International Journal of Engineering Research and General Science Volume 3, Issue 4, July-August, 2015
ISSN 2091-2730

# A Survey on Different Protocols for Secure Transmission of SMS

Santhi Mol P.
Dept. of Computer Science and Engg.
Sree Buddha College of Engg. For Women
Pathanamthitta, Kerala, INDIA
santhimol123@gmail.com

**Abstract**—Short Message Service (SMS) is one of the most important mobile services. SMS enables the sending and receiving of messages between mobile phones, and is being used in many applications like healthcare monitoring, mobile banking, etc. Nowadays security is the most challenging aspects in the internet and network application. The main important drawback of the traditional SMS is lack of security. This is because sometimes SMS information may be credential like passwords, account numbers, etc. Traditional SMS service does not provide encryption of the information before its transmission. Cryptography is a main category of computer security that converts information from its normal form into an unreadable form. Various authors have proposed different techniques to provide security to transmit messages. This paper provides a comparative study of different protocols for end to end secure transmission of SMS.

**Keywords**— AES, Cryptography, Encryption, Protocols, Security, SMS, Transmission.

## INTRODUCTION

SMS has become one of the most important, fastest and strong communication channels to transmit the information. On December 3, 2013, SMS service has completed its 21 years as on December 3, 1992 [1]. The world's first SMS was sent by Neil Papworth from the UK through the Vodafone network [1]. Cryptographic system is "a set of cryptographic algorithms together with the key management processes that support use of the algorithms in some application context [2]." The main characteristics of encryption algorithm are the ability to secure the protected data against attacks.

Jawahar Thaku et al. [2] provide a detailed comparison between three common symmetric key cryptographic algorithms that is DES, AES and Blowfish. This paper showed that Blowfish algorithm is better than other encryption algorithms like DES and AES. So Blowfish algorithm is considered as a standard encryption algorithm. In [1] some existing symmetric key algorithms like DES, triple DES with 3 keys and AES have been implemented. Out of these algorithms AES takes minimum time to encrypt and decrypt the SMS with various sizes where one SMS size is 160 characters. DES and Triple DES are not considered as secure algorithms, since some attacks have been found on both algorithms. AES with 128 bit key has proved to be a secure and efficient algorithm to encrypt SMS but, its security cannot maintain in subsequent years. Various researchers have found several attacks on AES with 128bit key. So a variant of AES is introduced in [1] that is Modified AES (MAES). MAES with 256 bit key is more secure than original AES.

## SECURE TRANSMISSION PROTOCOLS

There are so many protocols introduced by different authors for end to end transmission of SMS. These are distinguished with its efficiency. This paper provides a comparative study of different protocols for end to end secure transmission of SMS.

Gary Belvin [4] proposed two separate protocols for secure text messaging. First establishes a secure session on top of the Short Message Service utilizing a shared secret. The second protocol is used to establish that shared secret. The Secure SMS (SSMS) initiates a secure session over SMS like Secure Real-time Transport Protocol (SRTP) establishes a secure session over RTP. SSMS encrypts and authenticates each text message with a sequence number to prevent replay attacks. SSMS also has forward secrecy characteristics that safeguard previously transmitted text messages in the case of an endpoint compromise. SSMS gives integrity, confidentiality, and replay attack protection for SMS messages like SRTP does for RTP media streams. The security of SSMS is built on a single, externally provided, master key that is analogous to the SRTP master key. The key Agreement Protocol for SMS (KAPS) establishes a secular shared secret using a minimal set of messages. KAPS uses the Elliptic Curve Diffie-Hellman primitive for share secret computation, with key continuity and one-time verbal authentication for man-in-the-middle detection. KAPS has the advantage of being completely peer-to-peer and time related.

J. L. C. Lo et al. [5] proposed a protocol called SMSSsec that can be used to secure a SMS communication. SMSSec has a two-phase protocol with the first handshake using asymmetric cryptography which occurs only once, and a more efficient symmetric *n*th handshake which is used more dominantly. SMSSec is presented to ensure an end-to-end secure SMS communication. Throughout this paper, SMSSec is found to be secure, reliable and efficient.

