International Journal of Electrical and Electronics Engineers
Vol. No.8 Issue 01, January-June 2016
www.arresearchpublication.com
IJEEE
ISSN 2321 - 2055

SECURE SMS FOR END-TO-END TRANSMISSION USING PROTOCOL IN WIRELESS NETWORKS

Kannadhasan.S[1], Bhapith V.B[2]

[1,2]*Research Scholar, Department of Electronics and Communication Engineering, Anna University, Chennai, Tamilnadu (India)*

ABSTRACT

The information sent from one mobile to another mobile is called as SMS (Short Message Service). This SMS service is used in many applications such as healthcare monitoring, mobile banking, mobile commerce, and so on. The information may contain account number and password, but the traditional Cellular architecture system does not provide privacy for that information. For this reason we go for proposed system to achieve privacy in SMS. In our proposed system, we implement a secure and efficient protocol called the Easy SMS. It provides secure end to end communication before the transmission of SMS. The proposed protocol Easy SMS prevents various attacks like SMS disclosure, over the air modification, replay attack, man-in-the middle attack, and impersonation attack. In existing system, SMS Sec and PK-SIM are used for secure communication between mobiles. But these protocols do not achieve privacy in it. In our proposed system, the computation overhead is reduced compared to the existing protocols. It also reduces the communication overhead, bandwidth utilization and message exchanged ratio. EasySMS is the first protocol completely based on Symmetric key cryptography and it retains the original cellular architecture.

Keywords: Encryption, Decryption, SMS, GSM

I. INTRODUCTION

SMS is supported by all Global System for Mobile Communications (GSM) mobile phones and is also available on third generation (3G) wireless networks. SMS messages are also sent via Web-based browser applications, instant message (IM) applications and Voice over Internet Protocol (VoIP) applications, such as Skype. An SMS message is sent from a device to a Short Message Service Center (SMSC), which, in turn, communicates with mobile networks to determine the subscriber's location. Then, the message is forwarded as a small data packet to the destination device. Subsequent messages sent by the original source device undergo the same process, also known as store and forward.

Cryptography is an algorithmic process of converting a plain text or clear text message to a cipher text or cipher message based on an algorithm that both the sender and receiver know, so that the cipher text message can be returned to its original, plain text form. In its cipher form, a message cannot be read by anyone but the intended receiver. The act of converting a plain text message to its cipher text form is called enciphering. Reversing that act (i.e., cipher text form to plain text message) is deciphering. Enciphering and deciphering are more commonly referred to as encryption and decryption, respectively.

II. RELATED WORK

Various authors have proposed different techniques to provide security to the transmitted messages. An implementation of a public key cryptosystem for SMS in a mobile phone network has been presented but, the security analysis of the protocol has not discussed. A secure SMS is considered to provide mobile commerce services and is based on public key infrastructure. A framework Secure Extensible and Efficient SMS (SEESMS) is presented which allows two peers to exchange encrypted communication between peers by using public key cryptography. Another new application layer framework called SSMS is introduced to efficiently embed the desired security attributes in SMS to be used as a secure bearer for m-payment systems and solution is based on the elliptic curve-based public key that uses public keys for the secret key establishment. An efficient framework for automated acquisition and storage of medical data using the SMS based infrastructure is presented and the results conclude that the proposed SMS based framework provides a low-bandwidth, reliable, efficient and cost effective solution for medical data acquisition. It generates huge overheads and not suitable for the real world applications. It is not clear whether the proposed approaches are able to prevent SMS against attacks. All the approaches/protocols/frameworks generate a large overhead as they propose an additional framework for the security of SMS. Due to physical limitations of the mobile phones, it is recommended to develop a protocol which would make minimum use of computing resources and would provide better security. However, implementation of framework always increases the overall overhead which is not much suitable for the resource constraints devices such as mobile phones. Thus, in this paper we compared our proposed protocol with the existing SMSSec and PK-SIM protocols. The reason for choosing these protocols for comparison is that these are the only existing protocols which do not propose to change the existing architecture of cellular networks. We wanted to compare our proposed protocol with some existing protocols devoted to provide end-to-end SMS security with symmetric key cryptography, but there is no such protocol exists. Both protocols are having two phases similar to the proposed protocol and are based on symmetric as well as asymmetric key cryptography while the proposed protocol is completely based on symmetric key cryptography functionality. Both protocols are based on client-server paradigm, i.e., one side is mobile user and the other side is authentication server but they do not present any scenario where an SMS is sent from one mobile user to another mobile user. The SMSSec protocol does not illustrate the security analysis.

