Enhancing Security System of Short Message Service for M-Commerce in GSM

Neetesh Saxena
Student M. Tech, GGSIPU Delhi

Ashish Payal
Asstt. Prof, USIT, GGSIPU Delhi

Abstract- **Global System for Mobile (GSM) is a second generation cellular standard developed to cater voice services and data delivery using digital modulation. Short Message Service (SMS) is the text communication service component of mobile communication systems, using standardized communications protocols that allow the exchange of short text messages between mobile phone devices. SMS will play a very vital role in the future business areas whose are popularly known as m- Commerce, mobile banking etc. For this future commerce, SMS could make a mobile device in a business tool as it has the availability and the effectiveness. The existing SMS is not free from the eavesdropping, but security is the main concern for any business company such as banks who will provide these mobile banking. Presently there is no such scheme which can give the complete SMS security. Now, a new security scheme for improving the SMS security is proposed here. At first plaintext of SMS would be made as cipher text with the help of existing GSM encryption technology, then this cipher text would be digitally signed with the help of public key signature. These will be made compatible to existing infrastructure of GSM security. The proposed scheme will give total authenticity, data integrity, confidentiality, authorization and non-repudiation which are the most essential issues in m-commerce or mobile banking and in secure messaging.**

Keywords- SMS, mobile banking, ciphering, digital signature, public key algorithm, public key signature, data integrity, authenticity.

I. INTRODUCTION

Short Message Service (SMS) has become an extension of our lives and plays an important role in daily life. SMS is a popular medium for delivering Value Added Services and are suitable for mobile banking, payment reminders, stock and news alerts, railway and flight enquiries etc [6]. These types of messages are normally computer generated messages sent over Short Message Peer to Peer (SMPP) protocol. Sending an SMS is cheap, fast and simple. It is a store-and-forward, easy to use, popular, and low cost service. SMS is the text communication service component of mobile communication systems, using standardized communications protocols that allow the exchange of short text messages between mobile phone devices. SMS will play a very vital role in the future business areas whose are popularly known as M-Commerce, mobile banking etc. For this future commerce, SMS could make a mobile device in a business tool as it has the availability and the effectiveness. The existing SMS is not free from the eavesdropping, but security is the main concern for any business company such as banks who will provide these mobile banking. Presently there is no such scheme which can give the complete SMS security [14].

A. GSM: Global System for Mobile Communication

GSM (Global System for Mobile Communications) is the most popular standard for mobile telephony systems in the world [3]. In 1982, the European Conference of Postal and Telecommunications Administrations (CEPT) created the Group Special Mobile (GSM) to develop a standard for a mobile telephone system that could be used across Europe. The GSM Association estimates that 80% of the global mobile market uses the standard. GSM is used across more than 212 countries and territories. GSM pioneered low-cost implementation of the short message service (SMS), also called text messaging, which has since been supported on other mobile phone standards as well.

In the GSM, only the airway traffic between the Mobile Station (MS) and the Base Transceiver Station (BTS) is optionally encrypted with a weak and broken stream cipher (A5/1 or A5/2). The authentication is unilateral and also vulnerable [4]. The development of UMTS introduces an optional Universal Subscriber Identity Module (USIM), that uses a longer authentication key to give greater security, as well as mutually authenticating the network and the user - whereas GSM only authenticates the user to the network (and not vice versa). The security model therefore offers confidentiality and authentication, but limited authorization capabilities, and no non-repudiation. The BTS act as a transmitter and receiver of the radio signals from mobile phones. The BTS translates the radio signals into digital format and then it transfers the digital signals to the Base Station Controller

(BSC). The BSC controls multiple BTSs within a small geographical area. The BSC forwards the received signals to Mobile Switching Centre (MSC) and the MSC interrogates its databases (Home and Visitor Location Register (HLR and VLR)) for the location information about the destination mobile handset [6]. If the signal originates or terminates at the fixed telephone line network then the signal will be routed from the MSC to the Gateway MSC (GMSC). If the received signal is an SMS message then the message would be stored in the Short Message Service Centre (SMSC) and the message will wait to be delivered. Even after the SMS is delivered, the message content still maintains in the SMSC persistence database. If the signal needs to be redirected internationally then the signal will be routed via the International Switching Centre (ISC) to another country. The maintenance is controlled by the Operation and Management Centre (OMC). The Equipment Identity Register and Authentication Register (EIR and AUC in respective order) databases are used for equipment verifications and user authentication [14].

