Scientific Research and Essays Vol. 6(6), pp. 1147-1165, 18 March, 2011
Available online at http://www.academicjournals.org/SRE
DOI: 10.5897/SRE11.107
ISSN 1992-2248 ©2011 Academic Journals

Review

Review of mobile short message service security issues and techniques towards the solution

A. Medani[1]*, A. Gani[1], O. Zakaria[2], A. A. Zaidan[3,4] and B. B. Zaidan[3,4]

[1]Faculty of Computer Science and Information Technology, University of Malaya, 50603 Kuala Lumpur, Malaysia.
[2]Faculty of Science and Information Technology, National Defence University of Malaysia, 5700 Kuala Lumpur, Malaysia.
[3]Faculty of Engineering Multimedia University, 63100, Cyber Jaya, Malaysia.
[4]Predictive Intelligence Research Cluster, Sunway University, No 5, Jalan Universiti, Bandar Sunway, 46150 Petaling Jaya, Selangor, Malaysia.

Accepted 23 February, 2011

The short message service (SMS) is one of the highly used and well-tried mobile services with global availability within all GSM networks. The existing SMS is limited to the transmission of secure plain text between different mobile phone subscribers. SMS does not have any built-in procedure to authenticate the text and offer security for the text transmitted as data, because most of the applications for mobile devices are designed and developed without taking security into consideration. This paper details an overview of the current SMS security aspects and concerns during the SMS transmission. It also chronologically presents the existing mechanisms used to protect the SMS with the goal to provide useful advices for further research. In addition, the security and efficiency of these mechanisms are analysed, considering the limitation on the mobile devices and the security requirements. Finally it suggests the SMS security future direction for generating extra research topics.

Key words: Short message service security, short message service cryptography, short message service security analysis, mobile communication, mobile public key infrastructure.

INTRODUCTION

The use of mobile devices has increased rapidly over the years, particularly, during the last decade. These wireless devices were initially started as devices to store personal information. Short message service (SMS) will play an important role in the future business areas, which are popularly known as m-commerce, mobile banking, governmental use, and daily life communication. Furthermore, SMS has become a popular wireless service throughout the world as it facilitates a user to be in touch with any mobile phone subscriber anywhere in the world, instantaneously and without any hassle (Grillo et al., 2008; Zhang et al., 2005).

MOTIVATION

The primary purpose of SMS is to deliver text messages from one mobile device to another. It provides many benefits to our everyday life. However, it is considered safe and secure when sensitive information is transmitted using the typical SMS services?, many possible threads of SMS can arise, hence, it is important to prevent the SMS content from being illegally intercepted/interrupted by illegal sources as well as to ensure the origin of the message from the legitimate sender (Hossain et al., 2008).

One of the important challenges in the mobile communication industry is to ensure the mobile services are properly used and not open to abuse (Al-Fayoumi et al., 2007; Hwu et al., 2006). Additionally, unencrypted SMS content during the transmission allows the mobile operator’s employee to read and modify the SMS content. Unfortunately, the SMS does not have any built-in vetting procedure to authenticate the text or provide security for the data/text transmitted (Hossain et al., 2008). It is obvious that parts of the SMS applications for mobile devices are designed and developed without taking into account the SMS security aspects. Therefore,

*Corresponding author. E-mail: a_madani24@hotmail.com. Tel: +(601) 72013194.

all SMS facilities should incorporate some form of basic security mechanism in terms of confidentiality, integrity, authentication and non-repudiation of the messages before it can deemed suitable for use by the government, commercial and military services (Garza-Saldana and Daz-Pérez, 2008; Hassinen, 2005; Hassinen and Markovski, 2003).

Exchanging normal SMS does not guarantee the confidentiality as it is not totally secure and reliable since the messages are transferred in a text-mode (readable) through an insecure transmitting channel. Due to the special nature of the mobile communications and the lack of security of the transmitting channel, achieving the security issues can be considered as a high priority issue. Beside improving and enhancing the secret of the SMS content without being unlawfully tempered (Wu and Tan 2009; Zhang et al., 2005; Zhao et al., 2008). In simple term, the unprotected communication channels and the increasing popularity of the wireless devices pose serious security vulnerabilities. Thus, it is important that both the mobile applications developer and the mobile service providers (mobile operator) ensure the correct identities of the communicating parties, while at the same time, ensure SMS content confidentiality and integrity during data transmission period in order to avoid these threats (Tiejun et al., 2008). The aim of this review paper is to provide useful advices for further research in the SMS security topic, which is considered one of the important topics since the SMS is part of our daily life, beside, many research centers around the world trying to improve it by using different techniques and security framework.

The main objectives of this paper are:

i) To explain SMS transmission steps and indicates the main components of GSM which are participating during the SMS transmission.
ii) To review all the current SMS security aspects and concerns during the SMS transmission.
iii) To present chronologically the existing mechanisms used to protect the SMS transmission.
iv) To analyze the security mechanism base on the mobile security requirements and mobile performance capability.
v) To suggests future direction for generating extra research topics in improving the SMS security.

Paper layout

This paper presents an overview of the current SMS security, presented in terms of the main challenges and techniques. These techniques are described historically and in a particular order. Outlines of the SMS main structure of SMS transmission operations that SMS should be followed between the communications partners, describing the SMS security concerns in every single point of the transmission framework as background needed in order to present the solutions, analysing all the SMS security techniques that can be used to protect SMS content, analysing the security requirements against mobile performance, future key challenges and offering our view in the SMS security future direction of SMS security and finally summarises the state of the SMS security are all given in the study.

SMS operations

Before talking about the security concerns during the SMS transmission, it is better to give details of the steps during the SMS content exchange. It looks easy conceptually to understand the normal mobile to mobile SMS transmission in general, but it is highly complex to implement the protocols and the mechanisms which precede with the transmission procedures. The SMS messages can go through 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. The next figure in this study presents a short overview of the message pathway. There are two types of pathways for the SMS transmission between different mobile subscribers.

Case 1

Internal exchange

When two mobiles subscribers intend to exchange the SMS and both subscribers belong to one mobile operator company.

Case 2

External exchange

When two mobile subscribers intend to exchange the SMS and both belong to different mobile operators (Lockefeer et al., 2010). Figure 1 illustrates the mobile network infrastructure and the sequences steps when exchanging the SMS content between two mobile subscribers (Case 1).

All the details related to Figure 1 will be tabulated in Table 1. Figure 2 illustrate the steps as a sequence flow of exchanging SMS between different mobile operator companies (Case 2). In this case the SMS should go through two SMS centres (SMSC). All the details related to the Figure 2 is fully tabulated in Table 2. It is clear that, there are two main layers participting in the sending and receiving of the SMS between different mobile subscribers. Normally, the SMS is sent (composes) through the application layer and then it goes through the transport layer (transmission medium) before arriving at the mobile destination through the application layer again (inbox). Thus, the security is mainly concerned with the

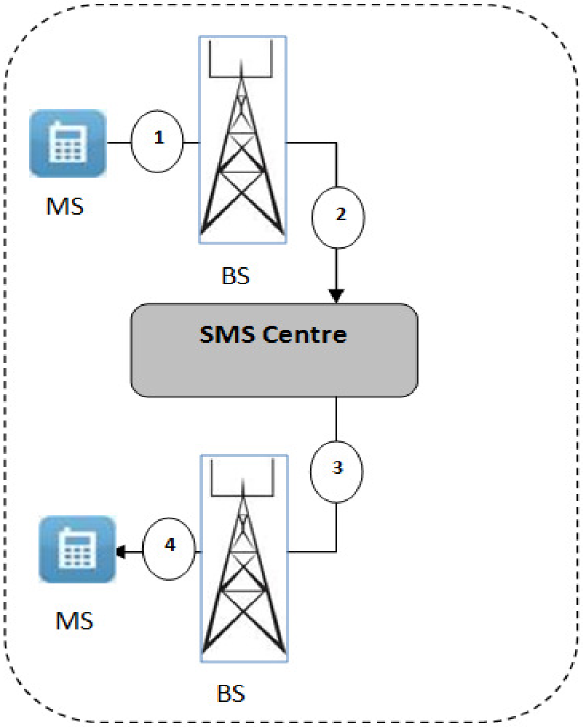

Figure 1. Internal SMS transmssion steps.

application and transport layers during the SMS transmission. Figure 3 presents a general overview of the SMS transmission layers (application and trasport layers).

SMS security concern

It is a well-known that the GSM Network cannot provide several important security services simultaneously (Kolsi, 2004). Thus, it is common for this feature to be exposed to some security risks during SMS contents transmission. Many encryptions standards used by mobile's operator to ensure the integrity and confidentially of transmitted content. Therefore, security in cellular telecommunication framework is important to secure safe communication and signaling data from interception as well as to prevent the cellular telephone scheme from various electronic interferences and threats (Islam and Ajmal, 2009; Margrave, 2000; Meyer and Wetzel, 2004a, b). Furthermore, as the integrity and confidentiality can be achieve by encrypting the medium, and the authenticity can be executed by installing a backend server for the authentication purpose to verify the authenticity of the user who is in ownership of the mobile device (Croft and Olivier, 2005; Guthery et al., 2000; Lo et al., 2008; Steiner et al., 1988), the authentication server is connected to the SMS centre (SMSC) as all the messages go through the SMS centers. Figure 4 illustrates the steps of authenticating the mobile devices (sender and receiver). All the details related to the Figure 4 are fully tabulated in Table 3. Although the GSM network applies different security techniques, openness of the wireless transmission makes the communicating parties vulnerable to information interruption/interception by hateful attackers (Margrave, 2000; Meyer and Wetzel, 2004a, b; Toorani and Beheshti, 2008).