III. PROPOSED SYSTEM

In our proposed system we used an efficient and secure protocol called EasySMS which provide end-to-end SMS security with symmetric key cryptography. And our proposed system is totally based on symmetric key cryptography. The various cipher algorithms are implemented with the proposed authentication protocol. The transmission of symmetric key to the mobile users is efficiently managed by the protocol. In EasySMS the low amount of bits are transmitted and generates less computation overhead, and reduces bandwidth consumption and message exchanged. And the SMS information can be prevented from various attacks when using easy SMS. The attacks are message disclosure, over the air modification, replay attack, man-in-the middle attack, and impersonation attack. In our concept the user able to send both SMS such as new message and secure message.

3.1 System Architecture

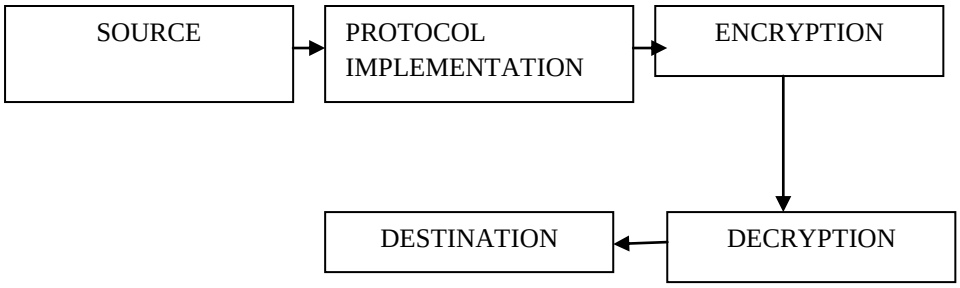

Figure 1: System Architecture

3.2 Selection process

In this stage the user chooses the option whether they want to send normal SMS or secure SMS and also chooses the receiver. If the user wants to send a normal SMS in the sense she/he can establish a connection without any authentication and then starts communication. Or otherwise a user wants to send a secure message to other user the proposed protocol EasySMS is to be executed. A secure message service is to be implemented in both sender and receivers mobile phones.

3.3 EasySMS protocol implementation

EasySMS protocol implementation is the second module of our proposed system. Here we used this protocol to achieve end to end secure communication. If the users want to send the message with secure then they select easysms application. Here the messages are protected from other unwanted persons and attacks. It use symmetric key encryption algorithm to achieve privacy.

3.4 Symmetric key encryption

For encryption process we propose Symmetric key encryption. In this stage the plaintext is converted into the cipher text with key. All the transmission among various AS take place by encrypting the message with a symmetric key shared between each pair of AS. The efficiency of a block cipher algorithm depends upon the block size and key size. We can encrypt large chunk of data in one cycle of the algorithm with a larger block size. If the number cycles are increases then the algorithm is slower. The Speed of the algorithm depends on the number of rounds used.

In our proposed system, we used symmetric key for security purpose. We create one new application for secure end to end communication. The new application name is Easysms. If the user selects the Easysms application for message transmission it first encrypt the message then only it send the message to the receiver with symmetric key. The receiver only sees the message by providing their symmetric key. Encryption is the conversion of data into a form, called a ciphertext, that cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood.

3.5 SMS Transmission

After completing the encryption process, then we start the transmission. Here the SMS is transmitted to the receiver with encryption key. The encryption key is generated when encrypting the message. This encryption

key provides privacy for that information. In our proposed system, we used symmetric key encryption algorithm for encryption.

3.6 Symmetric key decryption

After the message sending then the receiver can see the encrypted message by using their key. Here the message is decrypted by receiver. The cyber text is converted into the plain text is called decryption. In decryption, the system extracts and converts the garbled data and transforms it to texts and images that are easily understandable not only by the reader but also by the system. Decryption may be accomplished manually or automatically. It may also be performed with a set of keys or passwords.

One of the foremost reasons for implementing an encryption-decryption system is privacy. As information travels over the World Wide Web, it becomes subject to scrutiny and access from unauthorized individuals or organizations. As a result, data is encrypted to reduce data loss and theft. Some of the common items that are encrypted include email messages, text files, images, user data and directories. The person in charge of decryption receives a prompt or window in which a password may be entered to access encrypted information.

IV. PROPOSED PROTOCOL

In order to overcome the stated attacks, various cipher algorithms are implemented withthe proposed authentication protocol. We recommend that the cipher algorithms should be stored onto the SIM (part of MS) as well as at AS. Authors propose to include one more service as 'Secure Message' in the menu of mobile software developed by various mobile companies. Mobile operators can add some extra charges to send secure message by their customers over the networks. Whenever a user wants to send a secure message to other user, the proposed protocol namely EasySMS is executed which makes available the symmetric shared key between both MS and then ciphering of message takes place using a symmetric key algorithm.

