I. J. Computer Network and Information Security, **2016, 1, 1-8**
Published Online January 2016 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2016.01.01

Secure Model for SMS Exchange over GSM

Mohammed Baqer M. Kamel
University of Kufa, Najaf, Iraq
Email: mohammedb.kamel@uokufa.edu.iq

Loay E. George
University of Baghdad, Baghdad, Iraq
Email: loayedwar57@scbaghdad.edu.iq

Abstract—Distributed systems use General Packet Radio Service (GPRS) to exchange information between different members of the system. The members of the system depend critically upon their ability to access internet connection in order to exchange data via GPRS and the system will shut down in case of unavailability of Internet connection. There is a strong need for developing another backup communication media. In this paper a data transaction method based on encoded Short Message Service (SMS) over Global System for Mobile Communication (GSM) is proposed. This new method guarantees the functionality of the system in case of inaccessibility to GPRS which may be not always available due to measures such as attacks that affect its availability. The proposed method is based on third party agent who can keep the address secrecy of both communicators besides keeping confidentiality, integrity and availability.

Index Terms—GSM, SMS, GPRS, Message Security, Service Availability, Third Party Scheme.

I. Introduction

The emerging technologies make the mobile devices perform functions beyond just calling and sending messages. They are used by systems with a dedicated application to communicate with each other and sending specific data. Systems such as patient monitoring systems [1-3] and tracking systems [4-7] depend on GPRS in their connectivity between members of the system. GPRS is more exposed to intruders and possible attacks, since it uses the IP technology and connects to the public network Internet [8] which causes unavailability of GPRS service. Additionally, the GPRS service may be not available in some portions of time and after outage it needs addition recovery time which is the period of time that it needs to return to its normal behavior. According to Porcarelli et al [9] statistics, in a GSM with approximately 150 GPRS user, if the time of outage reaches about 300 seconds, another 140 seconds are needed to recover the delayed GPRS requests and return to normal service. This means that the possible member of a system may stay about 440 seconds without connection. On the other hand, there is a possibility that such systems have been established on limited resources infrastructure regions that the GPRS may not be always available. In such systems it is highly important that the communication services should be always functional such that the system members have full access at any time.

Obviously, in the "era of mobility", SMS token is very convenient since it is available for almost anyone without any additional devices, cards, etc. It also realizes the idea of two-factor authentication; i.e., "something what I know" and "something what I have" [10]. In fields such as the Information and Communication Technologies for Development (ICTD), SMS-based solutions have proven robust, flexible, and valuable to multiple communities. Anderson et al [11] have established systems based on SMS over GSM that more likely available than GPRS. These systems lack of security in mind and they mainly depend on the security provided by commercial applications or GSM system itself. The transmission of SMS over GSM has high level of security [12], but this security issues is host to host security (i.e. related to transmit of SMS from the sender subscriber to receiver, moving through GSM system and not really care about process to process security).

There are two major security vulnerabilities affecting SMS based communication: the lack of confidentiality during the transmission of a message and the absence of a standard way to certify the identity of the user (or at least his phone number) that sent the message. These vulnerabilities originate from the protocol used to exchange SMS messages and from the infrastructures used to implement it [13]. In this paper a secure model for communication based on SMS over GSM is produced. The system establishes a proposed security scheme which is the main security level of the system and worked above the GMS security level. The security scheme aims to provide both message confidentiality and sender authentication. SMS beside to voice are considered as primary services of the GSM. The system availability is achieved by replication of multiple communication channels. The system includes a third party server (two GSM servers, one primary and a secondary; i.e., backup) and a number of clients. In the following related works and the proposed scheme is explained in details.

II. Related Works

There are several published researches that aim to improve the SMS communication security over GSM. These researches propose methods on two main fields. The first field of researches aimed to improve SMS transmission security by changing the physical underlying GSM architecture and transport specification protocol. As instance, Hossain et al [14] provided communication secrecy by changing GSM protocol at transport level. The main disadvantage of this field is the need to not only perform the proposed security method, but change in the GSM architecture.

