PROVIDING END-TO-END SECURE COMMUNICATIONSIN GSM NETWORKS

Heshem A. El Zouka

Department of Computer Engineering, College of Engineering and Technology, Arab Academy for Science & Technology and Maritime Transport,
Alexandria, Egypt

ABSTRACT

The broadcast nature of radio medium in GSM networks makes them more vulnerable to various attacks. Any attacker can have complete control over the communication channel, listen to phone calls, read email, and spy on whatever data has been sent via GSM mobile communication system. This paper introduces a middleware security system that aims to protect the GSM communication channel and minimize the computational overheads of the provided authentication and cryptographic schemes of the network The proposed scheme supports an end-to-end secured communication between the GSM mobile devices and the GSM base stations; insure compatibility between wireless GSM devices (telephones, PDAs, etc.), and easy to install without any modification of the current systems

KEYWORDS

GSM Security, Authentication, Privacy, ECC, Mobile Communication, Integrity.

1.INTRODUCTION

Some good practices have been recently used to secure data in GSM networks and make them aware of the information they store and share on their devices. Over the past few years, a significant amount of malware and malicious code for Android and other platforms has increased dramatically. Compared to conventional computers, the threats to mobile platforms increased exponentially, including malware, communications interception, and exploitation and misconduct. Securing such devices, then, is quite important and more attention should be paid to it, as heavy date exchange and computing power prevail in every single domain [1].

Rapidly, different security measures have been developed to secure mobile communication systems and security countermeasures have been adapted to different layers of software supported on these GSM networks to secure the data they access and the shared information between GSM devices [2], [3]. To secure data in GSM, it has been suggested that the data should be encrypted using light weight encryption techniques such as stream cipher. The majority of encryption models that aim at preventing intruders from hacking mobile communication networks use stream coding based on linear feedback shift registers (LFSR). LFSR is a device that generates long binary streams and is very familiar to most cryptographers and coding scientists. In contrast; LFSR is used in mobile communication to generate a session key. Implementing the next key function of an LFSR in hardware requires only a few XOR gates. However, LFSR needs hardware implementation and cannot be used directly to generate suitable session keys. In our mode, a random number generator combined with RC4 stream cipher is used to generate the session keys [4].

DOI : 10.5121/ijnsa.2015.7402

GSM then employs the session keys for encrypting whatever data is going over the GSM channel. The proposed method is simple to implement and provides a robust approach to secure confidential data in GSM communication networks [5]. In addition, this method does not require any hardware implementation as compared to LFSR which requires the system to be implemented in hardware, and hence minimizing both the hardware overhead and the impact on system's performance. In the following sections the proposed algorithm will be described in details. In Section III the related work in the area of research is briefly discussed. In Section IV, the security requirements and concerns of GSM systems are introduced and the importance of protecting GSM mobile communication is discussed. Section V elaborates the proposed encryption algorithm which uses the random number generator to scramble the data sent over GSM networks. The experimental results are discussed in Section VI followed by conclusions drawn in Section VII

2.RELATED WORK

An LFSR is a simple logical circuit used to encrypt mobile phone conversations in GSM mobile communication. The purpose of this circuit is to transform a sequence of binary bits into long pseudo random sequence, where this sequence number can provide security for encryption [6]. The register of LFSR consists of a finite number of processes that are initialized by a set of initialization vectors (IV) of zeroes and ones; that is, most often, the session key.

The problem is how to design LFSRs with long periods. Such work is pioneered by some researchers, showing the best LFSR designs is related to primitive polynomial function and controlled by a clock. For each clocking pulse, the contents of the IV are shifted by one position and XORed with some other stream of bits [7]. During this process, one bit is generated as an output from the LFSR circuit. Nowadays, LFSRs have extensive military, industrial applications. LFSR is more efficient using hardware implementation and is known to produce a large sequence of bits with good polynomial properties.

However, the linearity of these generated sequences makes them potentially vulnerable to linear algebraic attacks. The use of LFSRs on their own, however, is insufficient to generate suitable key streams [8]. Often IV is applied to ensure varying key streams as shown in figure 1.

