile subscriber number (TMSI) is used in the dialogue between the mobile system and the network, except for the first contact attempt in a set-up phase. The MSC gives the mobile system a random IMSI for each set-up (**www.ericsson.com/support/telecom/part-d/d-6-4.shtml**).

Network Insecurities

Having looked at the various security procedures employed in the GSM network, it would be expected that a bridge of one of the processes will be close to impossible. However, over the years of the GSM deployment, a number of loop-holes have been found. The lapses discussed here are not all of the lapses found in the network but they are amongst the commonest.

1) SIM Attacks

The GSM SIM was originally designed to be tamper proof, copy proof and generally as difficult to break as possible. Overtime, series of issues have been discovered that have made the SIM less secure.

As earlier mentioned, the COMP 128 algorithm used for A3/A8 has many flaws which will be discussed later in this section. This makes it possible to obtain the Ki and the IMSI and these can be successfully used to program another SIM card using freely available tools and eventually "clone" a SIM[3]. SIM cloning which is made by breaking the COMP 128 algorithm could take up to 8-15 hours and requires physical access to the SIM (**Lord: 2003).** Nevertheless; a tool has been discovered to be popularly in use known as the

Dejan Karavic's SIM Scan. IBM researchers used 1000 randomly chosen inputs even though 500 random inputs should be sufficient and this reduces the amount of time to clone a SIM to minutes at most, seconds at best.

Researchers in IBM discovered a way of using side channels to obtain Ki (**www.research.ibm.com/resources/news/20020507_simcard.shtml**). This can involve as little as 8 well chosen plain texts or around 100 randomly chosen ones. By monitoring timing, power consumption and electromagnetic emissions, it is often possible to infer what is happening inside a device or system. Even though protection against Differential Power Analysis (DPA) has been implemented on the SIM, using a different form of input analysis ("partitioning attack") (**www.research.ibm.com/intsec/gsm.html**) and observing restrictions, addressing 9-bit quantities within 8-bit systems made it possible to determine which look-up tables were being accessed.

2) SMS Attacks

Short Message Service (SMS) popularly known as Text messaging is a huge source of revenue to any operator. Due to lack of education, it is generally trusted by people who choose to conduct business communication, disclose passwords or secret codes for Bank transactions, or receive system reports.

Job De Haans conducted a research on SMS and was able to crash (using a modified open source application) Nokia mobile phones. This seemed to be firmware specific but there are high chances of it being applicable to other phones. By using a broken User Data Header (UDH) within as SMS message, it was possible to crash Nokia 6210, 3310 and 3330 (**Lord: 2003).** Apart from crashing phones, he was able to Spoof SMS messages. It has been known that for sometime, originating address (OA) field in the SMS-DELIVER header can be arbitrarily set to anything using a variety of methods. For example, a strong trend of SMS Spam swept the UK, with most of them appearing to come from an invalid phone number. OA entries can even be alpha numeric which could hence complicate issues (**Lord: 2003).**

Flash messages (news flash, adverts) are those that immediately flash up on the screen and mostly sent by the network operator to supply services of discounts, bonanzas, etc. or just general network information. These messages could be sent from any mobile station and are immediately trusted by anyone. Alex DeLarge (**Lord: 2003)** pointed out that certain brands mobile phones software don't provide information about the originator of the message making it a significant target for use in social engineering attacks.

Using some specific software (Gnokii) (**www.gnokii.com**), it is possible to send a variety of messages to some handsets that the user might believe to come from the network provider. This same software could also be used to activate voice mail notifies on handsets or "ping" subscribers to see if their phones are switched on.

There are also faults in the area of cryptographic issues surrounding SMS. SMS default is sent in a predictable format, that is, in clear text form. When an SMS is sent from a mobile station to the service center (SC), it is in the SMS-SUBMIT format. The SC then sends a message to the recipient's mobile station in the format of an SMS-DELIVER. The structure of the SMS-SUBMIT and the SMS-DELIVER messages are different but still adhere to public standard and an SMS-SUBMIT's corresponding SMS-DELIVER is largely predictable. A message sender can also ask for a report, plus a report can be requested by the network to confirm the message was sent. The format of these reports is also reasonably predictable. Hence, it is possible to send certain SMS messages that will not alert the end subscriber but will still return a delivery report (**Lord: 2003).**

The signaling protocol used for transferring SMS messages known as Mobile Application Part (MAC) (**www.nettwerked.net**) within the various functions in the GSM network and also the protocols used between the MSC and BSC known as the Base Station Subsystem Application Part (BSSAP) are unencrypted protocols. Hence anyone interested can have access to the signaling system to read and modify information including SMS messages.