The second field of researches contributes by proposing application level security method. To apply such research trend there is no need to change any underlying physical GSM architecture. Another advantage is that, by developing the mobile phones and strong computing capabilities the execution of such methods is practical on mobile devices as the hardware available in the mobile devices are able to perform such algorithms. Igor et al [15] developed the security software, called "Green Head". It protects personal smart phones from receiving malicious, fake and useless information. This research deal with sender authentication, but the message confidentiality leaves unsecure. Jain [16] proposed a secure SMS transaction model that can be used in financial transaction security. This model is based on asymmetric cryptography to provide message secrecy and sender authentication. The ability to send direct messages between clients also make the whole system valuable in case of security breach on one of the clients. Croft and Oliver [17] proposed an approach to secure an SMS message using one-time pads using shared information between the communicating peers and the serving GSM network. Santis et al [13] presented a software framework which allows two peers using public key cryptography to exchange encrypted and digitally signed SMS messages. Also, they implemented a novel and simple security protocol to key exchange which minimizes the number of SMS messages to use. Although these researches do not need to change in underlying GSM architecture, but it has some concerns such as lack of message fragmentation which may leads to message corruption and possibility of duplication message processing.

III. Global System for Mobile Communications

The idea of cell-based mobile radio systems appeared at Bell Laboratories (in USA) in the early 1970s. However, mobile cellular systems were not introduced for commercial use until the 1980s [18]. Today GSM is used by over 1.5 billion people across more than 212 countries and territories [19].

The architecture of a GSM system can be divided into the mobile station (MS), the base station subsystem (BSS), and the network and switching subsystem (NSS) [20]. The MS is carried by the user, the BSS controls the radio link to the MS and the NSS performs the switching of calls between the MS and other fixed or mobile network users. It also handles mobility management.

According to Ghribi and Logrippo [21] explanation; the home location register (HLR) is a database used to store and manage permanent data of subscribers such as service profiles, location information, and activity status. Mobile service switching center (MSC) is responsible for telephony switching functions of the network. Also, it performs authentication to verify the user's identity and to ensure the confidentiality of the calls. The authentication center (AuC) provides the necessary parameters to the MSC to perform the authentication procedure. AuC plays as a separate logical entity but is generally integrated with the HLR. The equipment identity register (EIR) is on the other hand a database that contains information about the identity of the mobile equipment. It prevents calls from unauthorized or stolen MSs. The visitor location register (VLR) is a database used to store temporary information about the subscribers and is needed by the MSC in order to service visiting subscribers. Gateway mobile switching center (GMSC) is an MSC that serves as a gateway node to external networks, such as ISDN or wireline networks. The base transceiver station (BTS) handles the radio interface to the MS. It consists of radio equipment (transceivers and antennas) required to service each cell in the network. The base station controller (BSC) provides the control functions and physical links between the MSC and the BTS. A number of BSCs are served by one MSC while several BTSs can be controlled by one BSC.

IV. Short Message Service

SMS is a fairly basic service that enables GSM subscribers to send simple text messages of up to 160 characters to one another. SMS is a store-and-forward service, which means that messages are not sent directly between users but rather via MSC and short message service center (SMSC). This enables instant delivery, nominal tariffing, simultaneous SMS and voice capability, international roaming without international fees, and message delivery that is not hindered by network traffic [22].

The maximum message length in SMS was estimated in the beginning as 128 bytes, allowing the transmission of about 146 characters using 7 bits per character. This size could be enhanced to 140 bytes carrying 160 characters. In the mid-1990s it became possible to create longer messages and transport them by concatenated short messages. A mechanism for short message concatenation had been defined; which provided a technical solution for applications that needs to send messages and uses where messages could not be easily conveyed within 140 octets (= 160 characters coded by 7 bits per character). However, the cost of sending multiple segments of a concatenated message is much the same as the cost of sending multiple SMS messages [23].

The total time, including the setup and release phase, of sending a SMS message of 160 characters is roughly

4.6 seconds. While sending an empty message takes around 4.15 seconds. [20]. Analysis by Vodafone of their short message service gave the following results, which were, at the late 1990s, consistent with the results of other network operators [23].