The medium of SMS content transmission is not completely secure and vulnerable to malicious attackers who could use it to monitor and send wrong information between the communicating parties, thus, the GSM network suffers from various security weaknesses. This allows an attacker with the right tools and mechanisms to modify/read on the information that is being sent (Hassinen and Markovski, 2003; Hossain et al., 2008; Pesonen, 1999; Quirke, 2004). Furthermore, it is well-known that, it is possible to a man-in-the-middle (MITM) attack in GSM during authentication which allows an attacker to choose a mobile victim device or station authenticates itself to a fake base station which in turn forwards the authentication traffic to the real network, thus impersonating the victim mobile station to a real network and vice versa (Asokan et al., 2005). It is obvious that there are several security concerns and risks during the SMS broadcast or transmission operations. It can be defined that there are two types of network concerns which can happen on the transport layer (transmission medium) and the application concern (composing and saving the SMS content).

i) First section reviews the SMS security concern during network infrastructural components.
ii) Second section reviews the SMS security concerns during the application layer (sending and receiving).

Transport layer network medium

The SMS content transmits through various protocols and interfaces. Despite the various security measures being taken. GSM with the worldwide users suffer from several security limitations (Siddique et al., 2006) and, therefore, it can be considered that there is no security provided for the SMS end-to-end transmission, that means there are no evidence that SMS transmission circle (from source to destination) can be secure (Lockefeer et al., 2010). Table 4 analyses the important SMS security concern on different points (during GSM components) which can affect the security of the SMS message during the transport layer, as well as (the third column of the Table 4) presenting the concern descriptions for specific positions in Figures 1 to 4.

Application layer

Although there are some application layer protocols that simultaneously provide the confidentiality, integrity,

Table 1. Description of internal excahnge process.

Steps	Description
1	Mobile devices composes and sends the SMS to the nearest base station (BS) using on- the-air (OTA) interface, which is the standard for the transmission and reception of application-related information in wireless communications devices (Koien and Haslestad, 2003; Pitoura et al., 1998).
2	The BS forwards the SMS content to the mobile's home short message service centre (SMSC), over SS7 (Glitho, 1997).
3	After completing its internal processing, and interrogation of the destination location, the SMSC sends the message over SS7 to the nearest BS around the final mobile destination (Glitho, 1997; Wilson, 1992).
4	Through the OTA protocol again the BS station forwards the SMS to the final Mobile reception and then the Delivery acknowledgements will follow the reverse path.

Note: all the steps mentioned in Figure 1 are in the form of numbers.

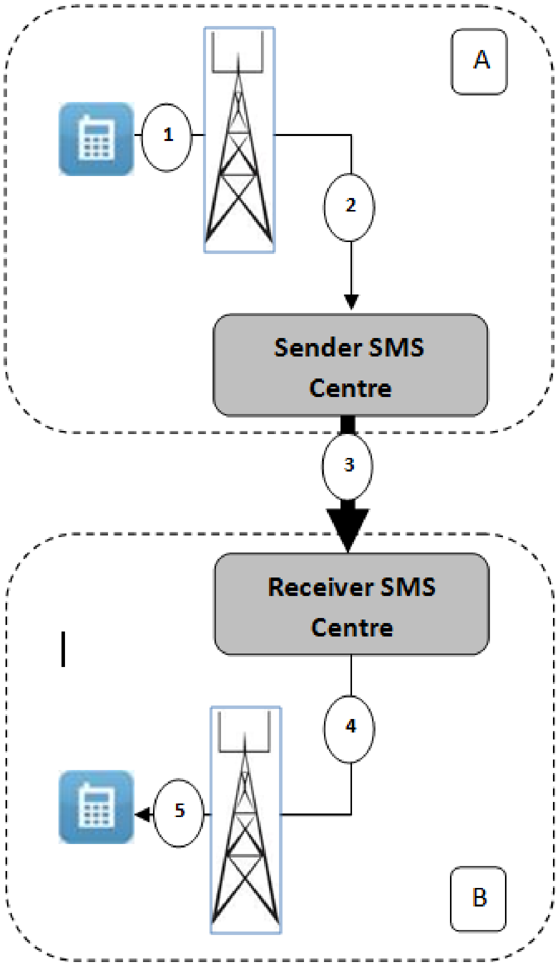

Figure 2. External SMS transmssion steps.

authentication, and non-repudiation processes, however, several possible attacks to this main security measure can arise (Toorani et al., 2008). In particular, there are concerns about the built-in nature of the SMS service that seems not in a position to discourage companies to consider the SMS as an effective means of exchanging the business records (Grillo et al., 2008). Table 5 reviews the important concern's types, that can affect the SMS messages during the application layer, and description is provided in second column for the concerned location by mentioning the specific location in Figures 1 to 4.

SMS security techniques

Unprotected communication channels pose serious security vulnerabilities. Thus, it is importantly pertinent that both the mobile applications and the mobile operators must apply some reliable protective techniques to avoid these assailable vulnerabilities. This used to protect the mobile subscribers from the undesirable communication attacks during the SMS transmission. It can be provided in the network base (transport layer) or in the application base (mobile application) (Tiejun et al., 2008). This section reviews and describes the security mechanisms used for protecting the SMS transmission besides analyzing this mechanisms based on the security requirements comparing with the mobile performance capability. Beside, describes on how this mechanism can be applied to avoid the security concerns. There are two types of techniques that can be applied in different ways as mentioned (application layer and network layer). This paper focuses on the application layer techniques, which are considered as the current SMS research issues since it is under the researchers' control and development.

Applications techniques

Application base means design and development of application in the mobile devices to secure the SMS content transmission. It considers one of the ways to protect the SMS privacy by encrypting the message body at the initial transmitter (sender) and then decrypting the

Table 2. Description of external excahnge process.

Step	Description
1	Similar to step 1 in Table 1.
2	Similar to step 2 in Table 1.
3	The sender's SMSC reformats the SMS message to the short Message Peer to Peer Protocol (SMPP) format and then sends it to the SMS gateway using TCP/IP over the public or private internet which links to the mobile recipient's SMSC. The SMPP is the telecommunication's industry protocol for exchanging SMS messages between SMS centres (Aziz, 2006).
4	Similar to step 3 in Table 1.
5	Similar to step 4 in Table 1.

All the steps mentioned in Figure 2 are in the form of numbers.

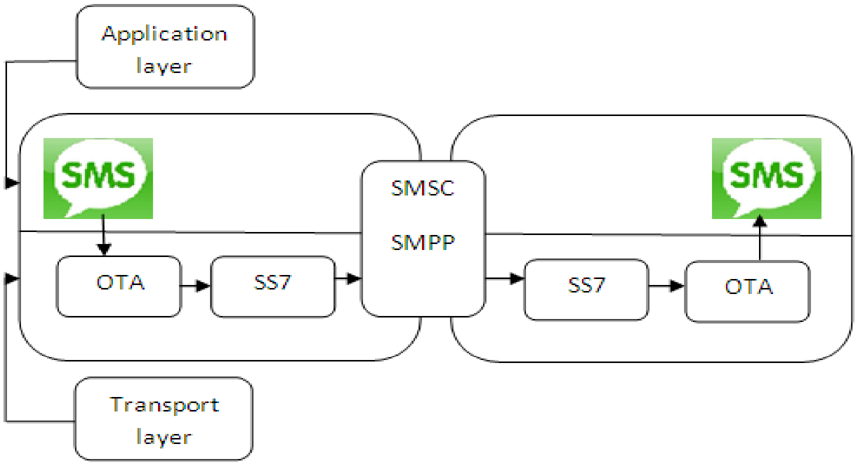

Figure 3. Transmission layers.

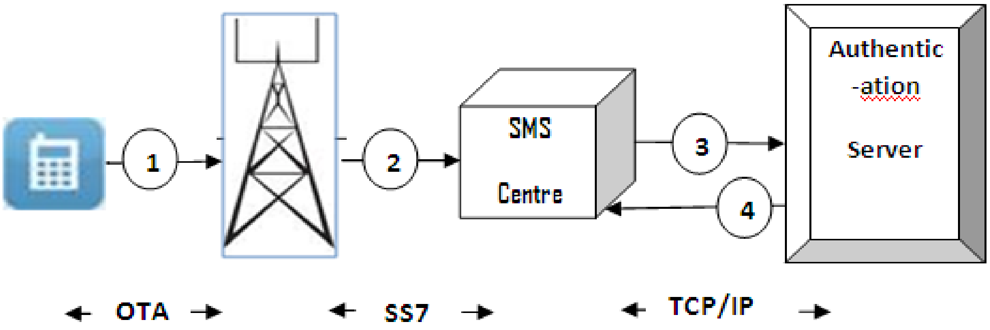

Figure 4. Mobile device Authentication process.

message at the receiving device (receiver). It called an end-to-end secure transmission. Of course, the needs for developing an end-to-end security mechanisms (including integrity, confidentiality, authentication, and non-repudiation) in the SMS services can arise due to the need of protecting the communication environment (Croft and Olivier, 2005; Zhao et al., 2008). It gives the opportunity for the developers to design and develop the security mechanisms in the mobile devices which it can relieve the mobile network provider from the responsibility

Table 3. Mobile devices authenticating steps.

Step	Description
1	Mobile device sends the SMS message to the BS via the OTA interface.
2	The mobile switching centre, MSC, routes the SMS between the BSs until the SMS reaches the SMS centre, SMSC, via the SS7 channels.
3	The SMSC forwards the SMS to the authentication server through the TCP/IP connection for verifying the SMS's sender.
4	The authentication server sends an acknowledgment back to the SMSC which then enquires the home location registration (HLR) to determine the mobile target location among the mobile network.

Note: all the steps mentioned in figure 4 are indicated in numbers.

of protecting the information during the transmission process (De Paula et al., 2005). In simple term, developing a security application in the SMS market is a critical aspect of the software development from the software engineering view, since (Nah et al., 2005) proved that the value of the mobile applications begins to assume serious inter-related highly confidential matters and that as a result there are predominantly urgent needs to protect the electronic transmission of data. Furthermore as application techniques are independent from the mobile operator sphere of activity, it can also reduce the security overhead.