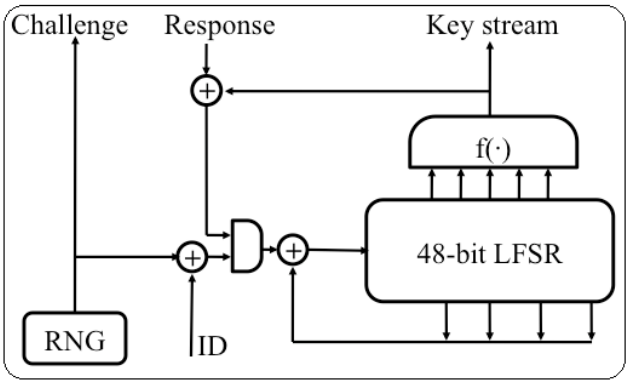

Figure 1. An additive stream cipher design

Several techniques for improving the linear complexity of LFSRs output sequences have introduced related work done in the literature. For example, in step generator, the LFSR system comprises three linear feedback shift registers, and the output of each register decides which of the other two is to be clocked to generate the output sequence. The initial vector of the three

LFSR is the key. An alternating stop-and-go generator consists of two LFSRs, where one of them is clocked if the output of a second is "1", otherwise it repeats its previous state. Other implementations pass the entire state of a single LFSR register into a non-linear filtering function in order to use nonlinear update function and hence improve the security of LFSR systems. The shrinking generator LFSR based key stream generator was proposed by coppersmith et al. [9] to be used in stream cipher applications and their variations are attractive because of regularity, scalability, and conceptual simplicity. Recently, several modifications of stream cipher have appeared in the literature of cryptography and key generations [10].

In GSM, A5 stream encryption is used [11]. Indeed, GSM features four A5 encryption models, namely A5/0, A5/1, A5/2, and A5/3. There is no encryption used on A5/0 algorithm and it is basically a plaintext. A5/1 is the original A5 algorithm used in Europe. A5/2 is a weaker encryption algorithm that was created for export, and attacks were rapidly found for this algorithm. Obviously, most of these encryption models suffer from small key space with a max length of 64 bits, which make them vulnerable to attacks.

Alternatively, A5/3 is a strong encryption model created as part of the third generation partnership Project to provide GSM mobile phone users with high level of security, and protect their valuable information such as telephone numbers, voice calls, email addresses, and so forth. A5/3 algorithm is based on the KASUMI algorithm that is specified in reference [12]. Although the algorithm were assumed to be secure, Biham et al attack on GSM A5/2 shows that the session key can be compromised by an adversary with sufficient access to the GSM data.

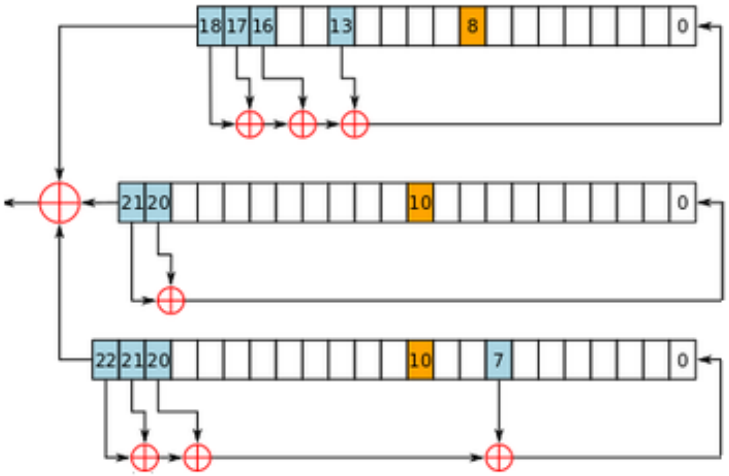

Figure 2. The operation of the keystream generator inA5/1, an LFSR-Based stream cipher used to encrypt mobile phone conversations

3.SECURITY REQUIREMENTS AND COUNTERMEASURES

Over the past few years, a significant amount of malware and malicious code for Android and other platforms has increased dramatically. Compared to conventional computers, the threats to mobile platforms increased exponentially, including malware, communications interception, and exploitation and misconduct. However, only 10% of the users of smart phones and tablets have installed security protection systems. In contrast, there are three main types of attacks on mobile devices [13].