In this section, we propose a new protocol named EasySMS with two different scenarios which provide end-to-end secure transmission of information in the cellular networks. First scenario is illustrated in Fig. 4.2 where both MS belong to the same AS, in other words share the same Home Location Register (HLR) while the second scenario is presented in Fig. 4.3 where both MS belong to different AS, in other words both are in different HLR. There are two main entities in the EasySMS protocol. First is the Authentication Server (AS), works as Authentication Center (AuC) and stores all the symmetric keys shared between AS and the respective MS. In this paper, we refer AuC as the AS. Second entity is the Certified Authority/Registration Authority (CA/RA) which stores all the information related to the mobile subscribers.

We assume that every subscriber has to register his/her mobile number with CA/RA entity and only after the verification of identity, the SIM card gets activated by this entity. Thus, this entity is responsible to validate the identity of the subscribers. We also assume that a symmetric key is shared between the AS and the CA/RA which provides the proper security to all the transmitted information between AS and CA/RA. It is considered that various authentication servers are connected with each other through a secure channel since one centralized server is not efficient to handle data all around. We consider all the transmission among various AS take place by encrypting the message with a symmetric key shared between each pair of AS.

International Journal of Electrical and Electronics Engineers
Vol. No.8 Issue 01, January-June 2016
www.arresearchpublication.com
IJEEE
ISSN 2321 - 2055

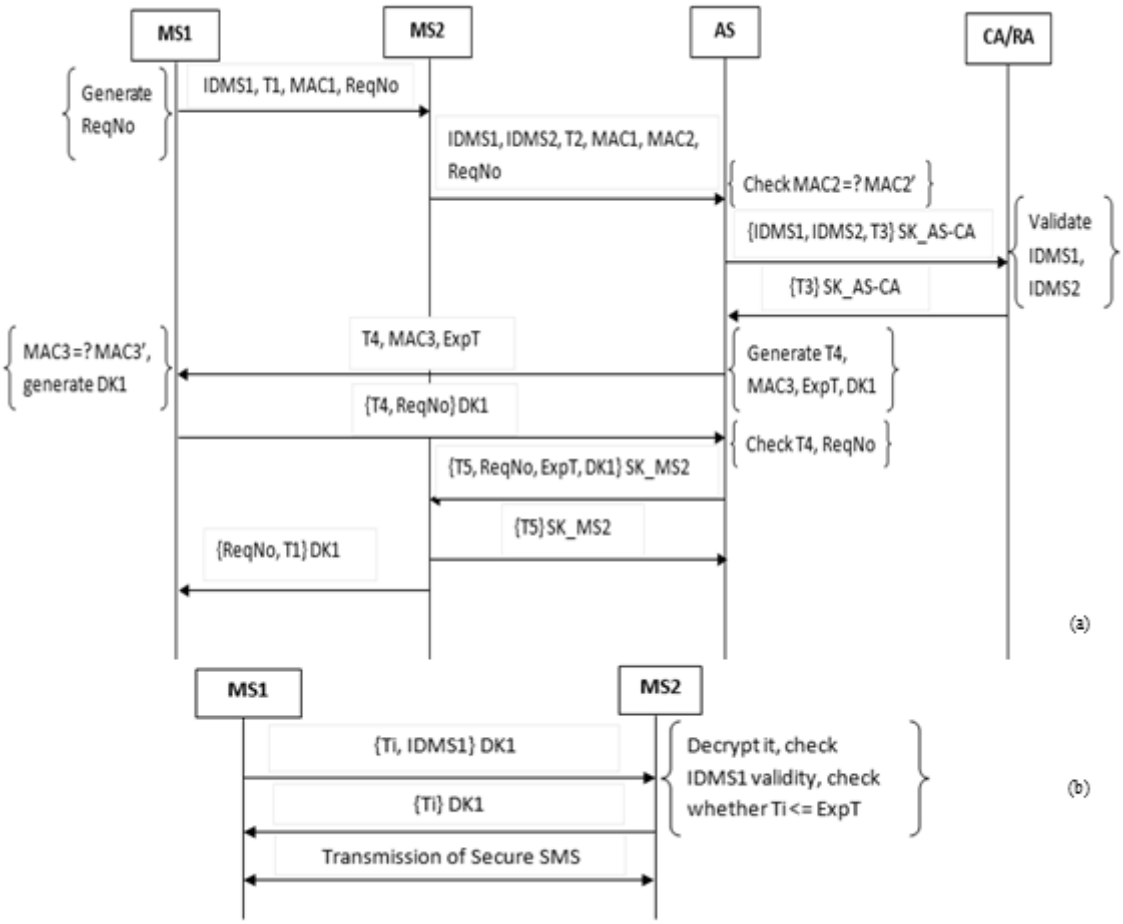

Figure 2: MS1 sends a message toMS2 and both MS belong to the same AS.