3) Encryption Attacks

Data in the GSM network have been said to be encrypted using the A5/1 or A5/2 encryption algorithm. A5/0 uses no encryption and it is deployed in countries with political obstacles in supplying cryptographic hardware. Examples of such are the former Soviet Union countries and some countries in the Middle East. A5/1, which is said to be the stronger of the two algorithms in use, has been studied by cryptographic professionals and mathematicians and has been discovered to be highly susceptible to cryptanalytic attacks.

Researchers like M. Briceno, R. Anderson, M. Roe and J. Golic (**www.cryptome.org/a51-bsw.htm**) had carried out various forms of attacks on the algorithm and their research have severed as the back ground for the most popular attacks on the algorithm. These attacks are the Baised Birthday Attack and the Random Sub graph Attack. The first attack requires two minutes of data and one minute of processing time while the second attack two seconds of data and several minutes of processing time (**Lord: 2003).** For each of these attacks, there are many trade-off parameters and three of them could be summed up in Table 1.

Table 1: **Three possible trade-off points in the attacks on A5/1.**[12]

Attack Type	Pre-processing steps	Available data	Number of 73GB disks	Attack time
Biased Birthday attack (1)	2^{42}	2 minutes	4	1 second
Biased Birthday attack (2)	2^{48}	2 minutes	2	1 second
Random Sub graph attack	2^{48}	2 seconds	4	minutes

The ideas used in these two attacks are not just restricted to this stream cipher but are applicable to other stream ciphers as well thereby bringing about new measures of security.

The non-linear output of the A5/2 algorithm as explained earlier makes it weaker than the A5/1 algorithm. Research has shown that the linear equations for the registers could be derived and solved from the output, thus making the algorithm less secure. Some other attacks on the A5 algorithm are the Brute-Force Attack, Divide-and-Conquer Attack (**www.chiark.greenend.org.uk/pipermail/uk crypto/1998-October/002552.html**). A3 and A8 are also susceptible to attacks since, as earlier stated, they are merely placeholders. These placeholders were used with a reference algorithm which was never intended to be actually used but like many reference algorithms, it was adopted as a standard through out the world (**www.cryptome.org/a51-bsw.htm**).

Another possibility is that someone will be able to crack the A8 key generation algorithm and retrieve the secret key, K_i, based on the random challenge, RAND, the session key, K_c, and the SRES response (assuming the same algorithm is used for both A3 and A8 as is the case with COMP128) with a minimal amount of work. For example, the attacker may find a RAND that produces the K_i as a result (an over simplified example). All three variables are obtained relatively easily. The RAND and SRES are sent over the air in plain text and the session key K_c can be relatively easily deduced from the encrypted frames and the known plain text given enough time. Vulnerability like this in the key generation algorithm would of course devastate the whole GSM security model and give the GSM Consortium something to think about when designing their next security algorithms (**www.chiark.greenend.org.uk/pipermail/uk crypto/1998-October/002552.html**).

4) Signaling Attacks

The A5 algorithms provide security for over the air interface for transmissions between the MS and the BTS. They are able to prevent to a certain level over-the air call interception and real time encryption cracking. After the BTS, traffic is transmitted in plain text within the operator's network (**www.gsmclone.net**). This means that if the attacker can access the operator's signaling network, he will be able to listen to everything that is transmitted including the actual phone call as well as the RAND, SRES and $K_{c.}$ The signaling protocol, SS7, used in the GSM signaling network is completely insecure if the attacker has access to it (**Lord: 2003).** Alternatively, the attacker could access the HLR to retrieve the Keys but this is lee likely due to the high security in relation to the HLR.