Safe mobile application structure or framework should provide different safety features and requirements. Figure 5 shows the main application or framework requirements (Lam et al., 2003). As is already known, the SMS provides a connectionless transfer of messages. A single message consists of 140 bytes and there is a unique SMS format or structure for the GSM network. Figure 6 illustrates the SMS header and the payload - SMS content- where the security mechanisms should be applied for the text inside the payload which contains the sensitive information. In the modern technology, cryptography provides powerful tools for protecting sensitive communications over a public network, but it imposes an overhead in terms of additional computation (Grillo et al., 2008). There are three types of crypto-graphic schemes, namely: i) secret key (or symmetric) cryptography, ii) public-key (or asymmetric) cryptography; and, iii) hash functions. Figure 7 demonstrates the end-to-end secure SMS transmission during the communication medium. It is clear that when the SMS message is locked (encrypt) at the sender side, only the receiver can unlock (decrypt) the SMS content. Thus, the message will be encrypted during all the transmission media.

Security techniques can be applied to the payload field in the SMS headers (Figure 6). Therefore, there are special packages that can be used to get access to the SMS header's field. WMA is used as an optional package for the J2ME that enables an application developer to a system that can send and receive an SMS (Messaging, 2002). Figure 8 illustrates the components within the WMA package. It is used for building the SMS applications. This package is now widely used and it is the main package used during the SMS transmission. The aforementioned components have different tasks as by combining them they can send and receive the SMS messages. Unfortunately, none of these components include any encryption mechanism to protect the confidentiality content of a SMS message during its transmission between the sender and the receiver and it is for this particular aspect that the security developers get a good opportunity to apply their proposed techniques for protecting the SMS transmission using the cryptography techniques and algorithms.

Several cryptography techniques used to overcome the SMS security problems and fulfill the security requirements. Although cryptography provides powerful tools for protecting sensitive communications over a public network, it imposes an overhead in terms of additional computational processes: this limitation can threaten the usability of the embedded devices (for example smart phones) with severe constraints on the computational power, battery life and user latency which impose limits on the amount of encryption operations that can be performed without a severe degradation of the device. Therefore, the right choice of the suitable mechanisms is highly and crucially important (Grillo et al., 2008).

Symmetric cryptography

The first technique used for protecting the SMS application is the type of encryption which provides an end-to-end security mechanism and is considered a high-quality solution for the SMS protection since the mobile device has limited resources, such as, insufficient memory, inadequate processing power and limited power supply (Lu et al., 2002; Nicholson et al., 2006). It represents a shared secret key between two or more communication parties that can be used to protect the SMS content. However, safe key distribution is quite

Table 4. SMS transmission concenrs.

Concern location	Figure location	Concern description
OTA interface	Figure 1 step 1 and 4.	Although the GSM standard is considered to be secure, beside it has a strong subscriber authentication and over the air (OTA) transmission encryption, but it depends on the countries policies and approval. Therefore, applying the new security mechanism can be difficult, which can generate SMS security risks as the (Croft and Olivier, 2005; Lo et al., 2008; Schneier, 2005).
OTA interface	Figure 1 step 1 and 4.	Choice of the type of encryption in a network should be specific. A5/1 and A5/2 are mostly used for the security of the OTA interface but they are not totally safe because they are based on the stream cipher and several serious weaknesses and limitations in the cipher have been recognized (Biryukov et al., 2001; Ekdahl et al., 2001; Lo et al., 2008).
SS7 channel	Figure 2 step 2. Figure 3 step 3.	All call setups, roaming, teardown messages, and database queries controlled by SS7, thus, It becomes the attackers' most important target. It is built for supporting the transportation and the SMS transmission through the core Network. Although the SS7 channel is already protected, it is still suffer from the lack of permissions for develop new mechanisms, because it considered under the SMS administration, management and control. Beside the SMS content can be read by the mobile operator workers during SS7 duration which is on the routing path between the message sender and the SMSC (Bais et al., 2006; Biryukov et al., 2001; Kawamoto and Nakamura, 2002; Lo et al., 2008; Moore et al., 2002; Sengar et al., 2005).
SMS center SMSC	Figure 2 step 3.	SMS center must provide the secure routing and protect SMS content storage with additional security system features. Always SMSCs are protected by a white list such as database or table, This list contains of a list of the IP or MAC addresses of machines from which a server will accept the connections whilst at the same it is supposed to deny all other unrelated connections. However, the SMSCs do not have all the requisite security features as will accept connections from any machine on the internet which could have been unlawfully added in the list by the attackers (Asvial et al., 2004; Le Bodic, 2005).
BSS attackers	Figure 1 step 1 and 4.	Although the GSM security mechanisms achieved successful result for avoiding some SMS security attacks, still there are several weaknesses found when it comes to the sensitive SMS applications. There are many GSM interception protocols located in a (possibly) closed area that listen to the information exchanged between the base stations (BSs) and the mobile stations (MSs) (Boman et al., 2002; Gonzalez-Castano et al., 2002; Lockefeer, et al., 2010)
Authentication server (AS)	Figure 4 step 3 and 4.	The connection between the SMSC and the authentication server is through the TCP/IP connection. It is not so easy to protect the transmission process as any intermediaries can be the potential attackers. The mobile operators is not responsible to protect this transmission process because it is considered to be outside its jurisdictional architectures (Lo et al., 2008) .

difficult (Abomhara et al., 2010). Furthermore, symmetric cryptography algorithms cannot provide authentication, non-repudiation and the message originality. Figure 9 illustrates that both the sender and receiver use the same key for both the encryption and the decryption operation. Dankers et al. (2002) stated that secret key techniques were based on the fact of sender and recipient shared a secret, which was used for various SMS cryptographic operations. It must be exchanged in a separate communication way whereby both of the communication parties should agree before establishing their SMS transmission.

A mobile operator can be used for exchanging the secret key by installing that key inside the SIM card. However, this type of SMS application is considered independent from the mobile infrastructure and the SIM card can be easily stolen and the secret key can be known by other illegitimate parties, thus, these techniques suffer from disparity of the key agreement as mentioned. However, (Ratshinanga et al., 2004) had

Table 5. SMS application security concenrs.

Concern type	Figure location	Concern description
Unencrypted storage	Figure 1 Mobile device	Network attacker can access the data stored inside the mobile SMS inbox. Although the communication way may be encrypted, still there are some risks. When the SMS reaches the final destination target, the decryption process of the content will clear the passage for the recipient reader. Therefore, encrypting the communication way is not enough to provide a full end-to–end SMS protection. It should, however, provide some additional locking techniques to ensure that the SMS stored inside the mobile device is safe and secure (Lo et al., 2008; Lockefeer, et al., 2010).
Identity Impersonation	Figure 1 Mobile device	The attacker can inject the SMS messages into the messaging network with falsified originator IDs. The attacker can copy the SP for a legitimate mobile user. It is possible to send an SMS message from the internet with the correct headers without the recipient being able to detect that it comes from the internet. Lacking of authenticating mechanism provide good ability to identify impersonation (Zhang et al., 2005; Zhao et al., 2008).
Message forgery and tampering	Figure 1 Mobile device	An attacker can also forge or tamper the payload field of an SMS packet, namely: Chikomo et al. (2006), Ratshinanga et al. (2004) and Zhang et al. (2005).
Eavesdropping	Figure 1	An attacker can get access to the messages transmitted through the current mobile networks. Beside, attacker can also intercept the messages from the internet or over the air (OTA) and can easily get interesting information since there are no strong protective measures applied to them (Lo et al., 2008; Zhang et al., 2005).
(MITM)	Figure 1 Mobile sender	The man-in-the-middle (MITM) or an intermediary attacker is one of the problems encountered in the public key cryptography during an exchange of the public key between the communicating parties. The attacker interrupts messages in the middle of its transmission and tries to cheat the two communicating parties by posing as a third party. (Schwiderski-Grosche and Knospe., 2002).

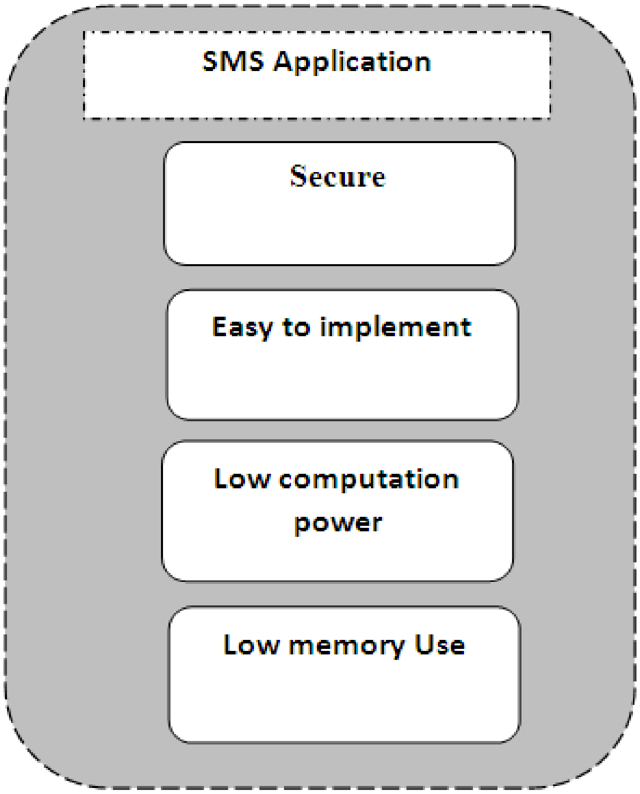

Figure 5. Mobile application requirments.