The time interval separating the instance of sending a message from a mobile phone to the instance of receiving that message at the recipient's mobile is typically 6-8 seconds. Approximately (1 to 2) seconds of this was attributed to message storage in the SMSC. The time interval separating the instance of sending a message from a mobile to the instance of receiving a delivery confirmation is typically (10 to 12) seconds. Due to the receiving mobile being out of coverage, in poor coverage or turned off, 38% of messages were not delivered on the first attempt to mobile phones. 98% of all messages were delivered on the first attempt where the destination was a fixed-network termination. Typically, 98% of messages were eventually delivered, provided that the retention time for the short message was set to 3 days.

Although it has not been possible to obtain the latest statistics, it is unlikely that the above performance will have changed significantly although there may well have been an improvement in the 38% figure for the first delivery attempt of mobile-terminated messages owing to improved mobile radio coverage

V. Proposed Communication Scheme

The proposed secure communication scheme is illustrated in Fig. 1. It is designed with number of security considerations in mind. Multi-parameter encryption is used to ensure secrecy of transmitted data that will pass through public channels in which the encryption process depends on various parameters; such as a sequence number (SEQ), a dedicated key, unique number of Subscriber Identity Module (SIM) and International Mobile Station Equipment Identity (IMEI) of the device. The introduced scheme guarantees the security of the overall system even in case of security breaches in one of the system members.

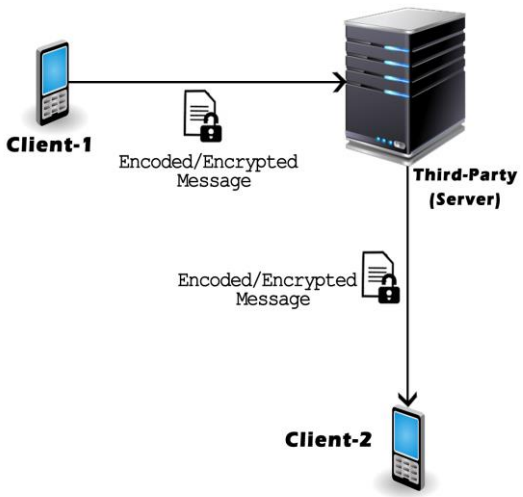


Fig.1. The Proposed Secure Communication Scheme

Data framing and coding method are introduced to reduce the size of messages packets during transmission and lets the transmitted data occupy as minimum as possible bits, also, it prevents the loss of whole data, in case of destruction of part of the sent packet. Each client can communicate with other members of the system through the third party server. At preprocessing step before transmission of data, the transmitted messages are framed to ensure removal of redundancy that may exist between the transmitted messages. The second step before sending the data is to encode the packet to reduce the number of bits according to the used symbols in the system. Note that, if the symbols are more than 57 symbols, the resulted message's size from encoding step will remain same as original message's size. The next step before sending the data is to add a sequence number (SEQ) and then encrypt the message. The SEQ is used to synchronize between client and server. The proposed secure communication diagram is illustrated in Fig. 2.