Deepthi Sucheendran et al. [7], proposed SMSSec protocol, which make use of the symmetric key shared between the end users thus providing secure and safe communication between two users. It also provides a way for remote destruction and remote locking in the case of the phone is lost or stolen.

A. De Santis et al. [6] proposed another protocol. That is (Secure Extensible and Efficient SMS) SEESMS. A Secure Extensible and Efficient SMS (SEESMS) mainly to transmit secure SMS it main goal is to support several cryptosystems through a modular architecture. SEESMS operates at the application level and can be used for changing secure SMS in the peer to peer. SMS based communication channel as bearer service to exchange non-reputable, encrypted, and tamper proof messages. SEESMS protocol fulfils a secure SMS messages exchange by using binary SMS messages instead of using a traditional message. Each binary SMS message can carry 140 bytes. SEESMS allows two peers to exchange encrypted communication between peers by using public key cryptography. In public key Cryptography, both sender and receiver use different keys. SEESMS assists the encryption of a communication channel through the ECIES and the RSA algorithms. This efficiency is obtained in two steps. First, all the cryptosystems available in the structure are implemented using mature and fully optimized cryptographic libraries. Second, an experimental analysis was organized to determine which combination of cryptosystems and security parameters were able to provide a better trade-off in terms of speed/security and energy consumption.

EasySMS [1] is a secure end to end transmission protocol. It is an efficient and secure protocol. Analysis of this protocol shows that this protocol is able to protect from various attacks, including message disclosure, over the air modification, replay attack, man-in-the middle attack, and impersonation attack. In this paper, this protocol compared with several existing SMSsec and PK-SIM protocols. These protocols having two phases similar to EasySMS protocol and are based on symmetric as well as asymmetric key cryptography while the proposed protocol is completely based on symmetric key cryptography. Authors claim that EasySMS is the first protocol completely based on the symmetric key cryptography and retain original architecture of cellular network. This paper shows that the EasySMS sends lesser number of transmitted bits, generates less computation overhead, and reduces bandwidth consumption and message exchanged as compared to SMSSec and PK-SIM protocols.

EasySMS is completely based on symmetric key cryptography. The efficiency of a block cipher algorithm depends upon the key size and block size. Since, with a larger block size we can encrypt large chunk of data in one cycle of the algorithm, thus, it speeds up the execution of algorithm. However, a larger key results in a slower algorithm, because in general, all bits of key are involved in an execution cycle of the algorithm. A large number of rounds make the algorithm slower but, are supposed to provide good security.

## SMS OPERATION

Global System for Mobile Communications (GSM) [3] is one of the popular mobile phone systems in the today environment. GSM classified into three types, mobile station (MS), base station (BS), network subsystem. The mobile station (MS) is a combination of mobile equipment and a Subscriber Identity Module (SIM) card. The mobile equipment personally identifies the International Mobile Equipment Identity (IMEI). The SIM card stores the high sensitive information such as the International Mobile Subscriber Identity (IMSI), Key (a secret key for authentication), and other user information. All this information may be protected by personal identity number (PIN). The Base Station Subsystem contains two major parts are Base Transceiver Station (BTS) and the Base Station Controller (BSC). The Base Transceiver Station manages the radio transceivers that define a cell and handles the Radio-link protocols with the Mobile Station. The Base Station Controller managing the radio resources for one or more BTS. The major component of the Network Subsystem is the Mobile services Switching Center (MSC).

SMS messages can send and receive in both directions, thus when a message is sent from a mobile device to another mobile device, it goes through several procedures before it is delivered. There are two types of pathways [3] for the SMS transmission between different mobile subscribers. They are internal exchange and external exchange. In Internal exchange, both mobile subscribers belong to one Mobile company. External exchange means both subscribers belong to different mobile company. In this case the SMS should go through two SMS Centers (SMSC). The reference [3] focuses on the detailed study of this two path ways.