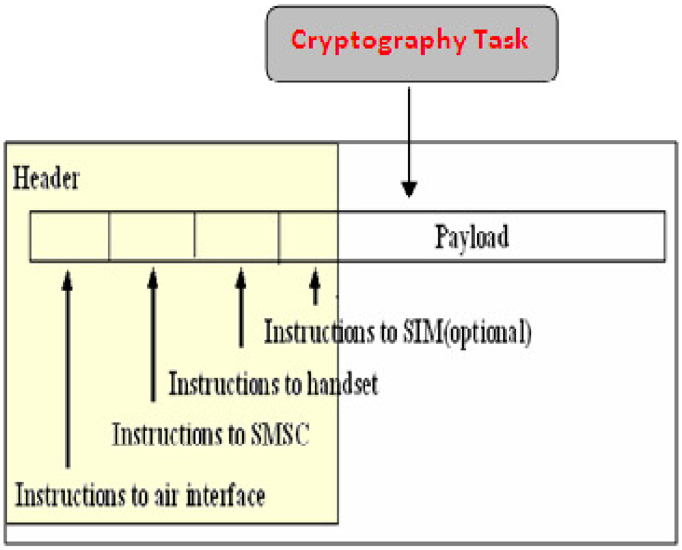

Figure 6. SMS framework.

presented a protocol to ensure the confidentiality and integrity of the SMS communication as this protocol was designed due to the lack of security in the WMA. It was based on the symmetric key cryptography or secret key cryptography. Although its success offered a perfect

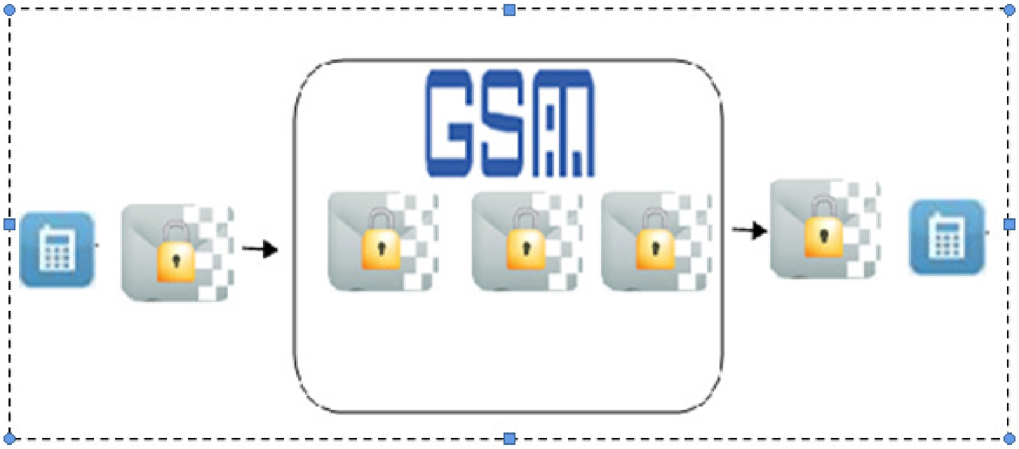

Figure 7. End-to-End secure transmssion.

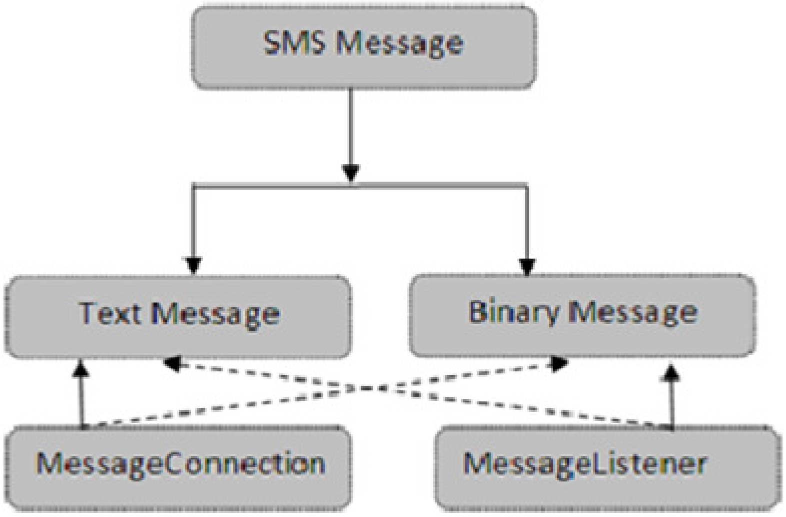

Figure 8. WMA component.

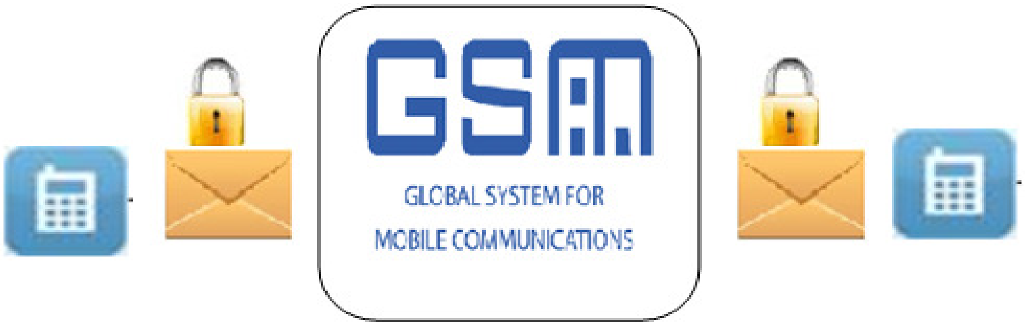

Figure 9. SMS symetrric cryptograhy.

result during the security analysis, it is, however, considered as a heavy process because the secret-key used to encrypt the SMS distribution and agreement is based on the asymmetric key encryption process between the server and the mobile client. Therefore, the shared key cannot exchange openly without the help of

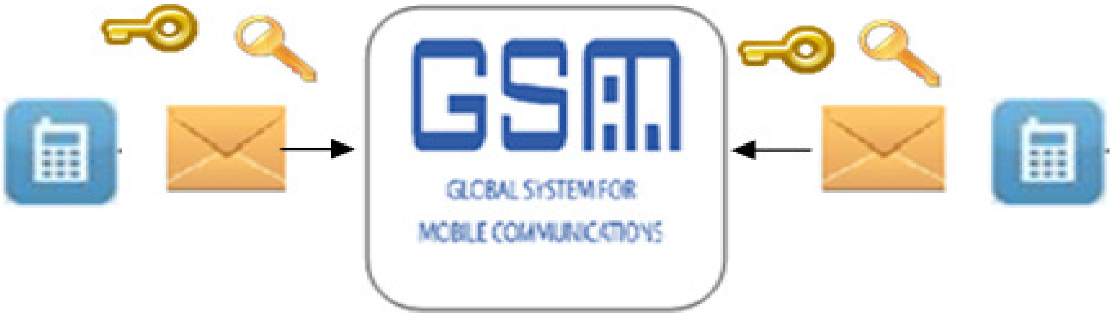

Figure 10. SMS symetrric cryptograhy.

Table 6. Symmetric vs. asymmetric.

Requirements	Symmetric key cryptography	Symmetric key cryptography
Keys for encryption and decryption.	Encryption and decryption using one key.	One key for encryption and a different key for decryption.
Speed of encryption and decryption.	Very fast.	Slower than symmetric key cryptography.
Size of cipher text.	Same as plain text.	Bigger than plain text.
Key distribution.	Big problem.	No problem.
Number of keys for senders with many communication parties.	Approximately to the square of the number of senders.	Same of the numbers of the senders.

other cryptography techniques. A combination of the asymmetric cryptography and symmetric cryptography can achieve more robust functionalities. It is clear that a symmetric key cryptography can be considered a light secure technique for exchanging a secure SMS application. However, the data security depends on the secrecy of the key that is if an attacker can stumble on a way to intercept the key, he/she can easily decode the encrypted SMS content. Thus, the security of the SMS content will be at risk during the key distribution or transmission processes (Lison and Drahanský, 2008).

Asymmetric cryptography

Several weaknesses pertaining to the key distribution in the symmetric key cryptography, thus, a new type of encryption method was developed. Diffie and Hellman (1976) studied the key agreement problem in the symmetric cryptography and resolved the issue by two different keys or a key pair in which one key is called the private or secret key, and the other is the public key. When a sender wants to communicate, the sender has to inform or send his public key to the other communicating parties to perform the encryption process for the plain text. He/she would then use his private key to decrypt the message.

Thus, no one else can decrypt the message except the person who knows the private key. As the public key can be distributed openly, unlike the private key, it must be kept secret. Using the key pair approach, the key distribution problem has been solved. Figure 10 illustrates that both the communicating parties generate two key pairs for the cryptography process. As pointed out, the main reason for using a public key cryptography is that there is some degree of protection during the exchange of the encrypted keys in an unprotected medium. However, it is not as simple as it seems because if the basic public key methods for communication are wrongly used due to inexperienced operation, it can eventually be open to abuse, and thus, susceptible to the man-in-the-middle (MITM) attacks.

The public key can therefore be considered as the first key establishment protocol based on the public key cryptography. However, the protocol does not provide authentication of the communicating parties which means that a man-in-the-middle attack is possible (Forsberg, 2007). This problem can be resolved by using a third trusted party to determine the authenticity of the receiver (Anuar et al., 2008; Gutmann, 2004; Wilson, 2005). The third trusted party method has been used to solve the key exchange authentication problem and it is simply an add-on to the authentication scheme in the exchange process which is called the public key infrastructure (PKI) (Jøsang et al., 2007; Jumaat et al., 2008). Table 6 shows the comparison between the symmetric key cryptography