Firstly, the confidentiality attacks, particularly on sensitive information that is shared on devices. It has been suggested that the data should be encrypted using light weight encryption techniques such as stream cipher. However, the fact that mobile devices resynchronies the stream cipher of every packet sent means that malicious users attempting to break the cipher in this way would not have sufficient time to succeed. If a device's session key is used as a trust key, legitimate devices can spoof that device and can intercept communications between that device and another which uses the session key as a trust key. One way to avoid this type of attack is by using user identity or user-specific encrypted contents shared on the device such as data related to mobile phone carriers and contracts, locations, etc.

Secondly, the privacy attack, which is another important security issue [14]. Since the address of the mobile device is freely available, once it is associated with an individual it can be used to carry out sensitive data, and other more questionable forms of attacks, violating user privacy. Security measures should be implemented in such wireless networks to protect the privacy of the users. For example, in order to construct a mutual authentication link between two communicating users, they need to use a lightweight encryption model that preserves their privacy [15]. For example, CDMA and GSM automatically support privacy protection with a scrambling function for all calls to make conversations incomprehensive to intruders [16]. Global system for mobile communication) (GSM) is more common in Europe and uses a stream cipher algorithms such as A5/1 algorithm, to protect the security and privacy of point-to-point wireless communication systems. However, in U.S.A, Code Division Multiple Access (CDMA) technologies use spread spectrum technique to provide strong protection system which makes it difficult to be intercepted except by skilled hackers and law enforcement [17].

Finally, the availability, or the possibility of making mobile frequencies unsusceptible to interfere from other devices, such microwaves. For example, Bluetooth technologies in mobile devices use the technique of frequency hopping, which improves the clarity and discourages casual eavesdropping. Another form of availability attack is the battery exhaustion attack. Unfortunately, it is very difficult to prevent this kind of attack without restricting the usability of the device.

4.VULNERABILITIES, THREATS, AND ATTACKS

The more application and software that recent mobile devices get connected to through the internet, the more vulnerable these devices become. It is extremely important now to separate the network traffic from the databases where sensitre information is stored, as both the mobile network users and their data are both monitored. This isolation and self-sufficiency is not on easy task though, because the resources on these devices are relatively limited in computing capabilities if compared to conventional PCs. Moreover, the lack of security on a network, and the problem of mutual authentication between mobile users are considered vulnerability. Also, information leakage through attacks posed by masqueraders of any kind and through any communication medium represents vulnerability [18].

As many devices use verified application markets such as Google play and App store where there is some control through a review of vendors and where approved applications distributed on these devices, still some other web applications may not be trusted. Moreover, the lack of security on a network, and the problem of mutual authentication between mobile users are considered vulnerable. Such vulnerabilities result from installing malicious codes, threats from malicious users, external attacks, or even internal malicious users who attempt to exploit vulnerabilities in these mobile devices in a manner similar to the way it is done in traditional computer systems.

Threats and attacks which affect mobile devices do not come close to the number of attacks that affect traditional computers, but they do exist. Android, in particular, has suffered attacks due to the use of third party hosted sites, and due to open application market. But even those with strong security aspects like BlackBerry have been suffering from attacks too. Mobile malware includes also fake Internet banking applications which steal confidential information and money, and in some cases steal online transaction authentication code sent by a bank to users' mobile devices via text messaging [19]. It is quite important, then, to deploy the applications which guarantee privacy and integrity of the information they handle. However, mobile messages could be corrupted due to malicious attacks or even due to network malfunctioning. So, it is important to protect the GSM communication network from any third party attacks, such as data modification, identity theft, spoofing, or any other malicious attacks. GSM network may face also threats from passive attacks as eavesdropping and active attacks as impersonation which lead GSM network to degrade its performance and resources.

To ensure protection against attackers, GSM cell-phones employ a set of cryptography protocols and algorithms to provide encryption and authentication [20]. The encryption algorithm used in GSM cell-phones to protect the actual communication transmission is the A5/1 as mentioned in the previous section of this paper. The A5/1 algorithm has been under attack for long time. The general idea of an attack in GSM network is to determine the session key for a particular piece of encrypted data (transmission in this case).

Then, the progress of the deciphering process can be followed, and effectively all data after that point can be decrypted. Thus, breaking a cryptographic algorithm is actually the computation of the reverse-engineering process of the stream cipher used in most GSM mobile systems. For example, if a cryptographic algorithm leads to an “n-bit” output, there are two straightforward methods to break the algorithm ; either by an exhaustive search for all possible keys until the target key is reached, or by applying pre-computing attack where 2n of input output pairs are stored in a table for further analysis.

