International Journal of Research in Computer Engineering and Electronics. 1 ISSN 2319-376X
VOl : 2 ISSUE :1

# Secured Local Alert System for College Campus through Short Message Service

Swaminathan.B [1], Srikanth.J [2], Chozharajan.P [3]

**Abstract**— The Short Message Service (SMS) allows user to send text-based messages to and from mobile telephones on a GSM network. There are many organizations like offices, colleges and universities now partner with third-party agents that have many security problems to send messages. Sometimes these services not work due to the limitations of cellular systems providing a false security to the receivers. To increase the security mechanism, encryption and decryption of messages can be done to prevent hackers enters into the system and then they do not change the messages being sent over the communication channel. Whenever sending text messages it is important it should be delivered by all the users to achieve more efficiency. Suppose these messages fail to reach means, sender will recognize the non delivered person of those messages. Then it has to notify those users about the failure of the message and then re-sending the message again.

**Index Terms**— SMS, Campus Alert, Security, GSM, SMSC, AES Algorithm, Mobile phone.

## 1 INTRODUCTION

Short Message Service (SMS) is a text message service that enables users to send short messages to other users on the Global System for Mobile communication (GSM) network. SMS uses a store-and-forward mechanism similar to SMTP mail service. Instead of mail servers, SMS Centers (SMSC) are used to store the SMS messages before they are forwarded to the mobile user's service provider or another SMSC. The network connections between the SMSC and nodes in a GSM network are usually protected by Virtual Private Network (VPN) tunnels [1]. SMS is a relatively simple messaging system provided by the mobile. SMS's are supported by GSM, TDMA and CDMA based mobile phone networks currently in use. SMS messages are transferred between mobile phones via a Short Message Service Center [2].

The SMSC is software that resides in the operators network and manages the processes including queuing the messages, billing payment of the sender and returning receipts to sender. It is also present on most other digital cellular networks and tends to operate in a similar fashion on each network providers. SMS enables two way communications between GSM users. Using this gateways, it is also feasible to interchange messages with other systems such as Internet email, the web etc. SMS has also been incorporated into many other mobile phone network standards, including Global System for Mobile communication (GSM), Code Division Multiple Access (CDMA) etc. Each of these standards implements SMS in slightly different ways and message lengths do vary [3].

The basic principle SMSC (SMS Center) is that encodes the messages to be submitted through the GSM network. The protocols used in SMS Centers are European Telecommunication Standards Institute (ETSI) has approved four SMSC protocols: SMPP (by Logica), CIMD (by Nokia), UCP/EMI (by CMG) and SMS2000 (by SEMA) [4]. These protocols have a little different functionalities and largely different character conversions. There are several SMS gateways able to interact with some or all of the SMS protocols. There is no standard method for service providers to interact with the SMS gateways. Only few of the SMS gateways accept all the SMSC protocols. Services that use SMS system are SMS banking, railways enquiry, stock updates, advertisements and promotions, alert message services, news updates, social networking etc [5].

## 2. EXISTING WORK

In the existing system, it is capable to send thousands of SMS's to the users mobile phones. The existing network is exaggerated by huge amount of network traffic, so it leads to interruption of communication between sender and receiver. Moreover the message send by the user will not reach short time it takes high time to deliver SMS. It uses third party service providers, so attackers will easily change the information's. Sender did not attentive about whether SMS is received or not.

The major drawbacks in the existing works are, security processes are not provided and also there is no alert system whether message received to receiver or not.

- *[1] B.Swaminathan, Associate Professor, Dept. CSE, Rajalakshmi Engineering College, Thandalam, Chennai, India.*
- *[2] J.Srikanth, Assistant Professor, Dept. CSE, Rajalakshmi Engineering College, Thandalam, Chennai, India.*
*[3] P.Chozharajan (Uni.Reg.No.:211611405006),PG student, Dept. CSE, Rajalakshmi Engineering College, Thandalam, Chennai, India.*

In emergency situation due to huge amount of network traffic, it is not possible to deliver messages to user.