When Both MS Belong to Same AS: This scenario is presented in Fig. 2 where MS1 sends a message toMS2 and both MS belong to the same AS.

First, the mobile user who wants to send the SMS (say MS1) transmits an initial request to other mobile user (say MS2) for the connection. This initial request consists of International Mobile Subscriber Identity (IMSI) of MS1 (say IDMS1), a timestamp T1, a request number ReqNo and a message authentication code MAC1 = f1SK1(IDMS1 ||ReqNo). Here, SK1 is a symmetric key shared between the MS1 and the AS2. On receiving the message from MS1, the mobile user who receives this request (say MS2) computes the MAC2 = f1SK2 (IDMS2||T2||MAC1). Then MS2 sends a message to the AS containing the IDMS1, IDMS2, T2, MAC1, ReqNo and MAC2 where IDMS2 is the IMSI of the MS2. The SK2 is a symmetric key shared between MS2 and the AS. With this message, the MS2 requests to the AS to check the validity of the IDMS1. When the AS receives a message from the MS2, it computes the MAC2' =f1SK2(IDMS2||T2||MAC1) and compares it with the received MAC2. If it holds then the AS sends not only the IDMS1 but also the IDMS2 to the CA/RA along with a timestamp T3 using a symmetric shared key between AS and CA/RA (say SK_AS-CA) to validate the identity of both MS. If, MAC2 and MAC2' are not equal then the connection is terminated. Next, the CA/RA checks the validity of both entities and sends the reply back to the AS with the received timestamp T3. On receiving the message from the CA/RA, if the AS finds any of the entities is invalid then the connection is simply terminated and MS1 needs to send a fresh connection request. If both entities are valid then the AS generates a new

timestamp T4, an expiry time to authenticate MS1 (say ExpT), a delegate key DK1 generated from the SK1 using a function f2 and a new message authentication code MAC3=f1SK1(T4||ExpT||ReqNo) and DK1= f2SK1(T4||ReqNo). Then the AS sends (T4, MAC3, ExpT) to the MS1. After receiving the message from AS, the MS1 first computes MAC3' and compares it with the received MAC3, where MAC3'= f1SK1(T4||ExpT||ReqNo). If both are same then MS1 computes the DK1. Next, MS1 sends T4 and the corresponding ReqNo to the AS encrypted with the DK1 key. The AS checks the received T4 with its stored value and confirms ReqNo. If both are correct then the authentication of MS1 iscompleted. Thereafter, the AS sends DK1 to the MS2 along with a new timestamp T5, ExpT and ReqNo after encrypting all using the SK of MS2 (SK_MS2) which is a shared key between AS and MS2.The MS2 simply confirms the reception of DK1 key by replying to the AS, the T5 encrypted with the SK of MS2. MS2 also sends ReqNo and T1 to the MS1 encrypted with DK1 so that MS1 can verify the correctness of T1 and ReqNo. This message also verifies the successful reception of DK1 by the MS2.

Once both MS have a shared secret symmetric key, they can exchange the message information in a secure manner using a suitable and strong cryptographic algorithm like AES. After phase-1, a session is generated which provides the secure communication between both MS for a specified time period ExpT. In this time period the same DK1 key is used to provide ciphering between MS1 and MS2 but after the ExpT time the session gets expire and MS1 needs to send a fresh request to MS2 with a new request number ReqNo with the same procedure of phase-1. Within the ExpT, the following steps are used for the communication between both MS. The MS1 sends the IDMS1 and a timestamp (say Ti) to the MS2 encrypted with symmetric key of MS1 i.e., DK1. MS2 decrypts the message using the same DK1 key and checks the validity of IDMS1 and verifies whether Ti <= ExpT. If both are correct then MS1 is successfully authenticated and proved as a validuser for the connection. Then MS2 replies the same received Ti encrypted with DK1 as an acknowledgement to MS1. Secure SMS communication between both MS takes place.

