SERVICE USAGE ANALYSIS WITH ENCRYPTED INTERNET TRAFFIC IN MOBILE MESSAGING APP

Barveen Banu. K[1], Asst. Prof. K. Chandra Prabha[2]
[1]*P.G. Student, Computer Application Department, Alagappa Chettiar Government College of engineering & Technology*
[2]*Head of the Department, Computer Application Department, Alagappa Chettiar Government College of engineering & Technology*

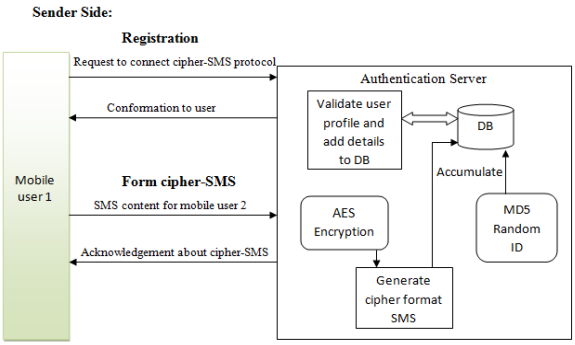
***Abstract*- In recent days, short message service (SMS) is being used in many daily life applications, including healthcare monitoring, Mobile banking, mobile commerce, and so on. But when we send an SMS from one mobile phone to another, the information contained in the SMS transmit as plain text Sometimes this information may be confidential like account numbers, passwords, license numbers, and so on, and it is a major drawback to send such information through SMS while the traditional SMS service does not provide encryption to the information before its transmission. In this paper, we propose an efficient and secure protocol called EasySMS, which provides endto-end secure communication through SMS between end users. The EasySMS protocol generates minimum communication and computation overheads as compared with existing SMSSec and PK-SIM protocols. On an average, the EasySMS protocol reduces 51% and 31% of the bandwidth consumption and reduces 62% and 45% of message exchanged during the authentication process in comparison to SMSSec and PK-SIM protocols respectively. Authors claim that EasySMS is the first protocol completely based on the symmetric key cryptography and retain original architecture of cellular network.**

***Index Terms*— Authentication, over-the-air, security, SMS, Symmetric key.**

I. INTRODUCTION

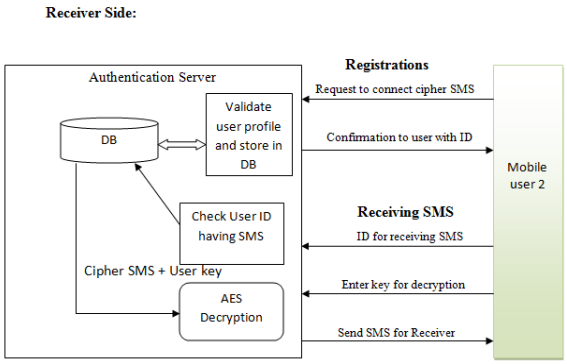
Short Message Service (SMS) has become one of the fastest and strong communication channels to transmit the information across the worldwide. On December 3, 2013, SMS service has completed its 21years as on December 3, 1992, the world's first SMS was sent by Neil Pap worth from the UK through the Vodafone network. The SMS are used in many real world applications as a communication medium such as in Transportation Information System, Mobile Deck, SMSAssassin, SMS-based web search such as SMSFind, Monitoring Community. Sometimes, we send the confidential information like password, pass code, banking details and private identity to our friends, family members and service providers through an SMS. But the traditional SMS service offered by various mobile operators surprisingly does not provide information security of the message being sent over the network. In order to protect such confidential information, it is strongly required to provide end-to-end secure communication between end-users. SMS usage is threatened with security concerns, such as SMS disclosure, man-in-the-middle attack.

II.SYSTEM ARCHITECTURE



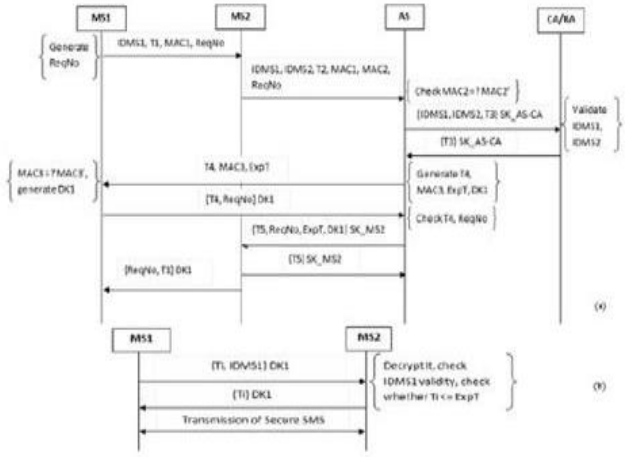
The mobile device that receive the user details with some parameters, that recognize the authenticate user. this restricts the non-owner users to see information about the SMS we send. However, any mobile device using this service can get some additional profile examination has to be handled with some unique parameter. Through this function, the mobile device can allow authenticated profile owner to access the data and send secure SMS to others.