B. Architecture of SMS in GSM Network [14]

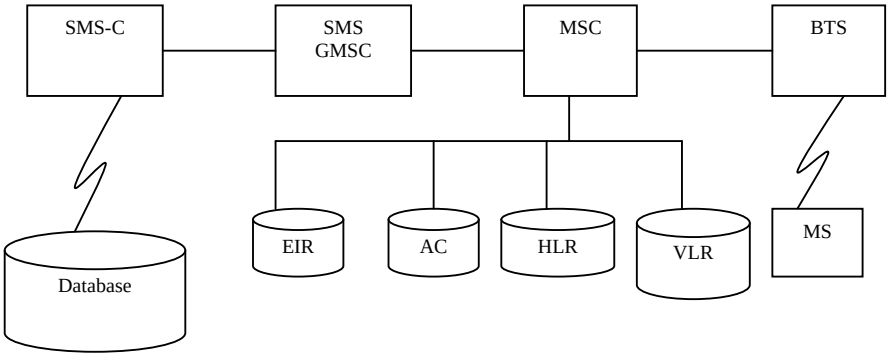

Figure 1: Existing SMS architecture in GSM

SMS-C: SMS Center

SMS GMSC: SMS Gateway Mobile Switching Center

MSC: Mobile Switching Center

BTS: Base Transceiver Station

VLR: Visitor Location Register

HLR: Home Location Register

AC: Authentication Center

EIR: Equipment Identity Register

C. SMS: Short Message Service

SMS stands for Short Message Service. It is a technology that enables the sending and receiving of messages between mobile phones. SMS first appeared in Europe in 1992. Later it was ported to wireless technologies like CDMA and TDMA. The GSM and SMS standards were originally developed by ETSI. ETSI is the abbreviation for European Telecommunications Standards Institute. Now the 3GPP (Third Generation Partnership Project) is responsible for the development and maintenance of the GSM and SMS standards [4].

The rapid development in mobile communication has transformed SMS as widespread tool for business and social messaging [9]. SMS services are growing day by day. With SMS, people can easily share personal and official messages in a cost effective manner. SMS enables the transmission of up to 1120 bits alphanumeric messages between mobile phones and external systems. It uses SMS center (SMS-C) for its routing operation in a network and can be transmitted into another network through the SMS gateway [10]. SMS usage is threatened with security concerns [5], such as eavesdropping, interception and modification. SMS messages are transmitted as plaintext between the mobile stations and the SMS center using the wireless network. SMS content are stored in the systems of the network operators and can easily be read by their personnel. The A5 algorithm [8], which is the GSM standard for encrypting transmitted data, can easily be compromised. Therefore, there is a need to provide an additional encryption on the transmitted messages. As suggested by the name Short Message Service, the data that can be held by an SMS message is very limited. One SMS message can contain at most 140 bytes (1120 bits) of data, so one SMS message can contain up to [2]:

1) 160 characters if 7-bit character encoding is used. (7-bit character encoding is suitable for encoding Latin characters like English alphabets.)

2) 70 characters if 16-bit Unicode UCS2 (2-byte Universal Character Set) character encoding is used. (SMS text messages containing non-Latin characters like Chinese characters should use 16-bit character encoding.) SMS text messaging supports languages internationally. It works fine with all languages supported by Unicode, including Arabic, Chinese, Japanese and Korean.

D. SMS Security in M-Commerce

The Global Service for Mobile communications with the greatest worldwide number of users. The SMS messaging has some extra security vulnerabilities due to its store-and forward feature, and the problem of fake SMS that can be conducted via the Internet [10]. When a user is roaming, the SMS content passes through different networks and perhaps the Internet that exposes it to various vulnerabilities and attacks. Another concern is arisen when an adversary gets access to the phone and reads the previous unprotected messages. To exploit the popularity of SMS as a serious business bearer protocol, it is necessary to enhance its functionalities to offer the secured transaction capability. SMS is a part of GSM networks that allows the alphanumeric message up to 160 characters to be sent and received via the network operator's SMS center to the mobile subscribers [12]. If the subscriber is not reachable, then SMS are stored in the GSM operator's SMS center and delivered when it is reachable. The existing SMS is the transmission of just plaintext. It can be easily read by the intruder or even the persons of the operator. Therefore, it is not secured enough for M-commerce or mobile banking [14]. SMS plays a very vital role in the mobile banking or M-Commercial purpose because of its simplicity and cheapness. Upcoming payment systems are based on the mobile device by using SMS. But there is some security issues related to services of SMS for such M-Commerce or mobile banking. The service includes [14]:

1) Confidentiality: only the valid communicating parties can view the SMS.