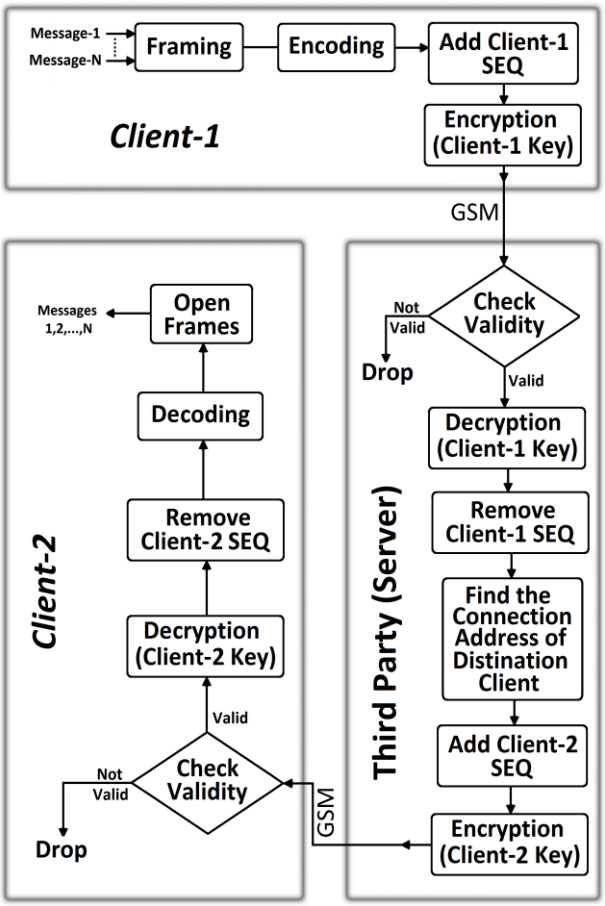


Fig.2. The Proposed Secure Communication Diagram

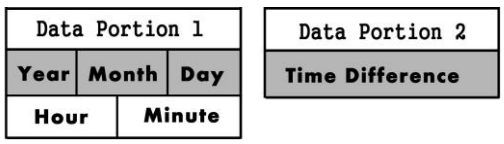
At the server side, the first step is to authenticate the incoming message. It is done by checking the SIM number of message's sender and then encrypting the message. If it is registered in the system, then the server starts decrypting the message using P2P key and the registered IMEI number of the sender's device. If the sender is valid, the message is passed on the next step; otherwise, the message is stored in a temporary table and then it will be dropped. After checking the validity of the

incoming message; the SEQ field indicates whether the received message is not processed before (i.e. there is no such message with same SEQ had been received from the sender client earlier) or it was checked before. This can be done by comparing the SEQ field of the incoming message with the SEQ field attached to the data of sender's client inside the server database); then the server removes the SEQ field of the message which belongs to the sender, adds appropriate SEQ of the receiver client, and then encrypts the message using P2P key and IMEI of the receiver's client.

Firstly, the receiving client, checks the validity of the incoming message to ensure that it has been sent from the server. Secondly, it starts decrypting the message and removing the SEQ. If the message passes validating and decrypting steps and the SEQ indicates the correct value, then the message is decoded and the possible padded bits will be removed. The last step will open the frames to regenerate the original message.

A. Data Representation

If a portion of data during transmission via GSM is lost and it was in sequence mode then losing each part of symbols in the message will corrupt the whole message. A framing pattern method is proposed for numbering the frames (reference, relative frames) of each message. The first frame in the pattern is the reference frame. The remainders are the relative frames and their values depend on their positions relative to reference frame. The relative frames contain less information, because they include the time difference between their value and the main value. Key factors for selecting the refreshing rate of reference frame is the data lose risk (which depends on trust level of mobile device) and available buffer size. If the reference frame is damaged during the transmission, then this pattern will be deleted which leads to the consequence "the relevant reference frame and the relative frames that depend on that frame will be dropped". The system can retrieve the data starting from the next reference frame. If one of the relative frames is damaged, it does not significantly affect all other data; except the dropped frame itself. The reference and relative frames data contents are shown in Fig. 3.



(a) Reference Frame (b) Relative Frame

Fig.3. Frame Format

B. Data Transaction Method

After representing the data in patterns, the data has to be encoded, if it is needed, before transaction. This step is done to ensure that the transmitted message will take as less size as possible.

Since the default GSM message uses standard ASCII symbols, then each symbol is coded using 7 bits. If the members of a system transmit messages that consists of a set of specific characters (as instance a system that only transmit numeric data) then using 7 bits for each symbol is considered as holding a sort of transmission waste. At initial phase of system setup, the expected number of exchanged symbols between system members has to be assessed. If the transmitted messages between members in a system contain (N) possible symbols and (N) is less than 57, then a coding step has to be applied.

Let say the number of possible symbols (N) that used in the message are between m and n-1, where n and m are multiply of 2; then the coding step uses (R) bits, instead of 7 bits to represent each symbol, where R is the lowest integer value satisfy the condition in (1):

$$n - m < 2R \tag{1}$$

The encoding step includes generating the message with R-bits/symbol; then, the generated message will be converted to sequence of bits. Finally, the binary sequence will be converted to ASCII symbols. Both sides of SMS exchange should have the necessary mapping table; which holds the codewords of all exchanged symbols (i.e., each symbol is stored along with the corresponding code word value). Since the generated string will be converted to ASCII format before sending via GSM, it has to be aware about one important issue; "the NULL symbol in ASCII table has a value 0 and it is represented as "0000000", but most of GSM mobile devices assume the NULL symbol as the end of a SMS. So, reaching to a NULL value, even if it occurs at the middle of a sentence, will cause cut in the received packet at this point, and the remaining characters will be ignored; and consequently this originates a problem at the receiving device, see Fig. 4 as an illustration.