Paper [6] suggested that the SMS created by the user will be sent to all but there is no security incident mechanisms provided in this paper. Whenever sending text messages, it is necessary that it should received by all the mobile holders. There is no alert system whether message delivered to user or not. It uses third party service provider's network, so attackers will easily change the message contents. In this paper [7], they estimate the security violations of the message interface on the availability of the cellular phone network providers. There is attacks targeting the entire network are also possible with resources available at most of the organizations. This analysis shows the investigation of the structure of cellular service provider's network. Then illustrate network performance and provides a number of techniques designed at effectively targeting attacks on these devices.

The connection among telecommunications networks and the Web creates lot of problems to deliver SMS. Due the huge amount of network traffic it is feasible to takes place denial of service to customers in major metropolitan areas. Therefore, messages are not delivered within the time it takes more time to deliver messages and also sender did not aware about whether SMS is delivered or not [8].

In this, the sending of messages from mobiles device through the internet creates many security problems to deliver SMS. It is probable to take places Dos attack through SMS service that degrades the message delivery process carefully. SMS are not delivered within the time it takes more time to deliver message [9].

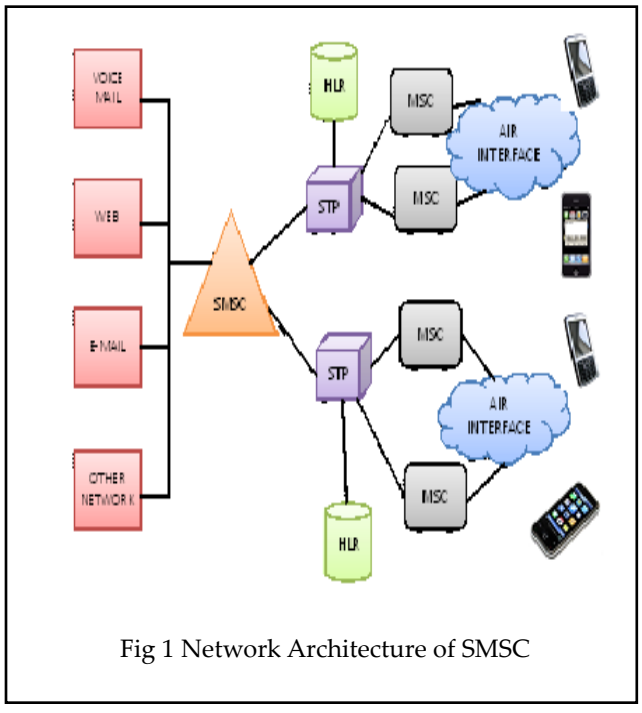


Fig 1 Network Architecture of SMSC

Bandwidth flooding attack causes huge traffic to receiver mobile phone with the mechanism of congestion in the communicating mobile devices and re-orders the message exchange process. Active Internet Traffic Filtering (AITF) protection mechanism prevents against such kind of attacks. It creates the process whnever trakkic occurs it stops the communication process [10].

## 3. PROPOSED WORK

### 3.1 SMS Creation and Encryption

The message should be created by college authorities to send all the students. For encryption of the messages Advanced Encryption Standard (AES) algorithm is used. AES is a block cipher with a block length of the 128 bits. AES permits three different key lengths of 128 or 192 and 256 bits. Encryption process consists of 10 rounds of processing for 128-bit keys size or 12 rounds for the 192-bit keys size and then 14 rounds for 256-bit keys size [11].

### 3.2 Message Delivery Process

Figure 1 represents the basic network architecture of SMSC deployment handling many input sources, like voice-mail service (VMS), e-mail, Web messaging, and other external short network services. Communication with the wireless network elements such as the home location register (HLR) and mobile switching center (MSC) is achieved through the signal exchange point (STP). SMS provides a method for exchange SMS to and from mobile phone. This service makes use of a Short Message Service Center (SMSC), which is used to store and forward system SMS. The wireless service providers provide the mechanisms required to find the receiver station(s) and transports short messages between the SMSCs and wireless stations.