The connection between the BTS and the BSC could be through cables, microwave links or satellites as the case may require. In cable connections, careful implementations of attack could go undetected for a long period of time. For microwave links, the air interface may be encrypted in some cases. This encryption is based on hardware and the specifications are available to law enforcement personnel and such. Generally, accessing the BTS and BSC transmission would enable the attacker eavesdrop on calls or retrieve the session key, K_c , by monitoring the channel, intercepting the call over the air interface and decrypting it instantly. With the knowledge of the K_c, the real-time encryption is not a problem.

In the GPRS network, the Serving GPRS Support Node (SGSN) is used to authenticate the MS instead of the MSC. It delivers packages to the MS through the multiple BTS's and communicates to the HLR when authenticating the MS to enable encrypted communications. Frames sent from the MS to the SGSN are in cipher text form because the network uses multiple time slots in parallel in order to achieve greater transmission rates. The BTS is unable to put the different frames in to different time slots since it sees them as separate calls. It is also unable to decrypt the frames because consecutive frames have not got consecutive frame numbers, hence the SGSN is needed to decrypt the frames and keep track of the frame numbers, as shown in Figure 9. Since decryption of the frames is done at the SGSN, there are lower chances of eavesdropping in the network since the frames are still encrypted between the SGSN and the BTS (**Lord: 2003).**

Generally, the security of the GPRS network largely depends on the positions of the SGSN in the network architecture and on their security. If they are vulnerable to attack, the authentication triples as well as the network are vulnerable.

SUGGESTIONS ON MITIGATING SECURITY THREATS

Most of the security threats in the GSM Network could be subdued even though it might be cost intensive. Signaling security treats require physical access to the signaling link and/ or operator's console. Hence operators should establish regular assessments to ensure that other systems (cables or SGSN in the GPRS Network) are not at risk of compromise from the attackers. The cost associated with compromise of operator systems could be immense and is unlikely to be detected unless the service is interrupted (**Lord: 2003).**

In the Authentication Center, the whole authentication could be broken down in to several security domains, each having its own unique security configuration. This will obviously be cost implicative but the system is less vulnerable to attack and this approach confines the damage of a compromised certification within a singe security domain. Unless all certification centers are compromised, no key can be forged (**Isomaki: 1999).**

In securing the A3 algorithm from crypto attackers, the most efficient approach will be to use a more cryptographically secure algorithm. This will imply new SIM cards to all subscribers and updating HLR software; only when this is done can SIM cloning, which is one of the most dangerous attacks, be minimized the most. Here, there is no need for hardware or software manufacturers' support or permission from the GSM Consortium. The main draw back, however, is the cost implication and the tedious tasks of redistributing new SIM cards to "all almost 1 billion" GSM subscribers (**Laurie: 1999).**