The Authenticated mobile user can send the SMS with some key to the server. The mobile who wants to send SMS must be registered with server. The mobile sends the SMS with certain key to server. The server can encrypt the original message using AES algorithm and the send SMS to receiver through base station and mobile station. The Encrypted message can travel through base station. Receiver receives the message in secure inbox. Now the receiver wants to decrypts the message. So receiver requests the key using random number generator from server then server generates the random number and sends it to the receiver. Server recognizes the random number from receiver; from this server authenticate the authorized receiver. Then server sends the symmetric key to receiver. After getting symmetric key, receiver decrypts the encrypted message and extracts the original message in secure inbox.



Due to physical limitations of the mobile phones, it is recommended to develop a protocol which would make minimum use of computing resources and would provide better security. However, implementation of framework always increases the overall overhead which is not much suitable for the resource constraints devices such as mobile phones. Thus, in this paper we compared our proposed protocol with the existing SMSSec and PK-SIM protocols.

III. WORKING PROCEDURE



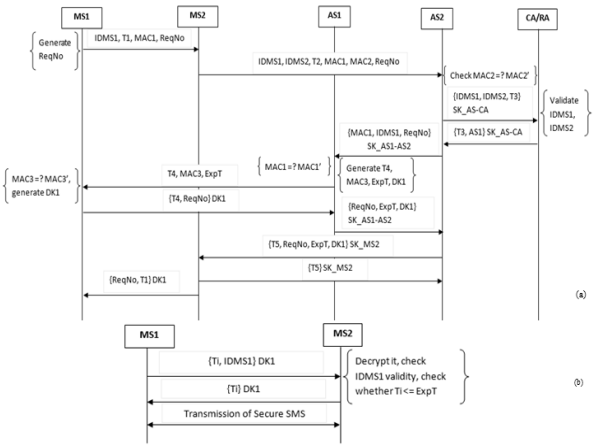
EasySMS Scenario 1: (a) Phase-1; (b) Phase-2.

Phase-1: (1) First, the mobile user who wants to send the SMS (say MS1) transmits an initial request to other mobile user (say MS2) for the connection. This initial request consists of International Mobile Subscriber Identity (IMSI) of MS1 (say IDMS1), a timestamp T1, a request number ReqNo and a message authentication code MAC1 = f1SK1(IDMS1 ReqNo). Here, SK1 is a symmetric key shared between the MS1 and the AS2. (2) On receiving the message from MS1, the mobile user who receives this request (say MS2) computes the MAC2 = f1SK2 (IDMS2||T2||MAC1). Then MS2 sends a message to the AS containing the IDMS1, IDMS2, T2, MAC1, ReqNo and MAC2 where IDMS2 is the IMSI of the MS2. The SK2 is a symmetric key shared between MS2 and the AS. With this message, the MS2 requests to the AS to check the validity of the IDMS1. (3) When the AS receives a message from the MS2, it computes the MAC2‘=f1SK2(IDMS2||T2||MAC1) and compares it with the received MAC2. If it holds then the AS sends not only the IDMS1 but also the IDMS2 to the CA/RA along with a timestamp T3 using a symmetric shared key between AS and CA/RA (say SK_AS-CA) to validate the identity of both MS. If, MAC2 and MAC2‘are not equal then the connection is terminated. (4) Next, the CA/RA checks the validity of both entities and sends the reply back to the with received timestamp T3. On receiving the message from the CA/RA, if the AS finds any of the entities is invalid then the connection is simply terminated and MS1 needs to send a fresh connection request. If both entities are valid then the AS

generates a new timestamp T4, an expiry time to authenticate MS1 (say ExpT), a delegate key DK1 generated from the SK1 using a function f2 and a new message authentication code MAC3=f1SK1 (T4||ExpT||ReqN o) and DK1=f2SK1(T4||ReqNo). Then the AS sends (T4, MAC3, ExpT)to the MS1. (6) After receiving the message from AS, theMS1 first computes MAC3‘and compares it with the receivedMAC3, where MAC3‘= f1SK1 (T4||ExpT||ReqNo). If both are same then MS1 computes the DK1. Next, MS1 sends T4 and the corresponding ReqNo to the AS encrypted with the DK1key. (7) The AS checks the received T4 with its stored valueand confirms ReqNo. If both are correct then the authentication of MS1 is completed. Thereafter, the AS sends DK1 to the MS2 along with a new timestamp T5, ExpT and ReqNo after encrypting all using the SK of MS2 (SK_MS2) which is a shared key between AS and MS2. (8) The MS2 simply confirms the reception of DK1 key by replying to the AS ,the T5 encrypted with the SK of MS2. (9) MS2 also sends ReqNo and T1 to the MS1 encrypted with DK1 so that MS1 can verify the correctness of T1 and ReqNo. This message also verifies the successful reception of DK1 by the MS2. SMS has a variety of advantages and disadvantages for M-Commerce purpose.