Mobile Switching Center (MSC) not knows more information about destination mobile location. To identify current location of the device, the MSC send queries to the Visitor Location Register (VLR), which temporarily stores information about clients. Sometimes this information is not known, MSC will begin process for locating the mobile device. MSC completes this task by generating and sending paging requests to all of the base stations.

After receiving a paging request from the MSC, a base station finds whether or not the destination device is nearby. It sends information about the current location of the receiver. Then SMSC forwards messages to the appropriate destination re-

ceivers. The SMSC usually rides on the Internet infrastructure for cost reasons and to tap into the huge number of Internet users. By connecting to the Internet, the SMSC has essentially bridged the GSM network with the Internet and introduced the vulnerabilities and threats of the Internet to GSM network.

### 3.3 Gateway

SMS gateway service providers can be classifying as aggregators or SS7 (Signaling System No 7) providers. The aggregator model is based on several agreements with mobile carriers to transfer two-way SMS traffic into and out of the operator's short message service center (SMSC), also called as local termination model. Aggregators lack direct admission into the SS7 protocol, this is the protocol where the SMS's are exchanged. These service providers have no visibility and organize over the message delivery, being not capable to offer delivery guarantees. SMS are delivered to the network providers SMSC, not to subscriber's mobile.

Other type of SMS gateway service provider is based on SS7 connectivity SMS messages, also called as international termination model. The main advantage of this model is the capability to route data directly to the SS7, which gives the provider total control and visibility of the complete path during the SMS routing. Therefore, it is possible to avoid delays and message victims, offering full message delivery guarantees of SMS and optimized routing. This uses frequency-shift keying to exchange message between the terminal and the SMSC gateway. Terminals are DECT-based, but it uses wired handsets and then wired text-only (no voice) devices. A direct-to-mobile gateway is a device which has built-in wireless GSM (Global System For Mobile Communications) connectivity. It permits SMS text messages to be sent and/or acknowledged by email, or from web pages or other Instant messaging software applications by acquiring a Subscriber Identity Module (SIM card).

The Gateway is a pioneering secure bridge to assist communication between applications and carriers around the world via the SMS channel. Gateway offers message encryption, decryption, storage, routing, reporting and other advanced features required to manage Secure SMS such as data wipe, configuration settings and updates. It provides secure communication between two or more mobile devices.Access to Secure Campus Alert is similar to using a standard SMS gateway. Secure messages are submitted from application using a set of Application Program Intrefaces. Messages received from colleges are identified on the handset by code number, any name or keyword that is given in the mobile phone user in the secure phone book. Gateway offers worldwide coverage independent of carrier's SMS coverage area.

### 3.4 Status Notification

In this, message delivered to receiver mobile means it sends back to sender that messages are delivered. Suppose if the destination mobile out off range means it stores the messages in the SMSC for later delivery that the SMS. If the mobile user comes to Switched on it delivers SMS and deletes SMS from the SMSC.

## 4 Result And Discussions

The output of the Campus Alert SMS delivery system is shown in Fig 2. The front end tool is C# & .Net framework is used to create the Campus alert system.