2) Integrity: the SMS can not be tampered by the intruders. The system should be able to find out such alteration.

3) Non-repudiation: no party can deny the receiving or transmitting the data communicating between them.

4) Authentication: each party has the ability to authenticate the other party.

E. SMS Security Threats

Understanding the basics of SMS security opens the door to preventing some common security threats in SMS usage [8][11]:

1) Man-in-middle Attack: This is the network that authenticates users. The user does not authenticate network so the attacker can use a false BTS with the same mobile network code as the subscriber's legitimate network to impersonate himself and perform a man-in-the-middle attack.

2) Replay Attack: The attacker can misuse the previously exchanged messages between the subscriber and network in order to perform the replay attacks.

3) Message Disclosure: Since encryption is not applied to short message transmission by default, messages could be intercepted and snooped during transmission. In addition, SMS messages are stored as plain text by the SMSC before they are successfully delivered to the intended recipient. These messages could be viewed by users in the SMSC who have access to the messaging system.

4) Spamming: While using SMS as a legitimate marketing channel, many people have had the inconvenience of receiving SMS spam. The availability of bulk SMS broadcasting utilities makes it easy for virtually everyone to send out mass SMS messages.

5) Denial of Service (DoS) Attacks: DoS attacks are made possible by sending repeated messages to a target mobile phone, making the victim's mobile phone inaccessible.

6) SMS Phone Crashes: Some vulnerable mobile phones may crash if they receive a particular type of malformed short message. Once a malformed message is received, the infected phone becomes inoperable.

7) SMS Viruses: There have been no reports of viruses being attached to short messages, but as mobile phones are getting more powerful and programmable; the potential of viruses being spread through SMS is becoming greater.

8) SMS Phishing: SMS phishing is a combination of SMS and phishing. Similar to an Internet phishing attack using email, attackers are attempting to fool mobile phone users with bogus text messages. When users are taken in by a bogus text message, they may connect to a website provided in the SMS message, and be tricked into download a malware application into their mobile phones.

II. PROBLEM DEFINITON

The message generated from External Short Messaging Entity (ESME) or a mobile phone is in plain text which can be easily read and modified before it reaches SMSC. Any wrong information received by the recipient can prove fatal for the user. To exploit the popularity of SMS in M-commerce and mobile banking, it is necessary to provide the proper security to SMS so that it could reach to the receiver's mobile safely to provide data confidentiality, integrity, authentication, and non-repudiation. However, such requirements are not provided by the traditional SMS messaging. It is very necessary to secure the SMS by encryption techniques and prevent it from the various attacks applied on SMS like man-in-middle attack, replay attack, non-repudiation etc so that it could provide the data security like confidentiality, authentication, integrity and non-repudiation.

III. LITERATURE SURVEY

In the literature, many authors have used different encryption techniques to provide confidentiality to SMS transmitted messages. Some of these works are presented in this section.