The advantages are it is easy to use, a common messaging tool among consumers, works across all wireless operators, affordable for mobile users, no specific software required for installation, allows banks and financial institutions to provide real-time information to consumers and employees and stored messages can be accessed without a network connection. Most important disadvantage of SMS is that it does not offer a secure environment for confidential data during transmission and there is no standard procedure to certify the SMS sender. There is a need for an end to end SMS Encryption with errorless message transmission in order to provide a secure with error free data transmission for communication. These two factors are important for SMS. In this paper, we have analyzed about mainly JCCC and Soft Input Decryption (SID). We proposed a novel theoretically scheme NTRU Sign algorithm in this paper. We are expect that it will improve the current security level speed and provide reliable message at receiver end.

Phase-2: Once both MS have a shared secret symmetric key, they can exchange the message information in a secure manner using a suitable and strong cryptographic algorithm like AES/MAES (explained later). After phase-1, a session is generated which provides the secure communication between both MS for a specified time period ExpT. In this time period the same DK1 key is used to provide ciphering between MS1 and MS2but after the ExpT time the session gets expire and MS1 needs to send a fresh request to MS2 with a new request number ReqNo with the same procedure of phase-1. Within the ExpT, the following steps are used for the communication between both MS: (1) The MS1 sends the IDMS1 and a timestamp (say Ti) to the MS2 encrypted with symmetric key of MS1 i.e., DK1. (2) MS2 decrypts the message usingmthe same DK1 key and checks the validity of IDMS1 and verifies whether Ti <= ExpT. If both are correct then MS1 is successfully authenticated and proved as a valid user for the connection. Then MS2 replies the same received Ti encrypted with DK1 as an acknowledgement to MS1. (3) Secure SMS communication between both MS takes place. In this paper, we propose and implement a service model to transfer messages safely for PDA on CDMA wireless networks and a secure message transfer protocol which considers characteristics of PDA. The proposed PUSH service uses SMS (short message service) to connect an offline client device with the wired network for data communication. After receiving SMS message, client device process the SMS message and creates a data channel thought RAS (remote access service), and then the data of the server can be pushed to client. The implemented securing protocol can provide safe data transmission on each communication channel thought two way channels of SMS and data. This protocol can reduce a number of transmissions for exchanging a safe session key by using security nonce table. As a result, intensity of encryption can be increased.



EasySMS Scenario 2: (a) Phase-1; (b) Phase-2.

When Both MS Belong to Different AS: This scenario is presented in Fig. 3 where MS1 sends a message to MS2 while both MS belong to the different AS. This case is one where both mobile users are located in the geographically far areas and they have different authentication centers. It may be the case where both MS are of different service providers so they genuinely have different authentication centers. This scenario is also subdivided into two phases.

Phase-1: (1) It is same as presented in step-1 of scenario-1. Here, SK1 is a symmetric key shared between MS1 and AS1. (2) The MS2 passes (IDMS1, IDMS2, ReqNo, T2, MAC1, MAC2) to the AS through which it is connected (say AS2).