In the above explained scenario both MS belongs to the same authentication server and secure SMS communication is established between them. The process of encryption and decryption is carried out using the same key

International Journal of Electrical and Electronics Engineers
Vol. No.8 Issue 01, January-June 2016
www.arresearchpublication.com
IJEEE
ISSN 2321 - 2055

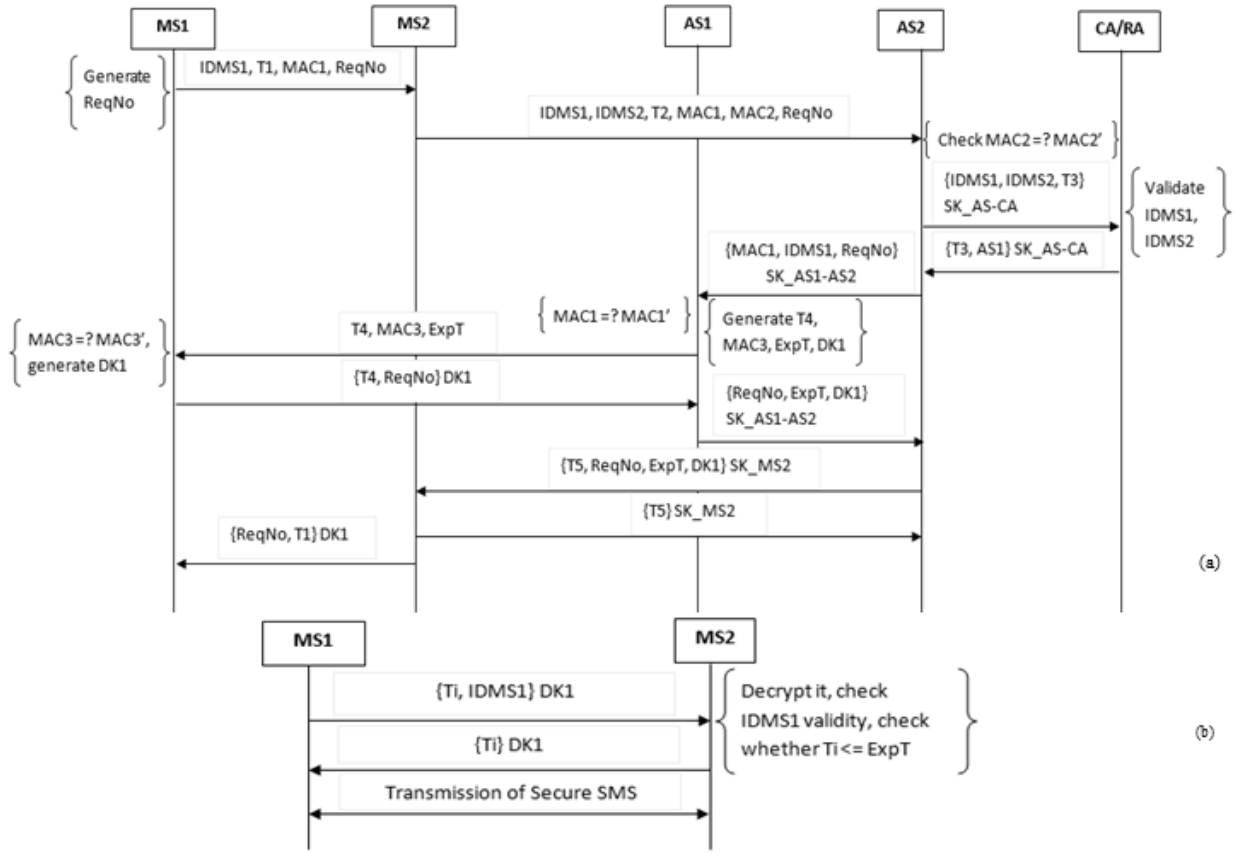

Figure 3: MS1 sends a message to MS2 while both MS belong to the different AS

This scenario is presented in Fig. 3 where MS1 sends a message to MS2 while both MS belong to the different AS. This case is one where both mobile users are located in the geographically far areas and they have different authentication centers. It may be the case where both MS are of different service providers so they genuinely have different authentication centers. This scenario is also subdivided into two phases. It is same as presented in step-1 of scenario-1. Here, SK1 is a symmetric key shared between MS1 and AS1.The MS2 passes (IDMS1, IDMS2, ReqNo, T2, MAC1, MAC2) to the AS through which it is connected (say AS2). The SK2 is a symmetric key shared between MS2 and the AS2. With this message, the MS2 requests to the AS2 to check the validity of the IDMS1. The MS2 stores the timestamp T1in the memory which was received from the MS1. The AS2 computes the same as presented in step-3 of scenario-1 and checks whether MAC2?=MAC2'. The CA/RA checks the validity of both entities and sends the reply back to the AS2 with the received timestamp T3 and the identity of AS to which MS1 belongs (say AS1). The AS2 checks the same as in scenario-1 step-5, if both entities are valid then the AS2 sends (IDMS1, ReqNo, MAC1) to the AS1 through a secure channel or using a symmetric key shared between AS1 and AS2 (say SK_AS1-AS2). We assume that all AS communicate with each other using the pre-computed symmetric shared keys. When the AS1 receives the message from the AS2, it computes MAC1'= f1SK1(IDMS1||ReqNo) and compares MAC1' with the received MAC1. If both are different thenthe connection is terminated. If both are same then the AS1 generates a new timestamp T4, an expiry time to authenticate MS1 (say ExpT), a delegate key DK1 generated from the SK1 of MS1 using a function f2, and a MAC3, where MAC3 = f1SK1(T4||ExpT||ReqNo) and DK1 = f2SK1(T4||ReqNo). Then the AS1 sends (T4, MAC3, ExpT) to the MS1. After receiving the message from AS1, MS1 repeats the same as in