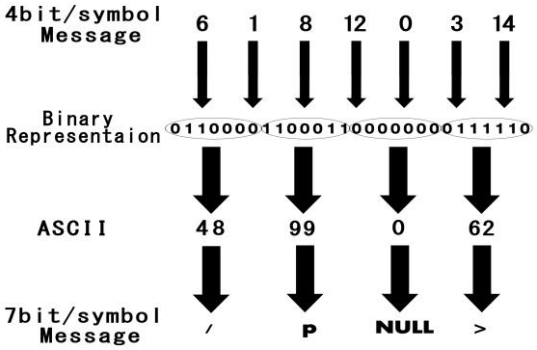


Fig.4. An example illustrates the production of "NULL" Symbol in the middle of received message

Therefore, generating NULL symbol in the middle of the packet has to be avoided, and this could simply avoided by never using the values that after combining them together may generate successive seven 0's. For instance, if each symbol is represented using four bits, then the code word "0000" should not be used to represent any symbol and the coding should start with using the code word value 0001 to encode the first symbol value; this will avoid generating NULL value. Table (1) shows the code words values that have not to be assigned.

Table 1. Avoided Code Words in Encoding

Bit/Symbol	# Available Symbols	Avoided Code Word	
2	2	00	Possible generating NULL
		11	Reserved
3	6	000	Possible generating NULL
		111	Reserved
4	14	0000	Possible generating NULL
		1111	Reserved
5	28	00000	Possible generating NULL
		00001	Possible generating NULL
		10000	Possible generating NULL
		11111	Reserved
6	56	000000	Possible generating NULL
		000001	Possible generating NULL
		000010	Possible generating NULL
		000011	Possible generating NULL
		010000	Possible generating NULL
		100000	Possible generating NULL
		110000	Possible generating NULL
		111111	Reserved

After the preparation of R-bits/symbol message and convert it to sequence of binary digits; it has to be converted to ASCII characters (i.e. convert each group of seven bits to an ASCII based character). As, shown in Table 1 the code word value (111111) is reserved to be used for padding purpose. It is possible that the resulted binary sequence cannot be divided into groups of seven bits, for that reason, the binary sequence will be padded by 1's if needed. The padding process should satisfy the following two requirements:

1. The padded 1's should be more than or equal to R

$$\beta = \alpha \underbrace{11...1}_{m} \quad , \quad m \geq R \tag{2}$$

in which α is the original binary sequence and β is the new binary sequence after padding.

2. The resulted binary sequence should be divided by 7

$$\beta \bmod 7 = 0 \tag{3}$$

Then, the encoder will convert the binary sequence into 7-bits/symbol message.

Each message is encoded before sending it. As mentioned, because the symbols of the message are between 'm' and n-1, using more than R bits per symbol is west of transmission data space. Each symbol in the message is coded by using R bits depending on a lookup table and, then, the generated binary sequence is converted to ASCII (7-bits per symbol). At decoding phase, first of all the message which has been received in ASCII, is converted to a sequence of binary digits. If the received message from client-1 can be divided by R (which is the base number and is determined at the system establishment depending on the number of possible symbols in the transmitted message between system members), this means that no padding is performed to the original message. If not, then this indicates that padding is applied on the original message and the padded digits have to be removed. It can be done by checking the binary sequence, taking R bits each time and convert it to the corresponding symbol by depending on the mapping table. This process is continued until the taken R bits contains 1's only (which indicates the padding has been started from this point), at that time the taken R bits and remainder bits are ignored. Algorithm (1) illustrates the steps of removal padding process.