5.THE ALGORITHM

Each SIM card in its GSM mobile terminal (MT) contains a different 128 bit secret key Ki (random challenge), known only to it and to the base station (BS) of the GSM network. When a GSM phone call is being processed, the BS sends via the network a generated 128 bit random number to the SIM of the MT. The SIM uses a hash function called A3 to generate a 32-bit random challenge (SRES), and send it back to the base station.

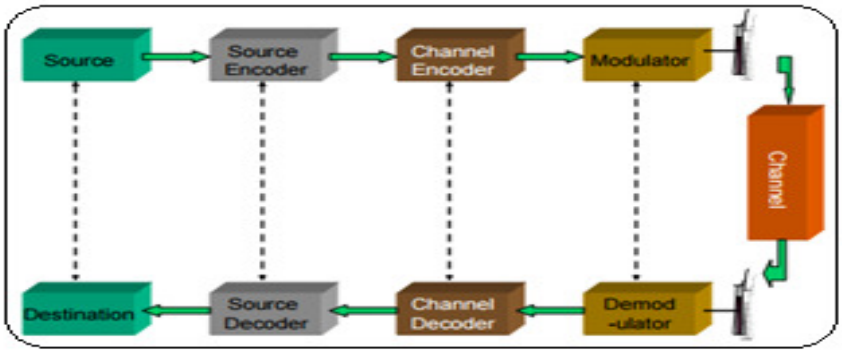

Figure 3. Typical wireless communication system

The BS compares the received SRES value with the computed one by using its own copy of the RAND challenge and the private key Ki [21]. If they are matched, the BS believes that the SIM is authentic and the call is allowed to proceed.

The call exchanged between the MT and the network is encrypted using an encrypted algorithm called A5 to produce a 64 session key Ks. Thus, for each new call the required A5 session key Ks is generated using a hash function called A8 which take the same 128 bit key Ki and 128-bit key to produce the 64 bit session key Ks. However, the authentication module only works between the BS and the mobile terminal and cannot provide end-to-end secure communication in the GSM network.

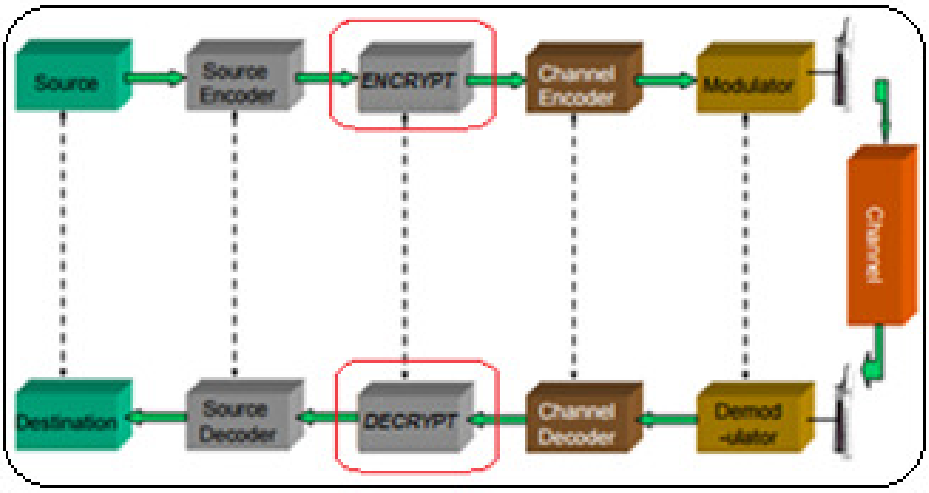

Figure 4. END-TO-END Security Model

Figure 3 illustrates a block diagram of the GSM data transmission. As shown, the block diagram consists of four main subsystems: a source encoder/decoder subsystem, channel decoding/encoding subsystem, and modulation/demodulation subsystem.