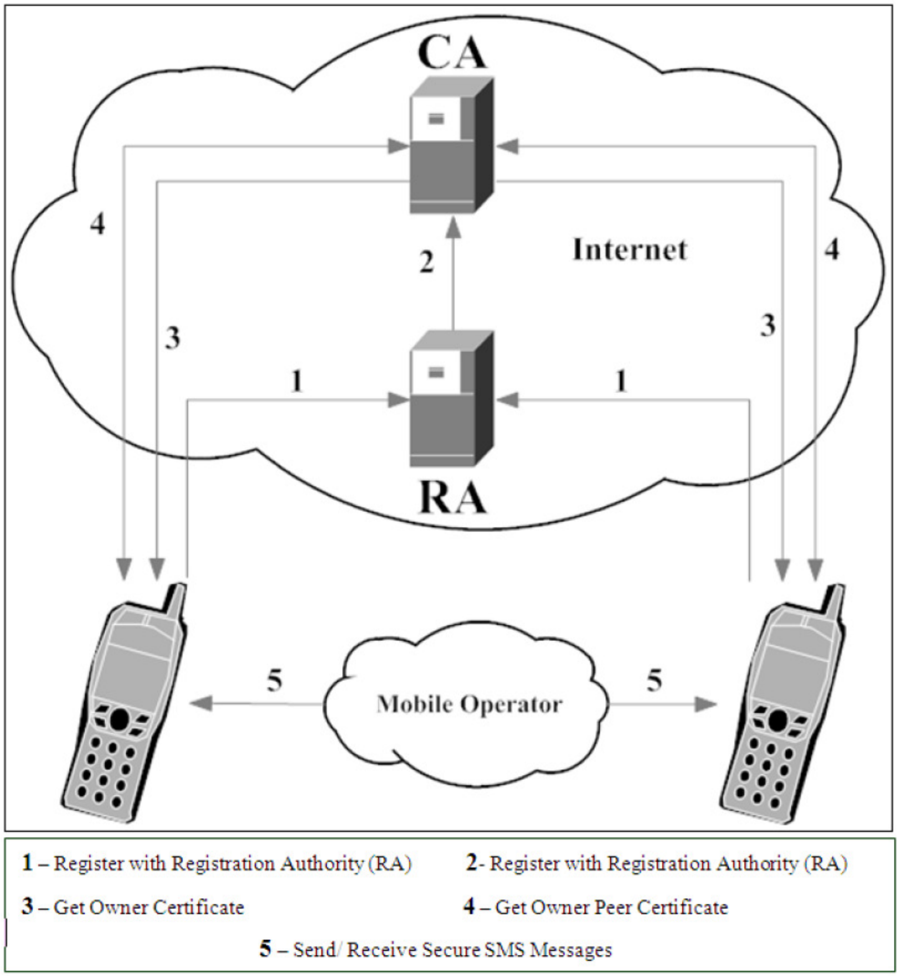
CA
Internet
RA
1
2
3
4
5
Mobile Operator
1 – Register with Registration Authority (RA)
2- Register with Registration Authority (RA)
3 – Get Owner Certificate
4 – Get Owner Peer Certificate
5 – Send/ Receive Secure SMS Messages

Figure 11. A High level view of registration/communication processes.

and the asymmetric key cryptography which basically based on different parameters.

Mobile PKI (M-PKI)

The PKI provides the means to establish trust by binding the public keys and identities together to give a reasonable assurance that the parties can communicate securely with the expected entity (Alanazi et al., 2010). Hence, it can be used to prevent the keys from the MITM attacker during public key distribution, besides; it also provides an end-to-end secure transmission between sending and receiving (Gutmann, 2004; Ratshinanga et al., 2004). Previously to the present mobile PKI issues and techniques should go through these coming sections to provide a general idea about the PKI framework. Figure 11 shows the Mobile PKI basic framework for securing the SMS transmission. Each mobile user registers the public key with a trusted party, along with the information about that entity over a secure medium. Basically, the trusted party is expected to ensure that the public key really does belong to the registrant, and all the associated data are accurate. If the relevant authority has granted the approval, a certificate will be issued and duly signed. As long as that mobile user has securely obtained the authority's public key, the exchanged certificate can be validated by checking on the authority's signature. Therefore, the PKI's main idea is to introduce a trusted third party (agent) to be securely involved with all the communicating parties (Alanizi et al., 2010; Anuar et al., 2008; Hassinen, 2006).

As mentioned earlier, a mobile user has to obtain another party's public key before exchanging the SMS message. Figure 12 shows the process of downloading the peer certificate from the CA to the user mobile application.

i) The mobile device sends an HTTP request to the CA enquiring about the peer certificate.
ii) The CA checks the availability of the requested certificate and signs it before sending it back to the

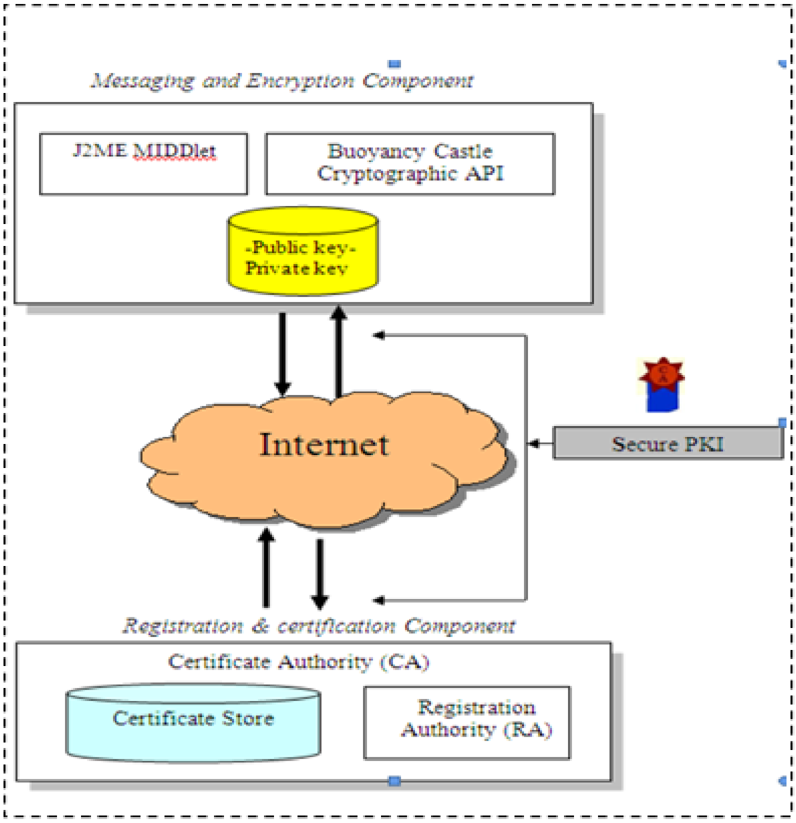
Messaging and Encryption Component
J2ME MIDDlet
Buoyancy Castle Cryptographic API
-Public key-
Private key
Internet
Secure PKI
Registration & certification Component
Certificate Authority (CA)
Certificate Store
Registration Authority (RA)

Figure 12. PKI certificate downloading.

mobile user application as an HTTP response.
iii) The mobile user application verifies the certificate and then extracts the public key to be used to secure the SMS message via an asymmetric key cryptography before saving the certificate in his certificate directory.

After downloading the other parties' certificate, the mobile user can extract the public key and then use it for securing the SMS content by applying the cryptography algorithms. Secrecy of SMS content can be guaranteed as all the security requirements (Anuar et al., 2008; Chanson and Cheung, 2001; Hassinen and Markovski, 2006; Kawamoto and Nakamura, 2002). Figures 13 and 14 illustrate the PKI operations for exchanging the SMS between different communication parties. It is clear that, the communication parties must obtain the digital certificate before applying the cryptography mechanisms for securing the SMS transmission. Implementation of the PKI in a mobile communication is the best solution for the subsequent decade since the demand for a secure mobile SMS becomes increasingly important .This because many applications have been built for the mobile phones, besides, PKI technology is easy to be understood and accepted among the security environment. Table 7 illustrates the PKI solutions for both transmission and application SMS security concerns as mentioned earlier (Tables 4 and 5).

Normally, the PKI is successful in the wire and desktop applications since they have a high power capability for the PKI processes.

Due to the performance limitations of the existing mobile devices capability, it is, thus, considered the PKI technology not suitable for the implementation of securing the SMS transmission (Beller et al., 1993; Chanson and Cheung, 2001; Kuaté et al., 2009; Lee et al., 2007; Lin and Harn, 1995; Zheng, 1996). Many proposed solutions based on the PKI mechanism. Table 8 reviews some of these proposed ideas for implementing the mobile PKI mechanism in the mobile area.

SECURITY AND PERFORMANCE ANALYSIS

Several challenges have to be overcomed for wide deployment in the mobile systems. These challenges include a complexity (difficulty) management of applying PKI mechanisms to the limited devices capability during the deployment process in the large scale heterogeneous mobile system (Seema et al., 2004). As known PKI technology is a kind of asymmetric cryptography techniques, which depends on high intensive computationally of generating keys, and that makes them less suitable

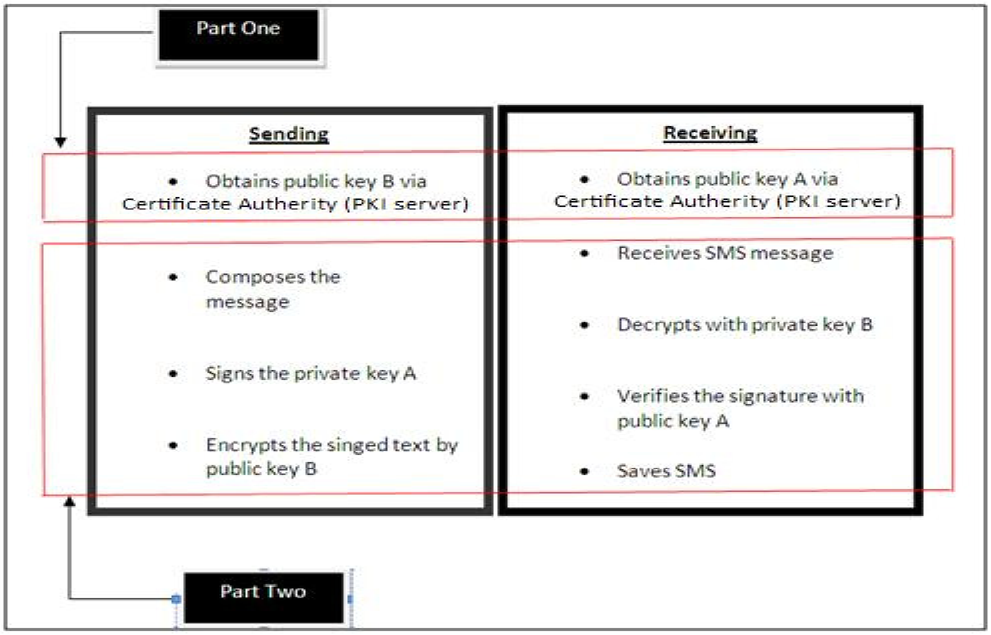
Part One
Sending
Obtains public key B via Certificate Autherity (PKI server)
Composes the message
Signs the private key A
Encrypts the singed text by public key B
Receiving
Obtains public key A via Certificate Autherity (PKI server)
Receives SMS message
Decrypts with private key B
Verifies the signature with public key A
Saves SMS
Part Two

Figure 13. Securing SMS transmission parts.