Algorithm (1) Removal of Padding

```
Goal: remove padding in case of existence
Input:  ReceivedBinSeq
        BinLen// the length of inputted binary
              sequence
Output: BinSeq// binary sequence without padding

Steps:
1   if BinLen mod R in not equal to zero then
2     Set i to 0
3     While i is less than BinLen
4       set t to ReceivedBinSeq.substring
        (start from i, take R characters)
5       if t is equal to 'R times 1' then
6         Set BinSeq to ReceivedBinSeq.substring
          (start from 0, take i characters)
7         Set i to BinLen
8       end if
9       Increment i by R
10    end while
11 else
12    Set BinSeq to ReceivedBinSeq
13 end if
```

C. Proposed Model Security

Many security issues should be available to make the system secure. The message encryptions using multi-parameters key, authentication type and the third party based scheme are three features of the system related to its security.

All data frames that are exchanged between members are encrypted by using Advance Encryption Standard (AES). Each member has a dedicated P2P key with the server. This encryption provides both message confidentiality and authentication. The block ciphering standard AES-128 is used in the proposed system for encryption. There is individual 128-bit key between the main server and each member. In the proposed system the secure hash algorithm is used. The process of key generation and message encryption consists of two steps. First, using SHA-1 digest generation algorithm to generate a 128-bit digest of the IMEI of the device and P2P key between the main server and the patient, which will be the AES key that is used in the encryption; and second, performs the encryption for the exchanged message.

At each SMS exchange instance, the server and receiver check the validity of the transmitted message. Each GSM user has a SIM with a unique number that allows him to use the subscribed services. In SMS over GSM connection the phone number of sender is checked. If the sender number of the transacted packet is a member of the system then the message is accepted, otherwise it is temporarily archived in a garbage table and then dropped. These features are used as the first layer of authentication as long as no two users have the same GSM number. The first security layer (i.e. authentication via SIM number) alone is not enough; so the system uses AES encryption as a second layer of security with the IMEI of the device and P2P key between each member and the main server. Also, each member of the system has an 8-bits sequence number (SEQ); it is registered inside the identity table in database. The sequence number ensures that the same message does not processed twice, and the message with different sequence number than the number in the database is dropped. The incoming packet will be decrypted using P2P AES key, and then concatenated sequence number as a first byte will be checked. If the SEQ is as the same as expected (i.e. the same number that is stored in the database beside the sender name) then the message will be considered valid and passed to the next step; if not, then the message will be dropped.

All members of the system can communicate with each other exclusively via third party (i.e. main server). There is no direct message transfer between members. This allows high level of security; if the privacy of one of the devices in the system is breached, its link with the server is only affected; other members, who have different IMEI and P2P AES keys and no direct link with the breached device, will be completely in safe.

VI. Proposed Model Test

A test is performed to check the SMS transmission time between system members. The messages are transmitted in various time of day. The sending time is the period of time between sending a message from client-1 till reaching that message to the server. For more than 135 tested messages, it is found that the elapsed sending time is variable; and takes between 5 to 8 seconds. Only two exceptions have occurred, they are received by the server from the second attempt because the primary GSM modem was turned off at the transmission time. Fig. 5 illustrates the GSM based message sending time of 135 tested messages.

The receiving time is the period of time between sending a message from client-1 till reaching that message to the client-2 through the server. The client-2 has received the transmitted message sent from client-1 after (11-16) seconds from the time of sending the message.

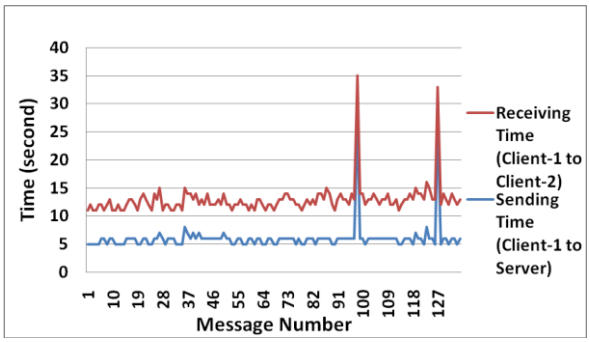


Fig.5. Secure Message Transmission Time

The proposed method execution has been tested on a mobile device with slow and single core Broadcom 832 MHz processor and 512 MB memory to ensure the performance of the resource usage. Fig. 6 shows the memory usage of the proposed model execution.