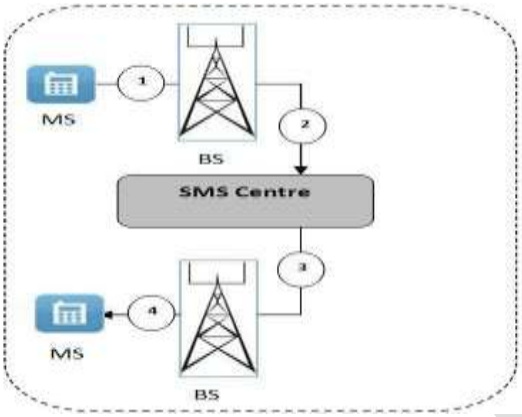


**Fig1**. Internal SMS Transmission

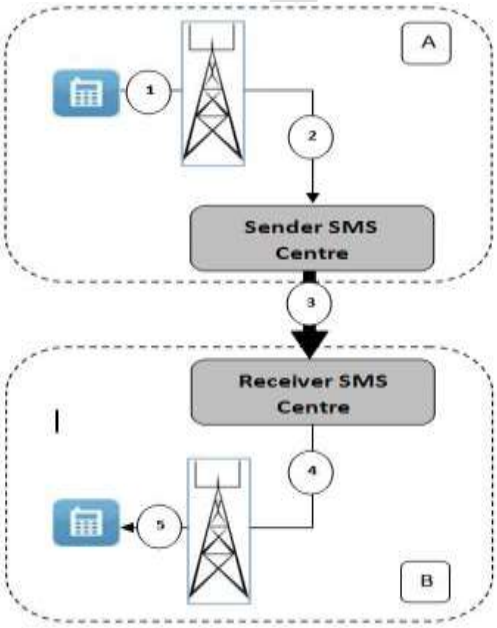


**Fig2**. External SMS Transmission

## CONCLUSION

SMS is the most important service used in different daily life application. The most challenging factor of this SMS is the secure end to end transmission. Here several secure protocols are discussed. They are SSMS and KAPS, SMSSsec, SEESMS, SecuredSMS, EasySMS etc. Here EasySMS is the one and only one protocol completely based on the Symmetric Key Cryptography. It prevents various attacks like SMS disclosure, OTA, man in the middle attack etc. It also reduces the bandwidth consumption. Here AES algorithm is used for encrypting the messages. AES with 128 bit key is more secure than other cryptographic algorithms. So this EasySMS protocol provides greater security.

**REFERENCES:**

[1] Neetesh Saxena, "EasySMS: A Protocol for end to end SecureTransmission of SMS", IEEE Transactions on Information Forensics and Security, Vol. 9, No. 7, July 2014 1157.
[2] Jawahar Thakur, Nagesh Kumar, "DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis", International Journal of Emerging Technology and Advanced Engineering, Volume 1, Issue 2, December 2011.
[3] A. Medani1, A. Gani1, O. Zakaria, A. A. Zaidan and B. B. Zaidan, "Review of mobile short message service security Issues and techniques towards the solution", Journal of Networks, Scientific Research and Essays Vol. 6(6), pp. 1147-1165, 18 March, 2011.
[4] Gary Belvin, "A Secure Text Messaging Protocol", May, 2011.
[5] J. L.C. Lo, J. Bishop, and J. H. P. Eloff, "SMSSec: An end-to-end protocol for secure SMS," Computer Security, vol. 27, nos. 5–6, pp. 154–167, 2008.
[6] A. De Santis, A. Castiglione, G. Cattaneo, M. Cembalo, F. Petagna, and U. F. Petrillo, "An extensible framework for efficient secure SMS," in Proc. Int. Conf. CISIS, 2010, pp. 843–850.
[7] Deepthi Sucheendran, Asst Prof. Arun R, Dr. S.Sasidhar Babu, Prof. P.Jayakumar, "Securedsms: A Protocol for SMS Security," IJCET, Volume 5, Issue 12, December (2014), pp. 37-41.