In a study by Mary Agoyi and Devrim Seral [1] large key size algorithms are not suitable for SMS encryption due to small memory and low computational power of mobile phones. Elliptic curve's ability of providing high security with smaller key size makes it very useful in resource-limited device such as mobile phone. This has put Elliptic curve at an advantage over the RSA and ELGamal in SMS encryption. In the paper of Alfredo De Santis, Aniello Castiglione and Umberto Ferraro Petrillo [2] the results seem to show that RSA and DSA cryptosystems perform generally better than ECDSA, except when using very large keys. Nassim Khozooyi, Maryam Tahajod and Peyman khozooyi [3] are discussed the security of mobile network protocol along with information security for governmental transactions. A new public key-based solution for secure SMS messaging (SSMS) is introduced by M. Toorani and A. Beheshti Shirazi [4]. It efficiently combines encryption and digital signature and uses public keys for a secure key establishment to be used for encrypting the short messages via a symmetric encryption. Since it deploys elliptic curves and a symmetric encryption algorithm, it has great computational advantages over the previously proposed public key solutions while simultaneously providing the most feasible security services. In a study of D. Lisonek and M. Drahansky [5] the application for securing of SMS has been designed and implemented, which prevents tapping and also substituting. For securing, it has been chosen the asymmetric cipher RSA. Brutal force decryption of RSA cipher with a length of 1,024 bit keys has not been successfully implemented yet. The best success is from year 2005, where J. Franke (University of Bonn) was able to factorize number with a length of 663 bits. The attacker also cannot be able of tapping and gradually building up the dictionary because it is used in the OAEP padding scheme. In the paper of C. Narendiran, S. Albert Rabara and N. Rajendran [6] an end-to-end security framework using PKI for mobile banking is proposed. The security framework solution allows us to provide strong customer authentication and non-repudiation by employing public-key cryptography for customer certificates and digital signatures. It is observed that the AES algorithm utilized less computation time and memory for encrypting the user's data. The AES model shows greater performance than the 3DES and RSA model that uses Public Key Infrastructure. Mahmoud Reza Hashemi and Elahe Soroush [7] proposed a secure m-payment protocol for mobile devices. They used a 163-bit key for ECC computations, which is proven to be equivalent to a 1024-bit key for RSA. The results show that ECDSA consumes less power than DSA. However, ECDSA and RSA digital signature algorithms have complementary power costs. RSA performs signature verification efficiently, while ECDSA imposes a smaller cost for signature generation. In the paper of Mohsen Toorani, Ali Asghar and Beheshti Shirazi [8], the security of the GSM network is evaluated, and a complete and brief review of its security problems is presented. Some practical solutions to improve the security of currently available 2G networks are also proposed.

Muhammad Saleem , Kyung-Goo Doh [9] proposes a method of building an extendable generic application which can be used to provide various types of information services using mobile SMS. Garza-Saldana and Diaz-Perez in their study [12] explained how symmetric encryption could provide confidentiality to SMS mobile payment protocol. Sonam in his study [13] investigated the security loopholes in SMS banking. He proposed and implements elliptic curve encryption scheme as a solution. Hosain et al [14] proposes a security system for improving the security of SMS by using A5 algorithm that is the exiting GSM technology. Kuate et al [15] describes and presented the implementation of an SMS security protocol called SMSsec. The SMSsec uses both asymmetric and symmetric encryption techniques to provide confidentiality to SMS messages. The paper [16] has demonstrated a wide range of shortcomings in widely used premium rate SMS business models. This paper [17] describes how we can use existing mobile technology to track the vehicle using SMS. This paper [18] proposes Home Network architecture integrated with WAP and SMS to support the connectivity between home and Internet/GSM networks.

IV. PROPOSED SOLUTION

The proposed approach provides secure end-to-end communications because it is required that SMS must be secured even from the network operator. The main concept of this proposal is that do the ciphering on SMS first, and then the digital signature are imposed. This signed encrypted SMS is finally transmitted. Asymmetric cryptography is used for encryption. This scheme secures the SMS against substitution with a fake SMS also.

This is realized through digital signing of the SMS. The advantage of asymmetric encryption is in its functionality. It provides security in a wide range of applications that cannot be solved using only symmetric techniques. The issue with asymmetric encryption is that it is slower than symmetric encryption because they require more computational processing power and which makes it impractical when trying to encrypt large amounts of data. But here, small data is to be encrypted like SMS and system don't want to send the shared secret key from one end to another of the peer entities, so it is suitable to choose asymmetric encryption for the SMS. This scheme supports some of the most used digital signature schemes (i.e. DSA, and ECDSA) and public-key based cryptosystems (i.e. RSA and El-gamal). A modified version of RSA is proposed with OAEP (Optimal asymmetric encryption padding) which will provide more security to the algorithm. Apart from these schemes, some message digest algorithms based on hash function or MAC function will also be analyzed and optimal solution based on these all algorithms will be implemented which ensure the proper security of SMS.

In the paper [6] digest algorithm used is SHA-1 as the message digest algorithm and encryption algorithms used are lightweight RSA algorithm with variable key sizes of 1024 bits, input plaintext 1KB, 3DES algorithm with variable key length 1024 is used and also AES algorithm with variable key length 256 is used for comparison with RSA and 3DES. I will propose and try to implement the improved solution model to this problem which will provide the greater security and efficiency to the model with the suitable key length with the different algorithms discussed above.

Programming Platform

All modern mobile phones allow to start and to run a user program. Java Micro Edition (J2ME) with Windows XP is used for the implementation of this work. Java ME: Java Micro Edition is developed by Sun Microsystems. This concept is hardware independent. The Java language is choose for the implementation of the framework because it is widely adopted in mostly all the mobile phones, ranging from the old-fashioned models to the latest ones.