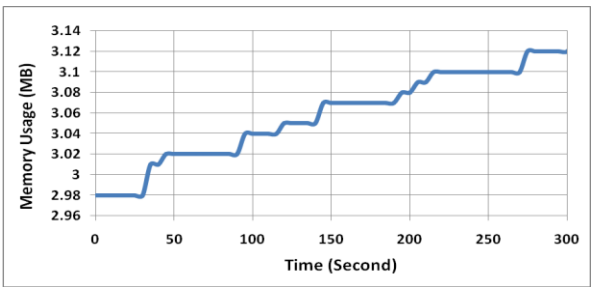


Fig.6. Memory Consumption of Proposed Model

Table 2. Monthly Proposed Model Operating Cost

Service Type (Frame/Day)	Service Cost (IQD)		
	Client	Server	Total
1	360	750	1,110
2	720	1,500	2,220
3	1,080	2,250	3,330
4	1,700	3,000	4,700
8	4,200	6,000	10,200
12	7,200	9,000	16,200
24	16,200	18,000	34,200

A test on operating cost of the proposed method has been performed. During testing, Asiacell mobile telecommunication service provider has been used which is cheaper in prices than other local mobile telecommunication providers. Table 2 shows the communication costs of the proposed model.

VII. Conclusions

Some remarks related to the behavior and performance of the proposed model were stimulated. Among these remarks are the followings:

Applying this model is important for the systems that critically depend on service availability. This model takes fair time (for Iraqi local GSM mobile infrastructure: it is as maximum about 16 seconds) to transmit a packet between two clients on a system. This time may be reduced (down to 11 seconds); this depends on the instantaneous available GSM quality service at the transmission time. This time includes sending the message to a trusted third party and, then, passing it to the receiver client. The times taken by proposed framing and coding methods depend on message size.

Padding is used as necessary step to enable encoded message to be converted to ASCII without affecting the original message.

The packet may consists of a set of similar characters. For instance in case of sending coordinates data there will be a number of similar values. The encoding method produces a set of 0's and 1's depending on mapping table. This binary sequence can be compressed further using Huffman, LZW or any efficient and fast entropy coding methods.

Symmetric encryption scheme is used, in which keys are distributed in a way that each client has a dedicated P2P key with the trusted third party. This method guarantees the confidentiality of the transmitted packet. Sender authentication is based on the IMEI of the device and SIM number of the sender. For an addition level of sender authentication asymmetric encryptions such as RSA can be used to authenticate the sender using private and public keys.

References

[1] M. Kamel and L. George, "Remote Patient Tracking and Monitoring System", International Journal of Computer Science and Mobile Computing, 2013. 2(12): 88-94.

[2] A. Bourouis, M. Feham and A. Bouchachia, "Ubiquitous Mobile Health Monitoring System for Elderly", International Journal of Computer Science & Information Technology, 2011. 3(3): 74-82.

[3] R. Paradiso, "Wearable Health Care System for Vital Signs Monitoring", International IEEE EMBS Special Topic Conference on Information Technology Applications in Biomedicine, Prato, Italy, 24-26 April 2003. pp. 283-286.

[4] M. Kamel, "Real-Time GPS/GPRS Based Vehicle Tracking System", International Journal Of Engineering And Computer Science, 2015. 4(8): pp. 648-652.

[5] K. Salim and I. Idrees, "Design and Implementation of Web-Based GPS-GPRS Vehicle Tracking System", International Journal of Computer Science Engineering and Technology, 2013. 3(12): 439-442.

[6] R. Gupta and B. Reddy, "GPS and GPRS Based Cost Effective Human Tracking System Using Mobile Phones", Viewpoint, 2011. 2(1): 39-45.

[7] N. Chadil, A. Russameesawang and P. Keeratiwintakorn, "Real-Time Tracking Management System Using GPS, GPRS and Google Earth", Electrical Engineering/ Electronics, Computer, Telecommunications and Information Technology, ECTI-CON 2008, 5th International Conference, 2008. pp. 393-396.