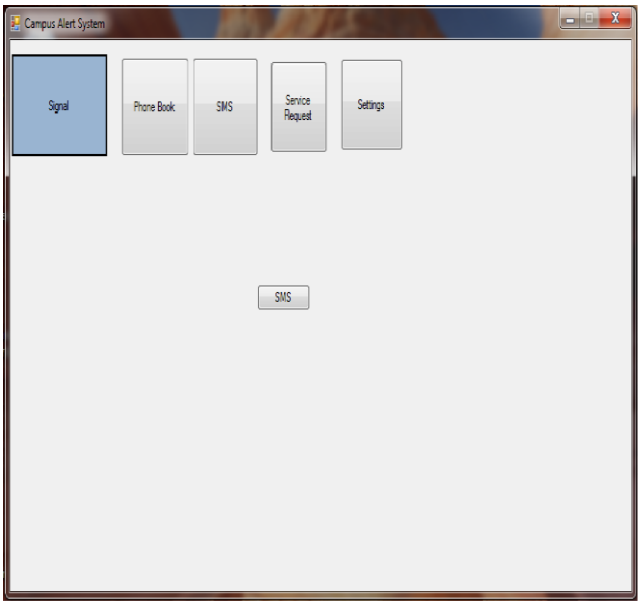


Fig 2.Campus Alert Output

In this, Network Settings form created to connect to the network provider. Then the next form is Phonebook form used to storing all the user contact numbers. SMS form is designed to create SMS and encryption of the SMS and then sending messages to all the people.

## 5 Conclusion And Fututre Work

Cellular networks are increasingly becoming the most important communication method to pass information between people. Text messaging is a trustworthy method for distributing SMS. But, security mechanism simply does not work some time. In paper encryption and decryption of messages can be done prior to sending to all the people to prevent attackers did

not change the information of the message. If these SMS fail to deliver, sender identifies the non recipients and then re-sending the message again.
In future, this system is implemented for Android Technology and then separate mobile application is creating for this work to deliver SMS more efficiently.

## REFERENCES

[1] "Technical Realization of the Short Message Service (SMS)," Technical Report 3GPP TS 03.40 v7.5.0, 3rd Generation Partnership Project, 2002.

[2] Saurabh Samanta, Radhesh Mohandas, Alwyn R. Pais "SECURE SHORT MESSAGE PEER-TO-PEER PROTOCOL" International Journal of Electronic Commerce Studies Vol.3, No.1 , pp.45-60, 2012

[3] K. Argyraki and D.R. Cheriton, "Scalable Network-Layer Defenseagainst Internet Bandwidth-Flooding Attacks," ACM/IEEE Trans.Networking, vol. 17, no. 4, pp. 1284-1297, Aug. 2009.

[4] Xiaowei Yang, David Wetherall and Thomas Anderson "TVA: A DoS-Limiting Network Architecture" IEEE/ACM Transactions on Networking, VOL. 16, NO. 6, DECEMBER 2008.

[5] P. Traynor, M. Lin, M. Ongtang, V. Rao, T. Jaeger, T. La Porta, and P. McDaniel, "On Cellular Botnets: Measuring the Impact of Malicious Devices on a Cellular Network Core" Proc. ACM Conf. Computer and Comm. Security (CCS), 2009.

[6] P. Traynor, "Characterizing the Security Implications of Third-Party Emergency alert systems over Cellular Text Messaging Services," Proc. Second IEEE Int'l Conf. Security and Privacy in Comm. Networks(SecureComm),2012.

[7] P. Traynor, W. Enck, P. McDaniel, and T. La Porta, "Exploitin Open Functionality in SMS-Capable Cellular Networks," J. Computer Security, vol. 16, no. 6, pp. 713-742, 2008.

[8] P. Traynor, P. McDaniel, and T. La Porta, "On Attack Causality in Internet-Connected Cellular Networks," Proc. USENIX Security Symp., 2007.

[9] P.Traynor, W. Enck, P. McDaniel, and T. La Porta, "Mitigating Attacks on Open Functionality in SMS-Capable Cellular Networks," IEEE/ACM Trans. Networking, vol. 17, no. 1, pp. 40-53, Feb. 2009.

[10] K. Argyraki and D.R. Cheriton, "Scalable Network-Layer Defenseagainst Internet Bandwidth-Flooding Attacks," ACM/IEEE Trans.Networking, vol. 17, no. 4, pp. 1284-1297, Aug. 2009.

[11] Rohan Rayarikar, Sanket Upadhyay, Priyanka Pimpale " SMS Encryption using AES Algorithm on Android," International Journal of Computer Applications (0975 – 8887) Volume 50– No.19, July 2012