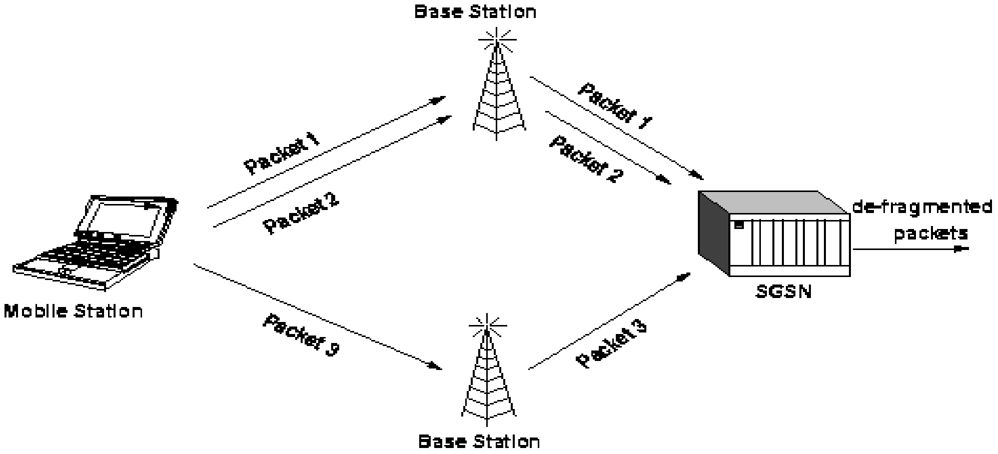

Figure 9: **GPRS Network Architecture**

For the A5 crypto attacks, a strong encryption is required. This will prevent the attacker from recording transmitted frames since he most likely will not be able to crack them. Implementing this will involve the equipment manufacturer and the GSM Consortium. The hardware and software manufacturers will need to release new versions (**www.chiark.greenend.org.uk/pipermail/ukcrypto/1998-October/002552.html**). Also, the network will be more secured if the traffic on the operators back bone is encrypted to avoid wire tapping signal interception (**www.nettwerked.net**). This implementation will only involve the hardware and software manufacturers.

IBM Researchers have developed a new method of protecting the SIM from partitioning attacks. This is done by replacing the single data table contained in the SIM with a sequence of table look-ups at completely random locations and this makes leaking of information out of the SIM very difficult. Application of this method has been possible since very little memory is involved in regard to the SIM. Subscribers should also be adequately educated and warned of the danger involved in careless handling of their SIM (**www.research.ibm.com/intsec/gsm.html**).

For SMS security, a protocol should be developed with the responsibility of tracking SMS paths. This will make detection of SMS sources possible and fraudulent activities will be minimized. A specific encryption algorithm could be deployed for SMS transmissions and this only be decrypted by the receiver similar to Public Key Infrastructure (**Mu'azu and Dangana: 2004**). Only after decrypting the message should a delivery report be sent by the receiver to the network and then to the sender.

Conclusion

Security is one of the most important requirements to the wide acceptance of personal communication and it is said to be as strong as its weakest link. Any operator that compromises network security is at the verge of a major business collapse as a result of the possible loss of confidence.

However, the security protocols employed in the GSM Network which are Authentication, Encryption, Equipment Identification and Subscriber Identity Confidentiality have not been as secure as expected. This is because lapses like SIM, SMS, Encryption and Signaling Attacks have been possible. Therefore, improvements on the signaling link, Algorithms used, SMS Service as well as on the SIM itself are highly recommended. These and many other suggestions, considered in detail, will improve the GSM Network Security.

References

1) **Ericsson Telecoms (1998), "**Understanding Telecommunications", Telia and Studentlitteratur.
2) **Isomaki, M. (1999)**, "Security in the Traditional Networks and in the Internet", White Paper, University of Technology, Helsinki.
3) **Laurie, P. (1999),** "GSM Interception", White Paper, University of Technology, Helsinki.
4) **Lord, S. (2003)**, "Modern GSM Insecurities", X-Force Security Assessments White Paper.
5) **Mu'azu, M. B. and Dangana, D. S. (2004)**, "Public Key Infrastructure (PKI) and Biometrics as Security Applications Over the Internet: An Overview", Samaru Journal of Information Studies, Vol. 4, No.1&2, pp5-11.
6) **Wetten, L. A. (2003)**, A Study of GSM Technology in Nigeria and its Place in the International Scene**,** Unpublished (B.Eng) Final Year Project, Federal University of Technology, Minna.
7) **www.nettwerked.net, "**GSM Security Technical White Paper For 2002"
8) **www.chiark.greenend.org.uk/pipermail/ukcrypto/1998-October/002552.html,** "Status of GSM Crypto Attacks"
9) **www.gsmclone.net**, "GSM Cloning: How it Works"
10) **www.cryptome.org/a51-bsw.htm**, "Real-Time Crypto Analysis of A5/1 on a PC"
11) **www.gnokii.com**
12) **www.research.ibm.com/intsec/gsm.html**, "Partitioning Attacks: How to Rapidly Clone Some GSM Cards"
13) **www.research.ibm.com/resources/news/20020507_simcard.shtml**, "IBM Research News"
14) **www.ericsson.com/support/telecom/part-d/d-6-4.shtml**, "Understanding Telecommunications"
15) **www.gsmsecurity.com/faq.shtml**, "GSM Securities: Frequently Asked Questions"
16) **www.gsmworld.com**, "Today's GSM"