[8] C. Xenakis, D. Apostolopoulou, A. Panou and I. Stavrakakis, "A qualitative risk analysis for the GPRS technology", IEEE/IFIP 2008 International Conference Embedded and Ubiquitous Computing, EUC'08, 2008. pp. 61-68.

[9] S. Porcarelli, F. Di Giandomenico, A. Bondavalli, M. Barbera and I. Mura, "Service-Level Availability Estimation of GPRS Mobile Computing", IEEE Transactions, 2003. 2(3): 233-247.

[10] L. Siwik and L. Mozgowoj, "Server-Side Encrypting and Digital Signature Platform with Biometric Authorization", I. J. Computer Network and Information Security, 2015. 4: pp.1-13.

[11] R. Anderson, A. Poon, C. Lustig, W. Brunette, G. Borriello and B. Kolko, "Building a Transportation Information System Using only GPS and Basic SMS Infrastructure", Information and Communication Technologies and Development, 2009. pp. 233-242.

[12] M. Mouly and M. Pautet, "The GSM System for Mobile Communications", Telecom Publishing, France, 1992.

[13] A. Santis, A. Castiglione and U. Petrillo, "An Extensible Framework for Efficient Secure SMS", International Conference on Complex, Intelligent and Software Intensive Systems, Poland, 2010. pp. 843-850.

[14] A. Hossain, S. Jahan, M. Hussain, M. Amin and S. Shahnewaz, "A proposal for enhancing the security system of short message service in GSM", Anti-counterfeiting, Security and Identification, 2008. pp. 235-240.

[15] Z. Igor, M. Dmitry, S. Andrey, K. Dmitry, T. Anastasia and Z. Alexander, "Security Software Green Head for Mobile Devices Providing Comprehensive Protection from Malware and Illegal Activities of Cyber Criminals", International Journal of Computer Network and Information Security, 2013. (5): pp. 1-8.

[16] M. Jain and A. Jain, "Financial Transaction Security Using Mobile SMS", International Journal of u- and e-Service, Science and Technology, 2015. (8): pp. 365-374.

[17] N. Croft and M. Olivier, "Using an approximated one-time pad to secure short messaging service (SMS)", Proceedings of the southern African telecommunication networks and applications conference , 2005. pp. 71-76.

[18] J. Sempere, "An Overview of the GSM System", IEEE Vehicular Technology Society, 1997. pp.1-33.

[19] B. Omijeh and G. Ighalo, "Modeling of GSM-Based Energy Recharge Scheme for Prepaid Meter", IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE), 2013. 4(1): pp. 46-53.

[20] Ch. Baath and J. Kuhn, "SMS over GPRS", Course report, Department of Microelectronics and Information Technology (IMIT), Royal Institute of Technology (KTH), Sweden, 2003.

[21] B. Ghribi and L. Logrippo, "Understanding GPRS: The GSM Packet Radio Service", Computer Networks, 2000. 34: pp. 763-779.

[22] L. Novak and M. Svensson, "MMS- Building on the

success of SMS", Ericsson Rev, 2001. 78(3): pp. 102-109.
[23] F. Hillebrand, F. Trosby, K. Holley and I. Harris, "Short Message Service (SMS), the Creation of Personal Global Text Messaging", John Wiley and Sons Publication, 2010.

Authors' Profiles

Mohammed Baqer M. Kamel, Assist. Lecturer at University of Kufa. He received the M.Sc. degree from University of Baghdad / Iraq. He also received IT Administration in Ziik from Technical University of Berlin / Germany. Interested Research Fields: Mobile Computing, Network security, GIS and GPS applications.

Loay E. George, Ph.D. and assistant professor at University of Baghdad, his interest research fields are: Digital video, image and audio compression techniques (transform coding, fractals, wavelet…). Information hiding (in image or audio media), biometrics for computer security applications (fingerprint, hand geometry), image recognition (including textural analysis, image classification and segmentation) for remote sensing and biomedical applications. Development of image retrieval systems, and GIS and GPS applications.

How to cite this paper: Mohammed Baqer M. Kamel, Loay E. George,"Secure Model for SMS Exchange over GSM", International Journal of Computer Network and Information Security(IJCNIS), Vol.8, No.1, pp.1-8, 2016.DOI: 10.5815/ijcnis.2016.01.01