V. IMPLEMENTATION AND RESULTS

These results show the end-to-end security of SMS sending between mobile stations.

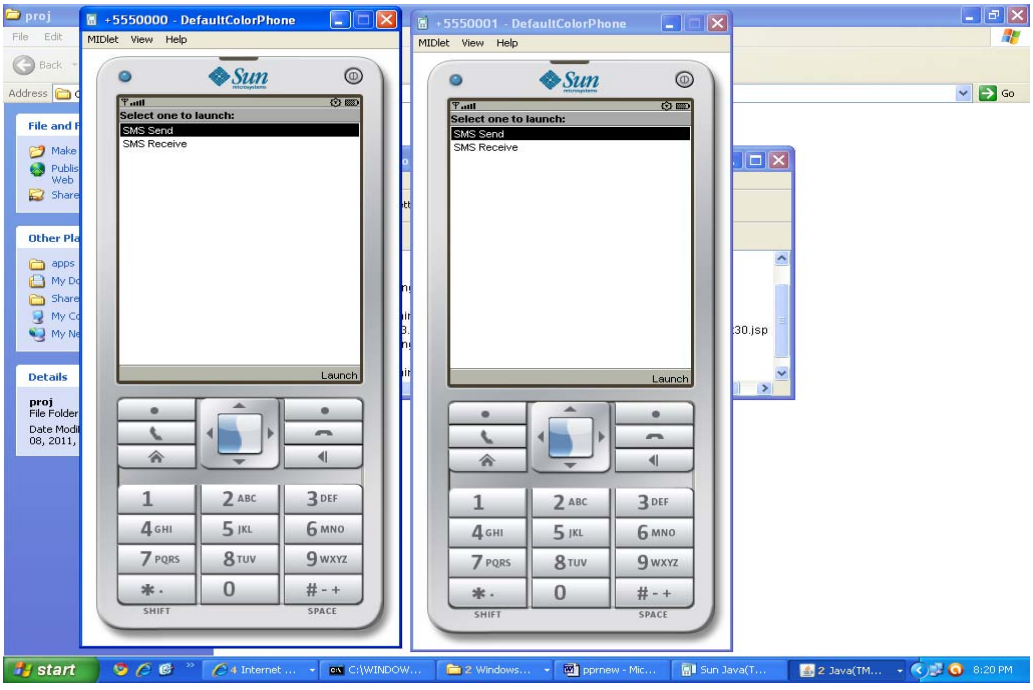

Figure-2: Mobile stations

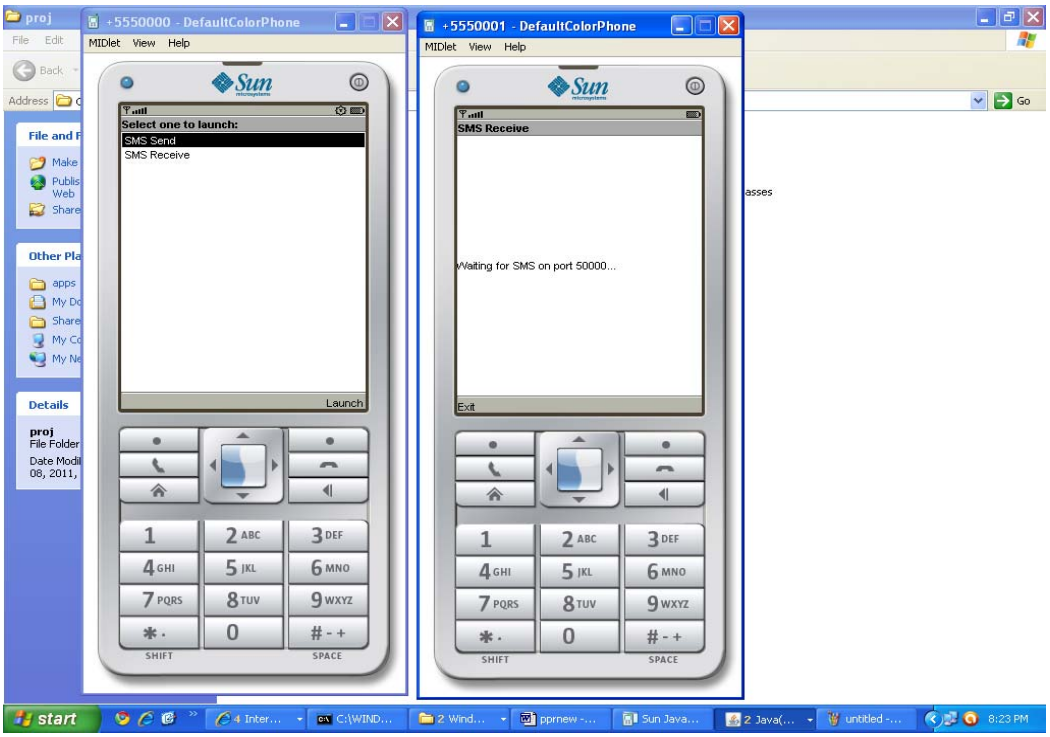