International Journal of Electrical and Electronics Engineers
Vol. No.8 Issue 01, January-June 2016
www.arresearchpublication.com
IJEEE
ISSN 2321 - 2055

scenario-1 step-6 and sends (T4, ReqNo) to the AS1 encrypted with DK1 key. The AS1 checks T4 and ReqNo as in scenario-1 step-7. Then AS1 conveys the confirmation of the authentication of MS1 by sending a message (ReqNo, ExpT, DK1) to the AS2 using SK_AS1-AS2 key. The AS2 sends DK1 to the MS2 along with a new timestamp T5, expiry time ExpT and request number ReqNo after encrypting all using the SKof MS2 (say SK_MS2) which is a shared key between the AS2 and the MS2. (MS2 repeats the same as in scenario-1 step-8, and sends encrypted reply of T5 to the AS2. It is same as in scenario-1 step-9.

V. RESULTS AND DISUSSION

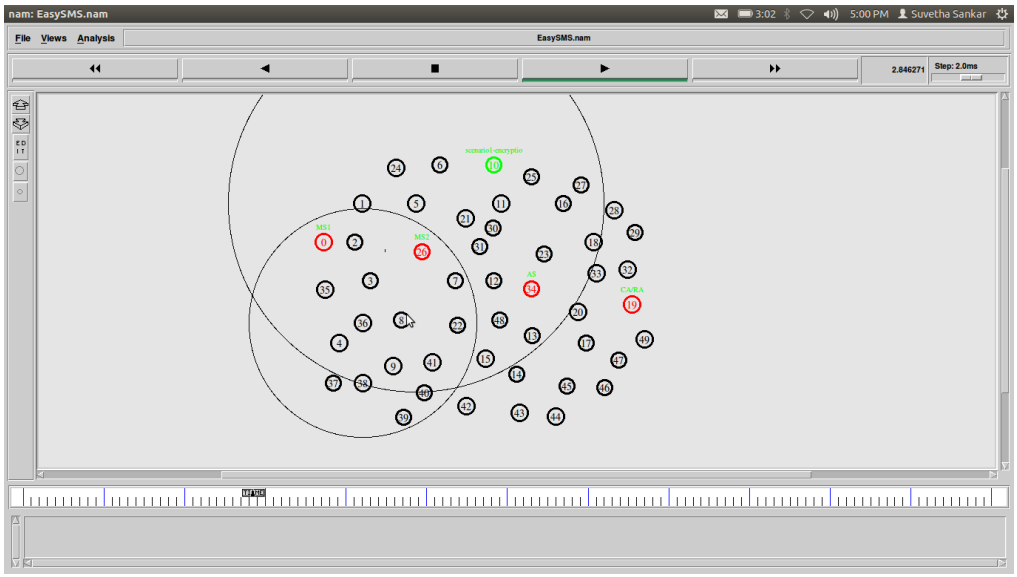

Figure 4: Encryption Authentication

The process of encryption as shown in Fig 4 takes place in this Phase. Here AS and CA/RA checks the validity of both MS. After authentication is validated, Encryption is done.