In case of wireless connection, the A5 security subsystem can function as an encryption/decryption module. Obviously, the system does not support end-to-end security, since the communicated data are protected only by the BS which involves two separate security channels.At the transmitter side, the source encoder converts the analog or digital information source to a sequence of binary digits by an A/D converter, including sampling at 8 KHz sampling rate. It usually generates 14-16 bits/sample. Before the sampling the direct component is removed by the FIR filter, and the transmitter pre-emphasis uses high-frequency boosting to enhance the high-frequency content of the signal.

The data is then sampled and broken into frames, and the coder operates on 160 sample frames that span 20ms. The linear predictive coders (LPC) filter takes a digitized signal and generates a set of predictive coefficients as well as a set of error coefficients (residual signal). Finally, long term predication (LTP) is used to eliminate the redundancy in digitized signal. At the receiver side, the process is reversed to obtain and decode the original data.

In the GSM system, the encryption-decryption subsystem takes place before modulation subsystem, which is easy to implement in the mobile terminal. However, it is highly desirable to have end-to-end secure protocol over the communication channel. In order to achieve end-to-end

secure communication, data must be encrypted before it enters the GSM network. An encryption module that enables end-to-end secure communication over the GSM channel is proposed. The proposed scheme does not require any modification in the BS neither the GSM standard. It only requires a small modification on the mobile terminals.

A real-time prototype is implemented demonstrating the end-to-end secure data communication over the GSM network. As illustrated in Figure 5, the security algorithm is inserted between the source encoder and the channel encoder of the MT, so that the coming signal from the source encoder subsystem would firstly arrive to the newly-added data Encryption/Decryption module and finishes the encryption. After that, it is sent to the channel module.

Hence, this encryption method must penetrate the RPE-LTP vocoder and have ideal encryption intensity. Simultaneously this encrypted signal can be recovered to get the original understandable data at the receiver. This proposed encryption method is a kind of signal source encryption technology, so it could achieve the end-to-end secured communication.

6.SECURITY ANALYSIS

This section discusses the results of the proposed method. It also presents the obtained driving strategies and the test cases that show how the system is secured, In order to implement such strategies, one must go through several steps which were discussed in details in the preceding sections. It is among all base stations and mobile terminals of the same traffic type. A key is used to secure communications between mobile terminals as well as decipher broadcast frames from the terminals. The following notation is used throughout the remainder of this section: BS and MT refer to Base Station and Mobile Terminal.

- K is a private key, whereas EC is an elliptic curve [22] and G the generator number.
- M is a message (stream of bits) and C is the cipher.
- R( ) is a family of pseudo-random numbers [23].
- AC (C, K) is an authentication code to the encrypted data which uses the same Key.

It is assumed that the communication between the Base Station Transceivers (BST) and Base Station Controllers (BSC) is highly secured. Messages between base station and mobile terminals are encrypted by ECC algorithm [24].

The advantage of using ECC is that it provides an equal security as RSA but with less overhead in the processing of messages [25]. Thus, to secretly communicate with each other, mobile terminals must have keys which are known only by the communicating terminals. A random public point G is chosen on the elliptic curve EC to produce a compressed public key [26].

In addition, BS chooses a random number RBS (its symmetric key), then the BS computes it session key SRBS = RBS * G . Mobile terminals also compute shared session key that each one share with the BS. The shared session key is computed by:

$$K = KMT * SRBS = KMT * RBS * G$$

This private key is used to secure communication between the base station and the mobile terminals. The cipher C is used to denote the encrypted message M with the shared session key K. After this message is encrypted, the authentication process takes place [27].

In order to verify data authenticity and integrity of the message M, it uses a key to authenticate messages, for example; MD5 [28]. The messages sent by mobile terminals to the BS are with the following structure:

$$MC = SRBS + C + AC (C, KF)$$

It is assumed that the BS has a powerful computing power and more energy than regular mobile terminals. Thus, after establishing the first channel of communication between the BS and mobile terminals, the BS authenticates the shared session key until the end of the session. Therefore, after authenticating keys, messages are coded as shown.

$$MC = C + AC (C, KF)$$

In this manner, the BS also distributes and authenticates session keys to the communicated mobile terminals. In the following section, the security analysis and simulation results are discussed.

7. EXPERIMENTAL RESULTS

To simulate the results, it is assume that an intrusion detection mechanism is implemented, and the intruder can launch a number of attacks as mentioned in the previous sections of this paper. The radio channel performance impact on the applied security protocol has been evaluated by means of the provided security protocols.