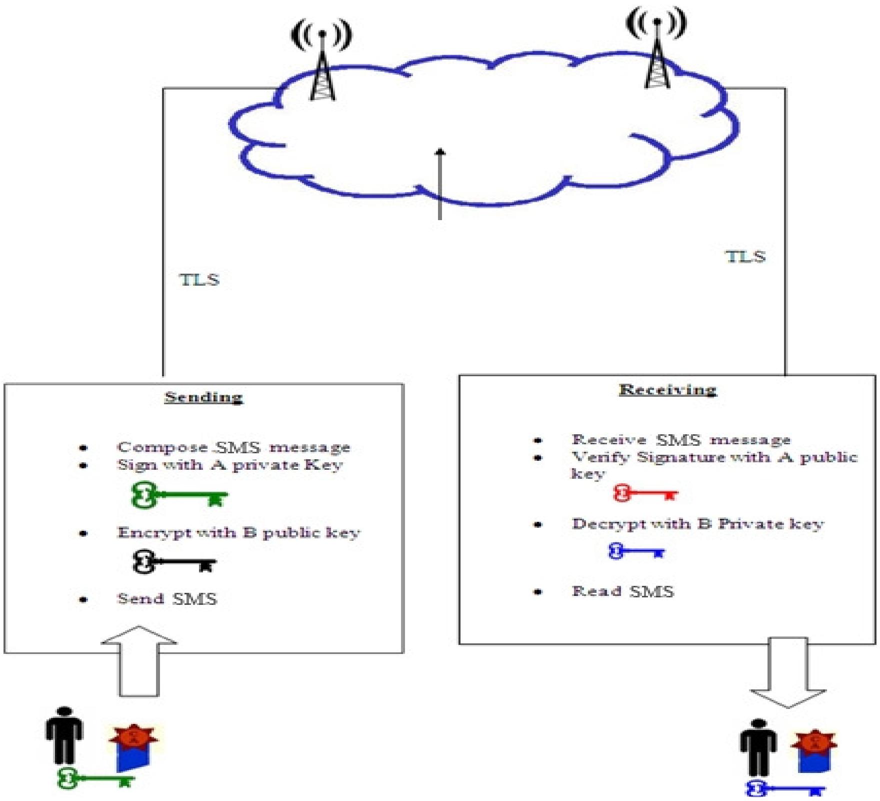

Figure 14. Securing SMS transmission overview.

for devices of limited size and processing power, such as, mobile phones (Dankers et al., 2002). In simple terms, if the mobile user likes to use the PKI mechanisms, these should have the full support for the PKI features which require a high mobile capability (Cai et al., 2005). Currently, all the mobile devices have limited computational

Table 7. Concerns solution by PKI.

Concern	PKI solution
Transport layer concerns	
Concern	**PKI solution**
All the network concerns mentioned in Table 4.	A public key infrastructure (PKI) provides an end-to-end secure transmission for the SMS content. All the intermediary people during the SMS transmission layer cannot read or modify the SMS content as it has been encrypted and duly signed by using the keys of the communicating parties. Therefore, the SMS content will be encrypted during the OTA, SS7 transmission media, and inside the SMSC and the BS. Even the Network employee's operators cannot read or modify the SMS content.
Application layer concerns	
Concern (Table 5)	**PKI solution**
Identity impersonation.	All The SMSs are signed by using the sender's private key which is unknown to the intermediary people including the network operator employees. Furthermore the PKI achieve the necessary of non-repudiation requirement.
Message forgery and tampering.	In the current PKI application, the message is signed by the sender which means attacker cannot know the private key of the sender, thus, attacker cannot tamper with the message neither can generate a correct signature. It is easy to verify the integrity of the message.
Eavesdropping.	An SMS message is encrypted, and only the sender and receiver know the decryption key (distributed via the certificate authority). Any attacker will need a great deal of effort (years) if he wants to decode the encryption, especially, if a strong encryption algorithm is used.
Unencrypted storage.	It can store the SMS inside the mobile inbox as a cipher text and when the user wants to check it, he can decrypt it by using his private key.
(MITM).	Thus, it can solve the authentication issue on both the communicating parties. The PKI utilizes the X.509 certificate for authenticating the communicating parties.

capabilities and a limited power supply since they are depending on batteries, thus, traditional PKI quite unsuitable for these existing devices (Lee et al., 2007). It is obvious that, mobile devices must have the high power capability to implement the PKI functions, beside owns associated capacity. That will provide a huge effort for the authentication process, and can lead to a significant achievement of higher levels of security. However, due of resources in the mobile devices, the PKI implementation consider as a serious drawback for the mobile devices application. Thus, the relationship between the high security requirements and the mobile performance is inversely proportional, as the PKI provides a high security level for protecting the SMS transmission; however, at the same time it decreases the mobile performance. Figure 15 shows the inverse proportional relationship.

Many researchers have been attempting to keep the PKI high security requirments, as well as to improve the mobile ability for applying PKI functions. Many researchers have been attempting to keep the high security level achevied by traditional PKI concept, as well as protecting the mobile devices from PKI complexity. Some reserachers attemped by using combination processes by making use of the symmetric key cryptography in the PKI to reduce the asymmetric cryptography overhead, while others attempted to bypass the part of the PKI operators to the trusted third party, such as, introduction of additional servers or doing away with the GSM mobile operators. Furthermore, some researchers are thinking of improving the cryptography algorithms and use the lowest computational power in the mobile application combined with the PKI techniques. Table 9 shows some alternative methods to reduce the PKI complexity. In short, the mobile communications security solutions that are based on the PKI rely on the mobile phone network operator or service provider as part of the proposed solutions. These server architecture solutions are implementable for governmental or big commercial usage. However, it is un-implementable for individual usage. Generally, the server architecture solutions need additional hardware (that is servers) as a result of which a qualified staff is required to maintain the servers. Moreover, the server architecture mobile security systems user has to get the mobile network operator or the service provider's approval as it still depends on the services of the mobile network operator or the service provider. Furthermore, the overhead cost of communication is increased due to the users' need to access to the servers in many cases, such as, uploading and downloading the cryptographic keys.

Researchers do not expect that the mobile operators will provide the security services to the transmitted data

Table 8. Proposed PKI impelemetation .

Methodology	Weaknesses
Developing a new sever to act as a trusted third party or a middleware between the main server and the mobile device (Chanson and Cheung, 2001).	Difficult to develop for practical application because it depends on using two SIM cards.
Describes a simple symmetric key key cryptography and creates a lightweight based identity AKE protocol (Forsberg, 2007).	It is considered as a light protocol because it is based on binding the sender and/or the receiver identities to the key establishment, as it also needs different communication and operation processes with the third trusted server.
Install fixed Internet line because the exiting fixed line had already been developed and evaluated (Kawamoto and Nakamura, 2002).	Devices can use only the x.509 standard as it is considered as a certificate internet standard and it is heavy for verification in the normal mobile standards.
Based on using identify based cryptography and other techniques to overcome memory limitation (Zhao et al., 2008).	Has to deal with the mobile server provider and suitable only for large commercial organizations.
Using approximated one-time pads (Croft, et al., 2005).	Cannot provide a secure communication between two mobile devices.
Combined with a structure called Latin square, and cryptography processing (Hassinen and Markovski, 2003).	Cannot fulfil all the security requirements, such as, integrity, authentication and non-repudiation.
Encryption generated from the one-time password is entered by the user (Chikomo et al., 2006).	Cannot provide the end-to-end security requirements.
Shared a secret password between all the communicating parties (Hassinen, 2005).	Sender and receiver must previously have agreed on the password and PKI mentioned but not used.
Encrypts the plain text to the cipher text by using the existing mobile network to achieve the confidentiality and then signed before sending it to the receiver (Hossain et al., 2008).	Mobile devices have to be compatible with the GSM mobile service provider's network because it provides an encryption scheme.
Uses 10 functions or steps to achieve a reliably total security (Harb et al., 2008).	The system uses a symmetric key cryptography which has a key distribution problem and does not provide an end-to-end security between the two devices.
Using PKI technology (Jumaat et al., 2008).	The mobile device must download the certificate from the M-PKI directly and then stores the certificate inside the mobile device to perform the verification process which incurs high power consumption besides having a memory limitation problem.
Using PKI for exchanging the secret key (Toorani et al., 2008).	Although the public key is used for generating the secret key to reduce the public key complexity, it still needs the SMSC to apply some security techniques.

through the SMS service for individuals, at least not in the near future. Additionally, in the current mobile systems, some applications based on the PKI have already been installed. They can satisfy the security requirements through the use of the X.509 as the certificate standards. Although the mobile PKI fulfills all the security requirements, it is still unsuccessful to provide heterogeneous PKI standards for other mobile devices (Leung et al., 2003). Furthermore, different certificate standards from different Certificate Authorities (CA), (vendors), are

Relation between the Security and the performance
Mobile efficiency
SMS
Security requirement

Figure 15. Protecting the SMS transmission.

Table 9. Alternative proposed PKI Impelemetation.