Figure-3: Receiver at port 50000

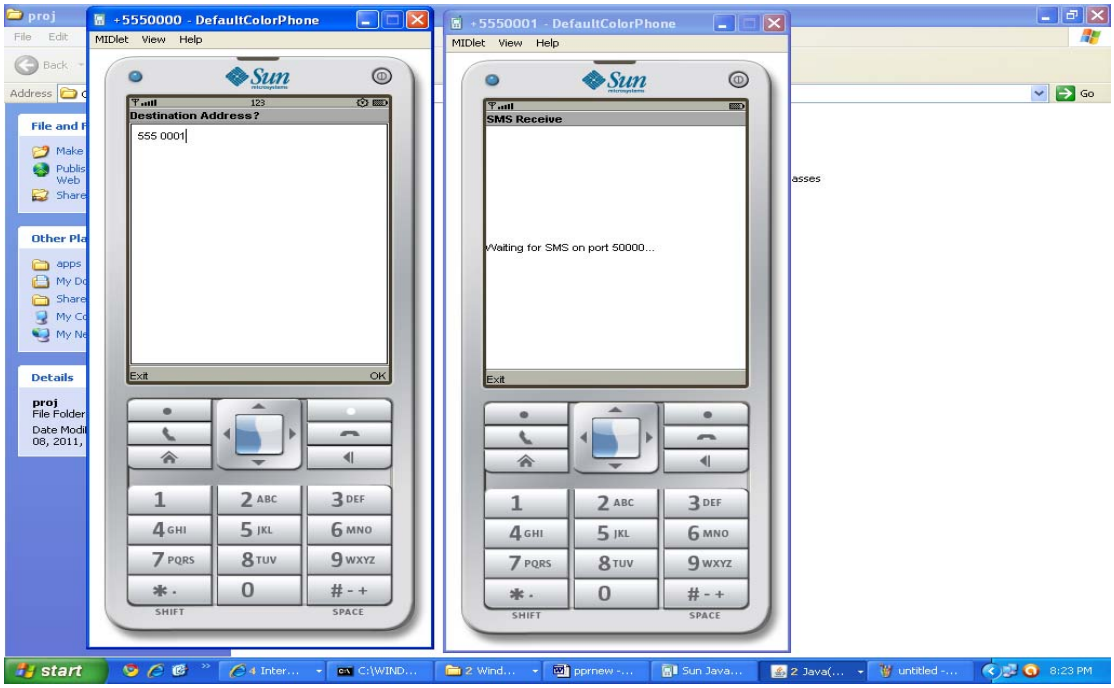

Figure-4: Destination address at sender mobile station

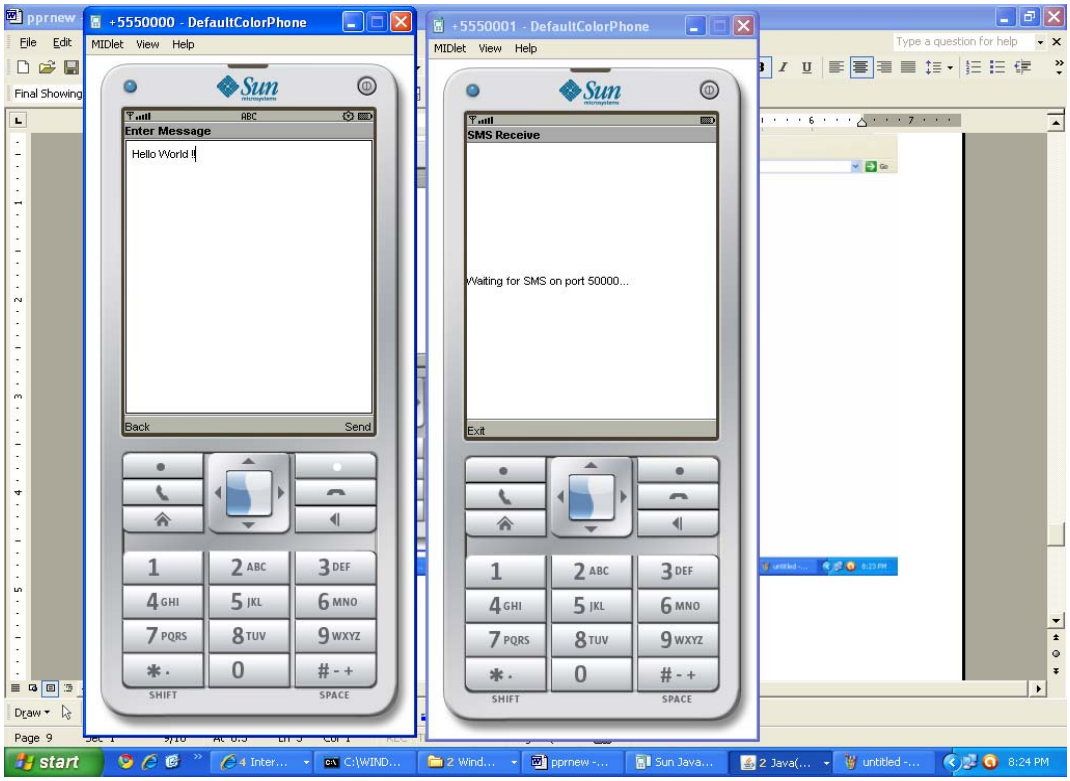

Figure-5: Add message at sender screen

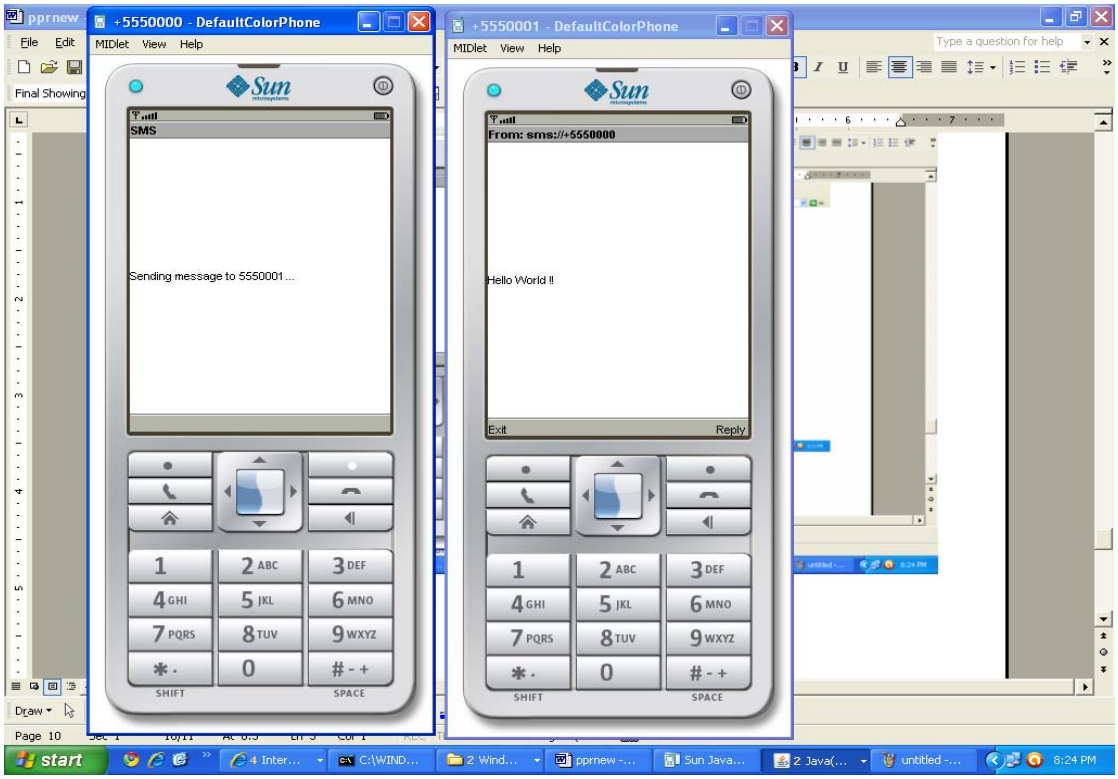

Figure-6: SMS reached at receiver

ACKNOWLEDGMENT

Authors want to thank for the support of GGSIPU Delhi. Apart from this, authors thankful to some faculty members of IMSEC GZb for their support in this project.