The simulation models the proposed security protocols including the accumulated latency of the processed frame, and compares it with a standard GSM model. The security model that is included in the simulator is a two layer of communication added to the modulation and demodulation modules as described in Section VI.

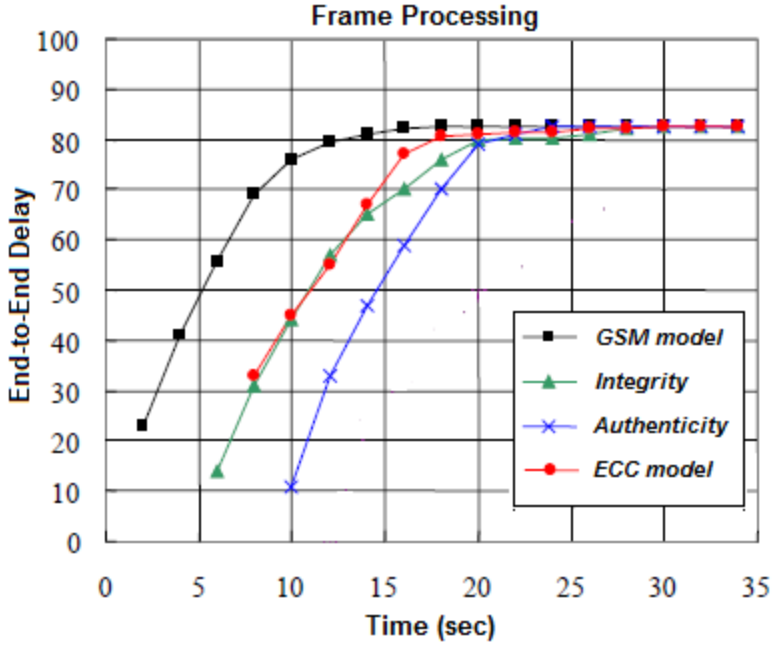

Figure 5. Performance Analysis of the Applied Security Protocols

The output security parameters of the simulator are framed at the output of the decoder and the security measures is obtained. The security model evaluation is illustrated in figure 5 for the GSM codec output for three different security parameters as a function of the proposed security protocol.

For each experiment, the traffic generation rate was varied from 5 to 28 Kbits/s. The average GSM end-to-end delay was measured. Each simulation was executed during 50 seconds, and the accumulated latency of the applied security protocols was computed as shown in figure 6.
If a mobile terminal is compromised and detected, the BS starts rekeying process of the effected channel. Then, the BS sends a message to the communicating terminals to erase the individual key used to communicate with previous compromised MT. In addition, the messages exchanged by mobile terminals are authenticated by AC [29]. Therefore, any message alteration makes the AC inconsistent and the message will be discarded. In order to alter or spoof a message, the adversary must have some information about the session key that has been used.

The attacker may also create malicious attack in attempt to drop some messages or perform a forward/replay attacks. The provided authentication protocol guarantees authenticity of the messages and their sources. As the mobile terminals share individual keys with their base stations, an attacker may impersonate any MT only if it has access to other identity keying materials.