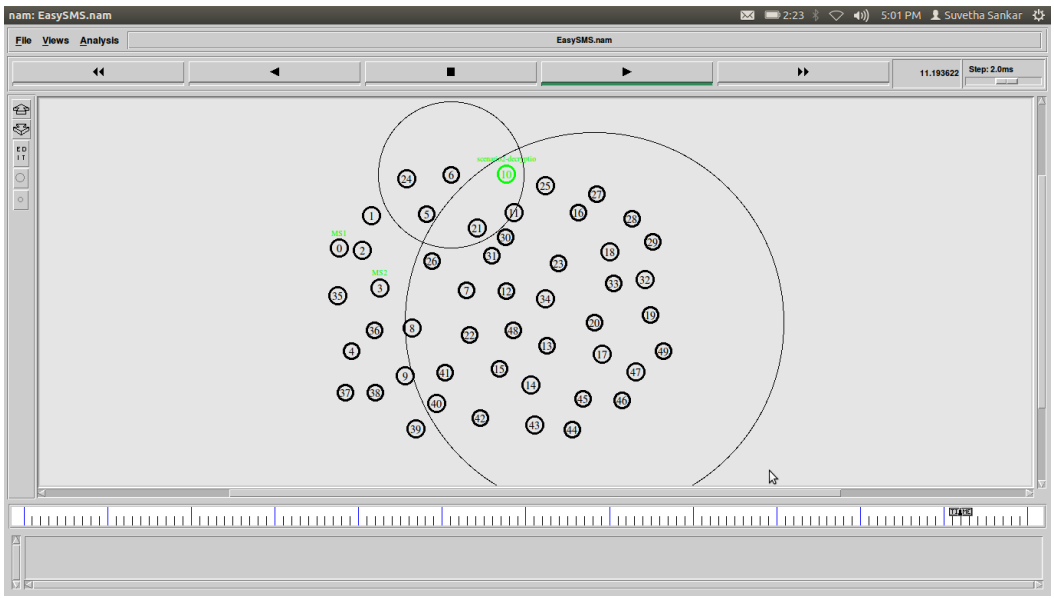

Figure 5: Decryption Authentication

International Journal of Electrical and Electronics Engineers
Vol. No.8 Issue 01, January-June 2016
www.arresearchpublication.com
IJEEE
ISSN 2321 - 2055

The process of Decryption as shown in Fig 5 takes place in this phase. Here mutual authentication between both MS takes place and Secure transmission of SMS takes place.

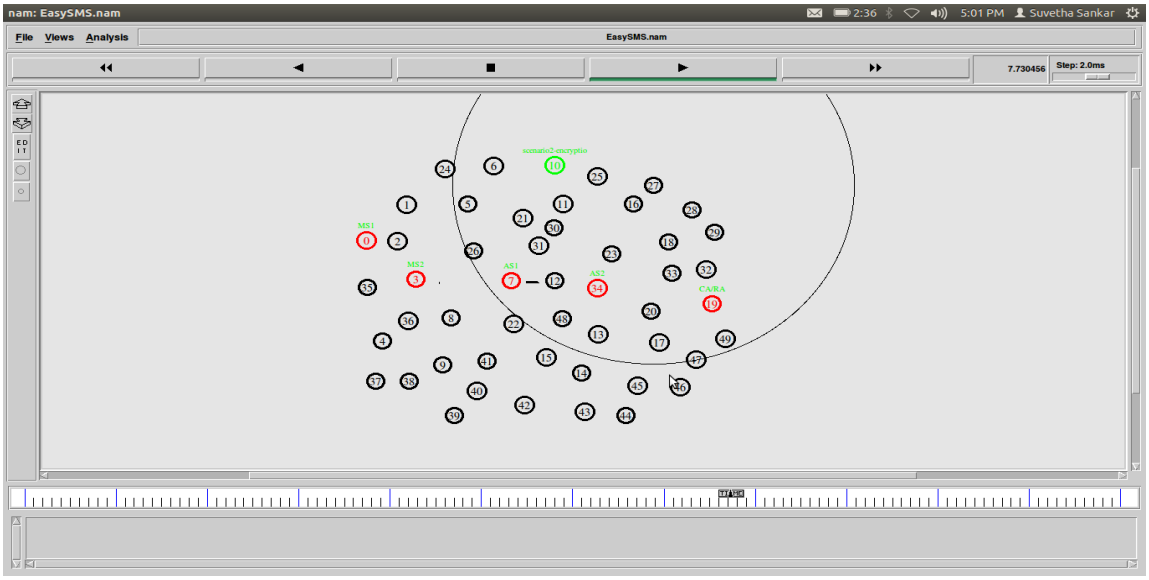

Figure 6: Authentication of MS1 and MS2 is done by AS1 and AS2 respectively

Authentication of MS1 and MS2 is done by AS1 and AS2 respectively. After authentication encryption takes place as shown in Fig 6