REFERENCES

[1] Mary Agoyi, Devrim Seral, "SMS Security: An Asymmetric Encryption Approach", Sixth International Conference on Wireless and Mobile Communications, 2010@IEEE, pp 448-452.

[2] Alfredo De Santis, Aniello Castiglione and Umberto Ferraro Petrillo "An Extensible Framework for Efficient Secure SMS" International Conference on Complex, Intelligent and Software Intensive Systems, 2010@IEEE, pp 843-850.

[3] Nassim Khozooyi, Maryam Tahajod, Peyman khozooyi, "Security in Mobile Governmental Transactions", 2009 Second International Conference on Computer and Electrical Engineering, 978-0-7695-3925-6/09 $26.00 © 2009 IEEE, pp 168-172.

[4] M. Toorani and A. Beheshti Shirazi, "SSMS - A secure SMS messaging protocol for the m-payment systems", in Computers and Communications, IEEE Symposium on, July 2008@IEEE, pp 700–705.

[5] D. Lisonek and M. Drahansky, "SMS Encryption for Mobile Communication", in Security Technology, SECTECH '08. International Conference on, Dec. 2008@IEEE, pp 198–201.

[6] C.Narendiran, S.Albert Rabara, N.Rajendran, "Performance Evaluation on End-to-End Security Architecture for Mobile Banking System", 978-1-4244-2829-8/08/$25.00, 2008@IEEE.

[7] Mahmoud Reza Hashemi, Elahe Soroush, "A Secure m-Payment Protocol for Mobile Devices", IEEE CCECE/CCGEI, Ottawa, May 2006, 2006@IEEE, pp 294-297.

[8] Mohsen Toorani, Ali Asghar Beheshti Shirazi, "Solutions to the GSM Security Weaknesses", the Second International Conference on Next Generation Mobile Applications, Services, and Technologies, 978-0-7695-3333-9 /08 $25.00 © 2008 IEEE, pp 576-581.

[9] Muhammad Saleem, Kyung-Goo Doh, "Generic Information System Using SMS Gateway", 2009 Fourth International Conference on Computer Sciences and Convergence Information Technology, 2009@IEEE, pp 861-866.

[10] J. Brown, B. Shipman, and R. S. Vetter, "SMS: The short message service," Computer, vol. 40, no. 12, 2007, pp. 106-110.

[11] W. Stallings, "Cryptography and network security", Prentice Hall, 2006, New Jersey, United State.

[12] J. J. Garza-Saldana and A. Diaz-Perez, "State of security for SMS on mobile devices", Proceedings of the Electronics, Robotics and Automotive Mechanics Conference, 2008, pp. 110 -115.

[13] Salman Firdaus bin Haji Sidek, "The Development of the Short Messaging Service (SMS) Application for the School Usage", 978-1-4244-6716-7/10/$26.00, 2010@ IEEE, pp 1382-1386.

[14] M. A. Hossain, S. Jahan, M. M. Hussain, M.R. Amin, and S.H. S Newaz, "A proposal for enhancing the security system of short message services in GSM", 2nd International Conference on Anti-counterfeiting, Security and Identification, ASID, Guiyang, China, 2008@IEEE, pp. 235-240.

[15] Jong-Won Seo, Je-Gyeong Jo, Hyung-Woo Lee, "SMS(Short Message Service) based Secure Authentication & Accounting Mechanism in Wireless Network", 2006 International Conference on Hybrid Information Technology (ICHIT'06), 2006@IEEE.

[16] Philip Garner, Ian Mullins, Reuben Edwards, Paul Coulton, "Mobile Terminated SMS Billing – Exploits and Security Analysis", Proceedings of the Third International Conference on Information Technology: New Generations (ITNG'06), 2006@IEEE.

[17] Asim Mukherjee, "Transport Security using Mobile Technology", ISI 2008, June 17-20, 2008, Taipei, Taiwan, 2008@IEEE, pp 275-276.

[18] Liu Pu, "Research of Home Network Based on Internet and SMS", 978-1-4244-4589-9/09/$25.00, 2009@IEEE.