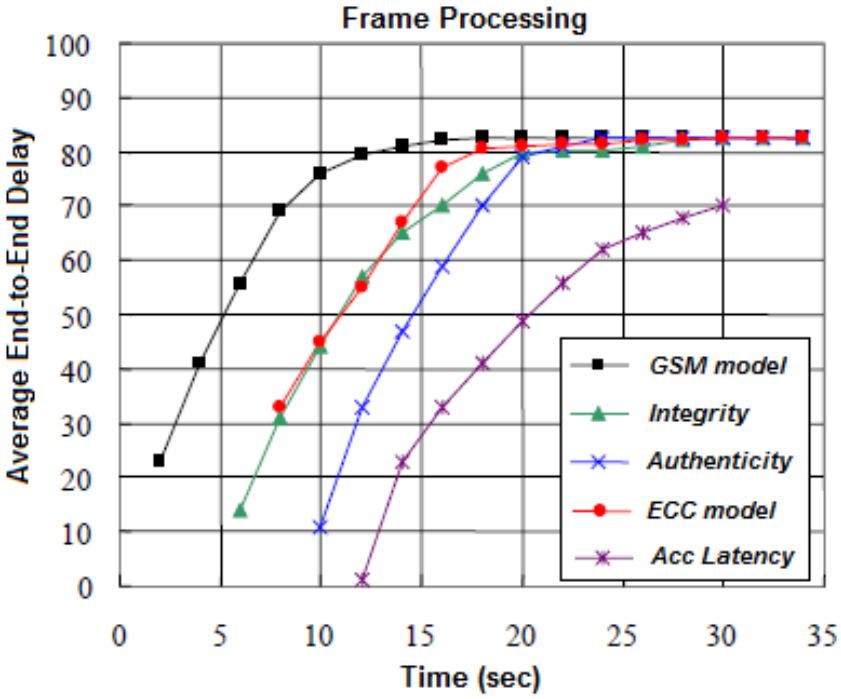

Figure 6. Average End-to-End Delay

In addition, the computing overhead of ciphering message are shown using ECC and AC on figure 5. Since it is more costly to transmit an ECC message than other unprotected messages, the ECC message were only used to perform very secure communication tunnel between the communicating mobile terminals. Figure 5 shows the impact of security policies on network traffic and estimated end-to-end path delay.

The experiments were conducted using the NS2 network simulator to evaluate the robustness of installing a security middleware on mobile terminal platform.

The performance of the proposed system was measured. In order to validate this contribution, we present the results of experiments showing the performance and efficiency of this approach was presented.

8.CONCLUSION AND FUTURE WORK

Mobile terminals are exposed to numerous security attacks that can adversely affect the success of GSM applications. Thus, securing GSM networks from these attacks is a challenging task due to its limited capabilities, and due to their wireless nature. In this paper, a middleware security system for GSM network was proposed. The middleware aims at providing end-to-end confidentiality, authenticity, and data integrity.

In addition, it also aims at minimizing the computational power of the mobile terminals. The proposed model uses a lightweight authentication and cryptographic schemes that aim at minimizing the computational and network overheads. By combining MT authentication and signaling encryption protocols a middleware system that can detect an intrusion with a great degree of accuracy was created. Moreover, BS capabilities were taken advantage of efficiently distribute the symmetric session's keys in large scale GSM network.

The middleware system protection is efficient against a number of attacks either by preventing them or minimizing the intrusion they may cause. In terms of computational power and performance, the results obtained show that the proposed system does not have a great impact on the mobile terminal resources.

For future work other security protocols are to be analyzed to test the effectiveness of the middleware security system on a larger scale mobile trafficking systems.

9.REFERENCES

[1] David G. W. Birch and Ian J. Shaw, “Mobile communications security private or public”, IEEE, June 1994.

[2] Dr. S. Muhammad Siddique and Muhammad Amir, “GSM Security Issues and Challenges” , SNPD’06, 2006.

[3] Slim Rekhis and NoureddineBoudriga, “Wireless Communications Security”, Ed. John Wiley & Sons, Ltd, 2010.

[4] Lakhtaria K. Protecting computer network with encryption technique: A Study. International Journal of u- and e-service, Science and Technology, vol.4, issue 2, 2011.

[5] Chomsiri, T.: A Comparative Study of Security Level of Hotmail, Gmail and Yahoo Mail by Using Session Hijacking Hacking Test. International Journal of Computer Science and Network Security IJCSNS, vol. 8, pp. 723-733, 2008.

[6] Koblitz, N.: A Course in Number Theory and cryptography. 2'nd edition.Springer-Verlag, 1994.

[7] Qiyan Wang, Khurana, H, Ying Huang, Nahrstedt, K, “Time Valid One-Time Signature for Time-Critical Multicast Data Authentication”, IEEE-Infocom, pp 19-25., April 2009.

[8] AtulChaturvedi, ShyamSundar, “A Secure Key Agreement Protocol Using Braid Groups Department of Mathematics”, Internationnal Journal of Advanced Networking and Applications (IJANA), vol. 01, issue 05, pp. 327-330, 2012.

[9] Don Coppersmith, ShaiHalevi, and CharanjitJutla. Cryptanalysis of stream ciphers with linear masking. In Moti Yung, editor, Advances in Cryptology CRYPTO 2012, volume 2442 of Lecture Notes in Computer Science, pages 515–532. Springer Berlin Heidelberg, 2012.