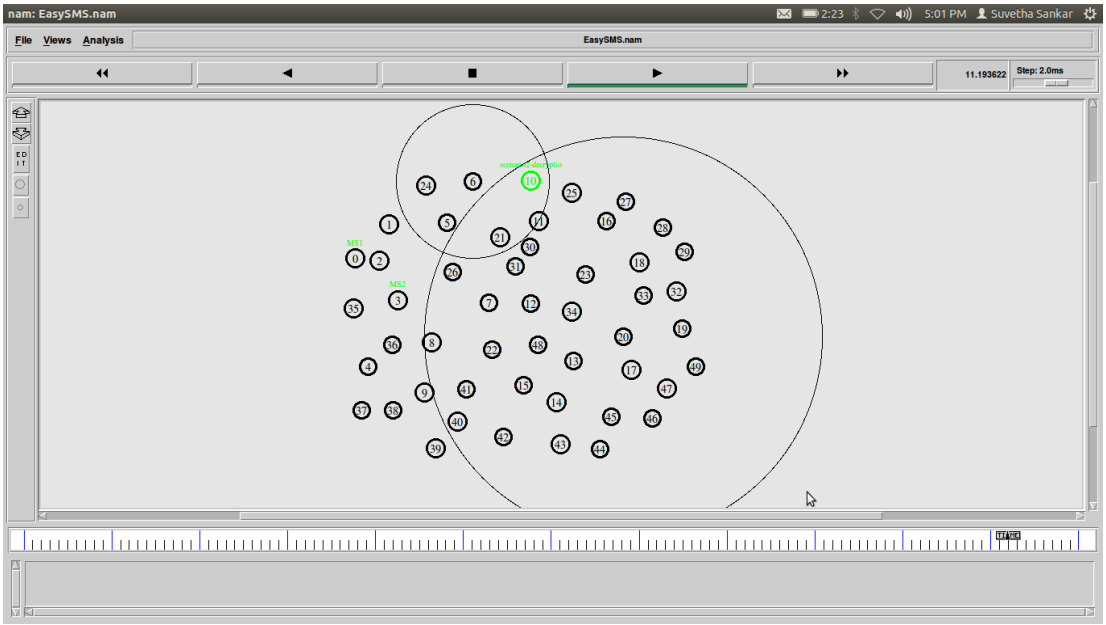

Figure 6: Mutual authentication between both MS

The process of Decryption as shown in Fig 7 takes place in this phase. Here mutual authentication between both MS takes place and Secure transmission of SMS takes place.

VI. CONCLUSION

EasySMS protocol is successfully designed in order to provide end-to-end secure communication through SMS between mobile users. The analysis of the proposed protocol shows that the protocol is able to prevent various

attacks. The transmission of symmetric key to the mobile users is efficiently managed by the protocol. This protocol produces lesser communication and computation overheads, utilizes bandwidth efficiently, and reduces message exchanged ratio during authentication than SMSSec and PK-SIM protocols.

REFERENCES

[1] Biryukov, O. Dunkel, N. Keller, D. Khovratovich, and A. Shamir, "Key recovery attacks of practical complexity on AES-256 variants with up to 10 rounds," in Advances in Cryptology. Berlin, Germany: Springer- Verlag, 2010, pp. 299–319.

[2] J. Choi1, J. Kim, J. Sung, S. Lee, and J. Lim, "Related-key and meetin-the-middle attacks on triple-DES and DES-EXE," in ComputationalScience and Its Applications (Lecture Notes in Computer Science), vol. 3481. Berlin, Germany: Springer-Verlag, 2005, pp. 567–576

[3] Y. Khiabani, S. Wei, J. Yuan, and J. Wang, "Enhancement of secrecy of block ciphered systems by deliberate noise," IEEE Trans. Inf. Forensics Security, vol. 7, no. 5, pp. 1604–1613, Oct. 2012.

[4] H. Kim, "Improved differential fault analysis on AES key schedule," IEEE Trans. Inf. Forensics Security, vol. 7, no. 1, pp. 41–50, Feb. 2012.

[5] C. F. Lu, Y. S. Kan, H. Chiang, and C. Yang, "Fast implementation of AES cryptographic algorithms in smart cards," in Proc. IEEE 37th ICCST, Oct. 2003, pp. 573–579.

[6] P. Mondal, P. Desai, S. K. Ghosh, and J. Mukherjee, "An efficient SMSbased framework for public health surveillance," in Proc. IEEE PHT, Jan. 2013, pp. 244–247.

[7] M. Toorani and A. Shirazi, "SSMS—A secure SMS messaging protocol for the m-payment systems," in Proc. IEEE ISCC, Jul. 2008, pp. 700–705.

[8] W. N. Venables and B. D. Ripley, Modern Applied Statistics With S, 4th ed. New York, NY, USA: Springer-Verlag, 2002, p. 497.

[9] S. Wei, J. Wang, R. Yin, and J. Yuan, "Trade-off between security and performance in block ciphered systems with erroneous ciphertexts," IEEE Trans. Inf. Forensics Security, vol. 8, no. 4, pp. 636–645, Apr. 2013.