Alternative ways	Description
GSM dependency	Using the existing A8 and A5 algorithms with all the parameters required for this encryption to be provided as per GSM specification (Hossain et al., 2008).
	Encryption and signing functions can be done by the crypto co-processor on-board of the PK-SIM card (Chanson and Cheung 2001).
	Choice of short number (unique number for mobile message service) for applying the encryption process (Zhao, et al., 2008).
Third party	A structure called Latin square had been use for applying cryptography processing (Hassinen and Markovski, 2003).
	Using the user authentication server (UAS) to act as a trusted third Party to assist the mobile client during authenticating and exchanging the keys (Chanson and Cheung, 2001).
	Using the current internet line as way for authenticating the communication parties (Kawamoto and Nakamura, 2002).
	One-time password entered by the user seems like using symmetric cryptography (Chikomo et al., 2006).
	Using the secret share techniques for applying the cryptography processes (Harb et al., 2008).
	Using share secret password between the communicating parties as encryption and decryption key (Hassinen, 2005).
	Using the secret key for encrypting the SMS during and between the communication parties. The SMS centre must provide time stamp during the transmission (Toorani et al., 2008).
	Using the symmetric key for encryption of the SMS message but exchange that symmetric key by using the IBC (Forsberg, 2007).
Cryptography Algorithm	Using Elliptic Curve algorithm which requires certain considerations that are not taken into account in the traditional public key infrastructures, such as, the key length generation, signature size, memory usage, and the required processing. It enhances the speed and leads to an efficient use of power, bandwidth and storage which are the basic limitations of resource-constrained devices (Soram, 2009; Toorani et al., 2008).
	Using elliptic curve algorithm for generation, signing and verification functions are considered as using high power consumption for the mobile devices in the PKI implementations. Besides it also provides a higher level of security and increased performance in the mobile devices as compared to the RSA (Tillich and Grossschaedl., 2004; Hankerson et al., 2004; Malhotra et al., 2007).
	Using the NTRU at the similar security level, the key size of the NTRU is less than a quarter of that of the RSA and the speed of the NTRU is much faster than that of RSA; where the key generation is more than 200 times faster, the encryption is 3 times faster and the decryption is about 30 times faster. These are not so widely used because they are new algorithms. Although the operation is much faster, the cipher size is huge as compared to the other algorithms (Xiaoyu et al., 2009).

Note: It can be used to resolve more than one alternative way at the same time to reduce the Mobile PKI limitation.

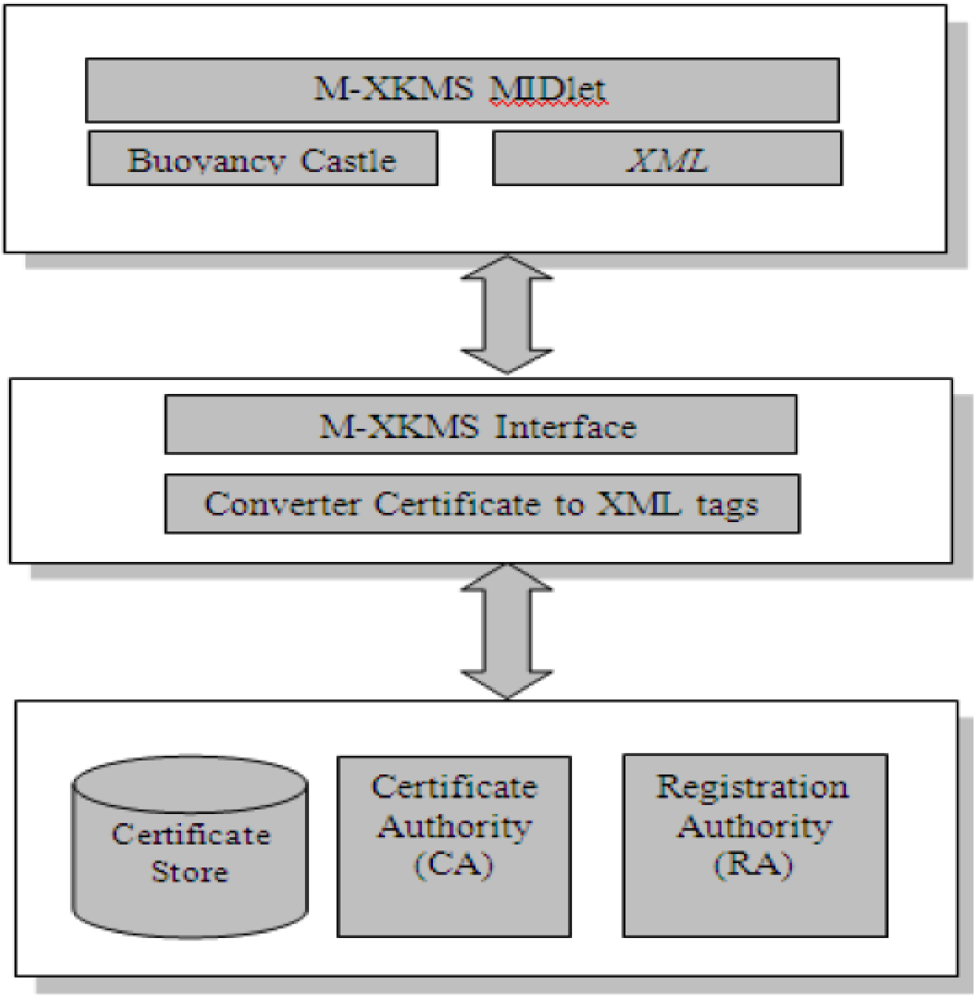
M-XKMS MIDlet
Buoyancy Castle
XML
M-XKMS Interface
Converter Certificate to XML tags
Certificate Store
Certificate Authority (CA)
Registration Authority (RA)

Figure 16. Securing SMS transmission.

considered as overheads for the mobile applications. Therefore, mobile applications have to proceed with different verification processing functions for different PKI certificate standards. In addition, any modification on the server side must also be made applicable to the user's mobile application. For example, changing or upgrading the certificate standards means upgrading of the mobile application process. Thus, the mobile application has to deal with any new certificate standards, as the current PKI cannot maintain integrity between the standards.

LIMITATION

Although this review paper details all security concerns of GSM systems and mobile devices during the SMS transmission, but it does not mention the techniques which could be used to secure GSM architecture. This is because we have already introduced the security techniques in application layer to provide end to end security and protection.

FUTURE DIRECTION

Presently, there are two directions for enhancing the PKI limitations, such as, a high power capability demand as mentioned earlier. Firstly, install the middleware server (with suitable requirement) between the mobile devices and the PKI server. This middleware can shield the mobile devices from the PKI complexities and precedes some on the PKI mobile operation on behalf of the mobile, such as, verifying and storing the mobile certificate to reduce the mobile power consumption. The XML Key Management Specification (XKMS) can be the main structure for that middleware (Inc, 2002; Kangasharju et al., 2005; Nguyen and Ivar, 2008; Weerasinghe et al., 2006). The XKMS can be a good solution for the client's (mobile device) deployment limitation and resolving different vendor's problem in the mobile PKI M-PKI implementation for the security of the end-to-end SMS transmission. Figure 16 demonstrates the installation of the middleware server base on the XKMS technology. Secondly, provide or create a direct communication (No certificate authority) between the mobile devices can be also a solution, as we have mentioned that the main duty of the certificate authority is authenticating the communication user, therefore, the main challenge is how we can ensure the authentication (Al-bakri et al., 2010).

CONCLUSION

SMS is an integral part of mobile communication and SMS security is undoubtedly useful and interesting but yet a challenging issue to consider. It holds great potential in applications related to businesses, government bodies as well as in military. This paper reviews the SMS security by outlining the different security issues related to SMS systems and the mechanisms used to overcome these issues during the entire SMS transmission circle from the mobile source to the final mobile destination. Based on the author's experience, it is apparent that PKI provides high level security to protect SMS during transmission because it resolve and avoids most of the issues related to SMS security. However, it decreases the mobile performance as it requires high mobile power capability to apply the PKI process. Alternative methods should be offered to improve the mobile PKI usage in a mobile environment.

REFERENCES

Abomhara M, Khalifa O, Zakaria O, Zaidan A, Zaidan B, Alanazi H (2010). Suitability of Using Symmetric Key to Secure Multimedia Data: An Overview. J. Appl. Sci., 10: 1656-1661.

Al-bakri S, Kiah M (2010). A novel peer-to-peer SMS security solution using a hybrid technique of NTRU and AES-Rijndael. Sci. Res. Essays., 5: 3455-3466.

Al-Fayoumi M, Nashwan S, Yousef S, Alzoubaidi AR (2007). A new hybrid approach of symmetric/asymmetric authentication protocol for future mobile networks. pp. 29-29.

Alanazi H, Jalab H, Alam G, Zaidan B, Zaidan A (2010). Securing electronic medical records transmissions over unsecured communications: An overview for better medical governance. J. Med. Plants Res., 4: 2059-2074.

Alanizi H, Kiah M, Zaidan A, Alam G (2010). Secure topology for electronic medical record transmissions. Int. J. Pharmacol., 6: 954-958.

Anuar NB, Kuen LN, Zakaria O, Gani A, Wahab AWA (2008). GSM mobile SMS/MMS using public key infrastructure: m-PKI. WSEAS Trans. Comput., 7: 1219-1229.

Asokan N, Niemi V,Nyberg K (2005). Man-in-the-middle in tunnelled authentication protocols. pp. 28-41.

Asvial M, Sirat D, Susatyo B (2008). Design and Analysis of Anti Spamming SMS to Prevent Criminal Deception and Billing Froud: Case TELKOM FLEXI.

Aziz Q (2006). Payments through Mobile Phone. Emerging Technologies, 2006. ICET '06. International Conference on. pp. 50-52.

Bais A, Penzhorn WT, Palensky P (2006). Evaluation of UMTS security architecture and services. pp. 570-575.

Beller MJ, Chang LF, Yacobi Y (1993). Privacy and authentication on a portable communications system. IEEE J. Selected Areas Commun., 11: 821-829.

Biryukov A, Shamir A, Wagner D (2001). Real Time Cryptanalysis of A5/1 on a PC. pp. 37-44.

Boman K, Horn G, Howard P, Niemi V (2002). UMTS security. Elect. Commun. Eng. J., 14: 191-204.

Cai L, Yang X, Chen C (2005). Design and implementation of a server-aided PKI service (SaPKI). pp. 859-864.

Chanson ST, Cheung TW (2001). Design and implementation of a PKI-based end-to-end secure infrastructure for mobile E-Commerce. World Wide Web. 4: 235-253.