[10] L.Lamport, "Password Authentication with Insecure Communication", Communications of the ACM, vol. 24, issue 11, pp 770-772, November 1981.
[11] Ross Anderson, Mike Roe "A5 - The GSM Encryption Algorithm", 1994.
[12] 3GPP Organizational Partners. Specification of the 3GPP confidentiality and integrity algorithms – document 2: KASUMI specification (3GPP TS 35.202 version 7.0.0 Release 7), 2007.
[13] Hoshizawa, Y., Are Java-Enabled Mobile Phones Secured?, in U. Gattiker, ed., 'EICAR Conference Best Paper Proceedings', European Institute for Computer Anti-Virus Research (EICAR), pp. 141–151, 2002.
[14] SearchSecurity, definition Encryption [online] available at: http://searchsecurity.techtarget.com/definition/encryption. Accessed on August 2014.
[15] H.Imai, M.G. Rahman, K. Kobara "Wireless Communications Security" ARTECH HOUSE, 2006.
[16] Kiran Kumar, M., MukthyarAzam, S., and Rasool, S.: Efficient digital encryption algorithm based on matrix scrambling technique. International Journal of Network Security and its Applications (IJNSA), vol. 2, issue 4, 2010.
[17] Maria Striki, John S. Baras, "Towards Integrating Key Distribution with Entity Authentication for Efficient, Scalable and Secure Group Communication in MANETs", IEEE International Conference on Communications, Vol.7, Inst. for Syst. Res., Maryland Univ., College Park, MD, USA, pp 4377 – 4381, June 2004.
[18] Goldwasser, S., Micali, S., L.Rivest, R.: A Digital signature scheme secure against adaptive chosen-message attacks, SIAM Journal of Computing vol.17, pp. 281-308, 1998.
[19] Tang and D. O.Wu, "An Efficient Mobile Authentication Scheme for Wireless Networks", IEEE Transactions on Wireless Communications, vol. 7, issue 4, pp. 1408 - 1416, April 2008.
[20] Stefan Piitz, Roland Schmitz, Friedrich Tonsing, "Authentication Schemes for Third Generation Mobile Radio Systems", The Ninth IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, Boston, MA , USA, vol.1, 8-11, pp 126 – 130, Sep 1998.
[21] Ramaraj, E., and Karthikeyan, S.: A New Type of Network Security Protocol Using Hybrid Encryption in Virtual Private Networking. Journal of Computer Science vol. 2, issue 9, 2006.
[22] Koblitz, N.: Elliptic Curve cryptosystems, Mathematics of Computation, vol. 4, pp. 203-209, 1987.
[23] Singh, A., Gilhorta, R.: Data security using private key encryption system based on arithmetic coding. International Journal of Network Security and its Applications (IJNSA), vol. 3, issue 3, 2011.
[24] P. Bh, D. Chandravathi, and P. Roja, "Encoding and decoding of a message in the implementation of elliptic curve cryptography using koblitzs method," International Journal on Computer Science and Engineering, vol. 2, pp. 1904–1907, 2010.
[25] Ammayappan, K. Saxena, A. Negi A, "Mutual Authentication and Key Agreement based on Elliptic Curve Cryptography for GSM" , International Conference on Advanced Computing and Communications (ADCOM), pp 183 – 186, Dec 2006.
[26] Rivest, R.L., Shamir, A and Adelman, L.: A method of obtaining digital signatures and public key cryptosystems. Comms.ACM, vol 21, issue 2, 1978.
[27] Pieprzyk, J. and Pointcheval, D.: Parallel Authentication and Public-Key Encryption. The Eighth Australasian Conference on Information Security and Privacy (ACISP '03). Wollongong, Australia) R. Safavi-Naini Ed. Springer- Verlag, LNCS, 2003.
[28] Rivest, R., The MD5 Message-Digest Algorithm. Network Working Group (April 1992), http://www.ietf.org/rfc/rfc1321.tt. Accessed on August - 2014.
[29] James, Birkett, Stebila, Douglas, "Predicate-Based Key Exchange", Information Security and Privacy: Proceedings of the 15th Australasian Conference, ACISP '11, Springer, Macquarie Graduate School of Management, Sydney, 2011.