Chikomo K, Chong MK, Arnab A, Hutchison A (2006). Security of mobile banking. University of Cape Town, South Africa, Tech. Rep., Nov. 1:

Croft NJ, Olivier MS (2005). Using an approximated one-time pad to secure short messaging service (SMS). pp. 71-76.

Dankers J, Garefalakis T, Schaffelhofer R, Wright T (2002). Public key infrastructure in mobile systems. Elect. Communi. Eng. J., 14:180-190.

De Paula R, Ding X, Dourish P, Nies K, Pillet B, Redmiles D, Ren J,Rode J (2005). Two experiences designing for effective security. p. 34.

Diffie W, Hellman M (1976). New directions in cryptography. IEEE Transactions on information Theory. 22: 644-654.

Ekdahl P, Johansson T (2001). Another attack on A5/1 [GSM stream cipher], 49(1): 284-289.

Forsberg D (2007). Use Cases of Implicit Authentication and Key Establishment with Sender and Receiver ID Binding. pp. 1-8.

Garza-Saldana JJ, Daz-Pérez A (2008). A State of Security for SMS on Mobile Devices, Electronics, Robotics and Automotive Mechanics Conference, CERMA '08. 4(5):110-115.

Glitho RH (1997). Use of SS7 in D-AMPS-based PCS: orthodoxy vs. heterodoxy. Personal Commun. IEEE., 4: 15-23.

Gonzalez-Castano FJ, Vales-Alonso J, Pousada-Carballo JM, de Vicente FI, Fernandez-Iglesias MJ (2002). Real-time interception systems for the GSM protocol. IEEE Trans. Vehicular Technol., 51: 904-914.

Grillo A, Lentini A, Me G, Italiano GF (2008). Transaction oriented text messaging with Trusted-SMS. pp. 485-494.

Guthery S, Kehr R, Posegga J. (2000). How to Turn a GSM SIM into a Web Server. p. 209.

Gutmann P (2004). Simplifying public key management. Comput., 37: 101-103.

Hankerson DR, Vanstone SA, Menezes AJ (2004). Guide to elliptic curve cryptography, pp. 1-305.

Harb H, Farahat H, Ezz M (2008). Secure SMS Mobile Payment Model. Anti-counterfeiting. pp. 1-17.

Hassinen M (2005). SafeSMS-End-to-End encryption for SMS messages. pp. 359-365.

Hassinen M (2006). Java based public key infrastructure for sms messaging. Information and Communication Technologies, 2006. ICTTA'06. 2nd. 1:

Hassinen M, Hyppönen K, Haataja K (2006). An open, PKI-based mobile payment system. Emerging Trends in Information and Communication Security, pp. 86-100.

Hassinen M, Markovski S (2003). Secure SMS messaging using Quasigroup encryption and Java SMS API. pp. 187-199.

Hossain M, Jahan A, Hussain S, Amin MM, Newaz MR, Shah SH (2008). A proposal for enhancing the security system of short message service in GSM. pp. 235-240.

Hwu JS, Chen RJ, Lin YB (2006). An efficient identity-based cryptosystem for end-to-end mobile security. IEEE Trans Wireless Commun., 5: 2586.

Inc VS (2002). Trust Assertion XML Infrastructure. p. 45.

Islam S, Ajmal F (2009). Developing and implementing encryption algorithm for addressing GSM security issues.Emerging Technologies, 2009. ICET 2009. International Conference. pp. 358-361.

Jøsang A, Zomai MA, Suriadi S (2007). Usability and privacy in identity management architectures. p. 152.

Jumaat NB, Zakaria O, Gani A (2008). GSM Mobile SMS/MMS using Public Key Infrastructure: M–PKI. WSEAS Trans. Comput., 7: 1219-1229.

Kangasharju J, Lindholm T, Tarkoma S (2005). Requirements and design for XML messaging in the mobile environment. pp. 29-36.

Kawamoto K, Nakamura N (2002). Study of Management on the Mobile

Public Key Infrastructure. NOMS2002, Apr, pp. 955-957.

Koien GM, Haslestad T (2003). Security aspects of 3G-WLAN interworking. Commun. Mag. IEEE, 41: 82-88.

Kolsi O (2004). MIDP 2.0 security enhancements. p. 8.

Kuaté PH, Lo JLC, Bishop J (2009). Secure asynchronous communication for mobile devices. pp. 5-8.

Lam KY, Chung SL, Gu M, Sun JG (2003). Lightweight security for mobile commerce transactions. Comput. Commun., 26: 2052-2060.

Le Bodic G (2005). Mobile messaging technologies and services: SMS, EMS, and MMS. DOI: 10.1002/0470014520.ch3, 1-425.

Lee Y, Lee J, Song JS (2007). Design and implementation of wireless PKI technology suitable for mobile phone in mobile-commerce. Comput. Commun., 30: 893-903.

Leung CH, Chan YY, Chan CSC (2003). Analysis of mobile commerce market in Hong Kong. pp. 408-412.

Lin H, Y Harn L, (1995). Authentication protocols for personal communication systems. pp. 261.

Lison KD, Drahanský M (2008). SMS Encryption for Mobile Communication. SECTECH '08 Proceedings of the International Conference on Security Technology, pp. 198-201.

Lo JLC, Bishop J, Eloff JHP (2008). SMSSec: an end-to-end protocol for secure SMS. Comput. Security, 27: 154-167.

Lockefeer L, Hubbers E, Verdult R (2010) Encrypted SMS, an analysis of the theoretical necessities and implementation possibilities, pp. 1-40.

Lu CC, Tseng SY (2002). Integrated design of AES (Advanced Encryption Standard) encrypter and decrypter. pp. 277-285.

Malhotra K, Gardner S, Patz R (2007). Implementation of Elliptic-Curve Cryptography on Mobile Healthcare Devices. pp. 239-244.

Margrave D (2000). GSM Security and Encryption. George Mason University, pp. 1-6.

Messaging, W. (2002). API (WMA).

Meyer U, Wetzel S (2004a). A man-in-the-middle attack on UMTS. p. 97.

Meyer U, Wetzel S (2004b). On the impact of GSM encryption and man-in-the-middle attacks on the security of interoperating GSM/UMTS networks. Personal, Indoor and Mobile Radio Communications, 2004. PIMRC 2004. 15th IEEE Int. Symposium on. 4: 2876-2883.

Moore T, Kosloff T, Keller J, Manes G, Shenoi S (2002). Signaling system 7 (SS7) network security, 2(3): 496-499.

Nah FFH, Siau K, Sheng H (2005). The value of mobile applications: a utility company study. Commun. ACM, 48:90.

Nguyen TT, Ivar J (2008). Security and Performance of Mobile XML Web Services. pp. 261-265.

Nicholson A, Smith I, Hughes J, Noble B (2006). Lokey: Leveraging the sms network in decentralized, end-to-end trust establishment. Pervasive Computing. pp. 202-219.

Pesonen L (1999). Gsm interception. lecture notes, Helsinki University of technology, Lauri. Pesonen@ iki. Fi, pp. 1-9.

Pitoura E,Samaras G (1998). Data management for mobile computing, pp. 1-11.

Quirke J (2004). Security in the GSM system. AusMobile, May, pp. 1-26.

Ratshinanga H, Lo J, Bishop J (2004). A Security Mechanism for Secure SMS Communication. pp. 1-6.

Schneier B. (2005). Two-factor authentication: too little, too late. Communications of the ACM. 48: 136.

Schwiderski-Grosche S, Knospe H (2002). Secure mobile commerce. Electron. Commun. Eng. J., 14: 228-238.

Seema N, Lu CT, Liang LR (2004). Analysis of payment transaction security in mobile commerce.Information Reuse and Integration, 2004. IRI 2004. Proceedings of the 2004 IEEE Int. Conf. pp. 475-480.

Sengar H, Wijesekera D, Jajodia S (2005). Authentication and integrity in telecommunication signaling network, pp. 163-170.

Siddique SM, Amir M (2006). Gsm security issues and challenges. pp. 413-418.

Soram R (2009). Mobile SMS Banking Security Using Elliptic Curve Cryptosystem. IJCSNS. 9: 30.

Steiner JG, Neuman C, Schiller JI (1988). Kerberos: An authentication service for open network systems. pp. 191-201.

Tiejun P, Leina Z, Chengbin F, Wenji H, Leilei F (2008). M-commerce Security Solution Based on the 3rd Generation Mobile Communication, pp. 364-367.

Tillich S, Grossschaedl J (2004). A survey of public-key cryptography on J2ME-enabled mobile devices. Computer and Information Sciences-ISCIS 2004935-944, pp. 935-944.

Toorani M, Beheshti SAA (2008). Solutions to the GSM Security Weaknesses.Next Generation Mobile Applications, Services and Technologies, 2008. NGMAST '08. The Second International Conference on. pp. 576-581.

Toorani M, Shirazi B, Asghar A (2008). LPKI-a Lightweight Public Key Infrastructure for the mobile environments. pp. 162-166.

Weerasinghe D, Elmufti K, Rajarajan M, Rakocevic V (2006). Xml security based access control for healthcare information in mobile environment. pp. 1-6.

Wilson DR (1992). Signaling System No.7, IS-41 and cellular telephony networking. Proceed. IEEE, 80: 644-652.

Wilson S (2005). The importance of PKI today. China Communications. p. 15.

Wu S, Tan C (2009). High Security Communication Protocol for SMS. pp. 53-56.

Xiaoyu S, Zhenjun D, Rong C (2009). Research on NTRU Algorithm for Mobile Java Security.Scalable Computing and Communications; Eighth International Conference on Embedded Computing, 2009. SCALCOM-EMBEDDEDCOM'09. Int. Conf. pp. 366-369.

Zhang F, Yang HW, Song C (2005). A security scheme of SMS system. pp. 1333.

Zhao S, Aggarwal A, Liu S (2008). Building Secure User-to-user Messaging in Mobile Telecommunication Networks. pp. 24-26.

Zheng Y (1996). An authentication and security protocol for mobile computing. pp. 249-257.