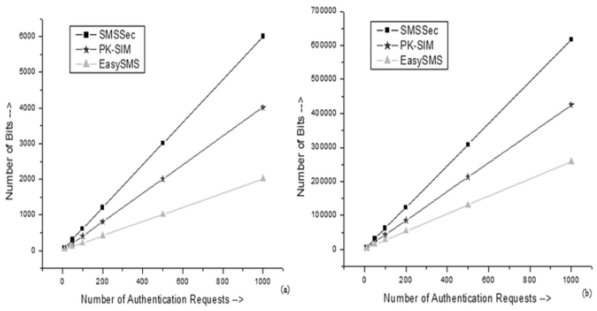
The SK2 is a symmetric key shared between MS2 and the AS2. With this message, the MS2 requests to the AS2 to check the validity of the IDMS1. The MS2 stores the timestamp T1 in the memory which was received from the MS1. (3) The AS2 computes the same as presented in step-3 of scenario-1 and checks whether MAC2?=MAC2'. (4) The CA/RA checks the validity of both entities and sends the reply back to the AS2 with the received timestamp T3 and the identity of AS to which MS1 belongs (say AS1). (5) The AS2 checks the same as in scenario-1 step-5, if both entities are valid then the AS2 sends (IDMS1, ReqNo, MAC1) to the AS1 through a secure channel or using a symmetric key shared between AS1 and AS2 (say SK_AS1-AS2). We assume that all AS communicate with each other using the pre-computed symmetric shard keys. (6) When the AS1 receives the message from the AS2, it computes MAC1'= f1SK1(IDMS1||ReqNo) and compares MAC1' with the received MAC1. If both are different then the connection is terminated. If both are same then the AS1 generates a new timestamp T4, an expiry time to authenticate MS1 (say ExpT), a delegate key DK1 generated from the SK1 of MS1 using a function f2, and a MAC3, where MAC3 = f1SK1(T4||ExpT||ReqNo) and DK1 = f2SK1(T4||ReqNo). Then the AS1 sends (T4, MAC3, ExpT) to the MS1. (7) After receiving the message from AS1, MS1 repeats the same as in scenario-1 step-6 and sends (T4, ReqNo) to the AS1 encrypted with DK1 key. (8) The AS1 checks T4 and ReqNo as in scenario-1 step-7. Then AS1 conveys the confirmation of the authentication of MS1 by sending a message (ReqNo, ExpT, DK1) to the AS2 using SK_AS1-AS2 key. (9) The AS2 sends DK1 to the MS2 along with a new timestamp T5, expiry time ExpT and request number ReqNo after encrypting all using the SK of MS2 (say SK_MS2) which is a shared key between the AS2 and the MS2. (10) MS2 repeats the same as in scenario-1 step-8, and sends encrypted reply of T5 to the AS2. (11) It is same as in scenario-1 step-9.

Phase-2: The phase-2 is same as discussed in the previous scenario of phase-2.

IV. ANALYSIS OF PROPOSED PROTOCOL

This section analyzes proposed protocol in various aspects such as mutual authentication, prevention from various threats and attacks, key management, and computation & communication overheads. Is the Secret Key SK Safely Stored? Since the malicious user does not know the structure of cryptographic functions like f1() and f2(), so he/she can neither generate the correct MAC1 nor correct delegation key DK1. Further, the secret key SK is stored on the authentication server/center as well as embedded onto the SIM at the time of manufacturing. Thus, it is almost impossible to extract the SK. The storage scenario of SK key we presented is same as nowadays used for the voice communication in the traditional cellular networks. If some service providers do not wish to use actual SK in the protocol execution, they can compute alternate secret keys with a new function f‖ as: SK1'=f‖SK1(IDMS1) and SK2'= f‖SK2(IDMS2). We do not prefer to do it because it increases the overall overhead of protocol.

Is There Any Alternative for IMSI?



Since a malicious user with only known IMSI (by some IMSI catcher but functions and secret keys are still unknown) cannot break the security of proposed protocol. Thus, the proposed protocol is secure. We can also have one alternate for it. We can propose a new function f`() which computes a temporary IMSI for each MS whenever it wants to communicate. At MS: compute IDMS1 = f`(IMSI1, MAC1); At AS: compute IMSI1 = f`(IDMS1, MAC1). This is simply possible by XOR ing the IMSI1 (or IDMS1) and MAC1 (twice), because the size of MAC1 is 64 bits while IMSI1/IDMS1 is of 128 bits. The function f`() should be known to MS as well as AS but publically unknown. But we recommend using a complex function to compute the same. However, we do not prefer because it increases the overhead at MS as well as at AS.

Mutual Authentication between MS and AS

In scenario-1 of EasySMS protocol, the AS authenticates MS1 by verifying the MAC2 and checks the identity of MS1 through CA/RA. When AS receives MAC2, it simply calculates MAC2‘and compares it with the received MAC2. If it matches, then authentication of MS1 is done by the AS. Similarly, on receiving MAC3, the MS1 computes MAC3‘to authenticate the AS. If MAC3 is equal to the MAC3‘then the authentication of AS is successful. All this ensures the mutual authentication between MS1 and AS through MS2. Similarly, in scenario-2, the AS1 authenticates MS1 through AS2 and MS2. The integrity is maintained between MS1-AS1 and MS2-AS2 by comparing the MAC1-MAC1‘and MAC2-MAC2‘respectively. The MS1 authenticates AS1 by comparing MAC3 with MAC3‘.

Efficient Key Management

The EasySMS protocol is able to efficiently handle the key management issue in both scenarios where the DK1 key (from the symmetric key of MS1) is securely transmitted by the AS to the MS2 (scenario-1) or by the AS2 to the MS2through AS1 (scenario-2). Thus, this protocol successfully ciphers the message before its transmission over the network. We preferred a symmetric key algorithm because these algorithms are 1000 times faster than the asymmetric algorithms and improve the efficiency of the system.

Resistance to Attacks

In this subsection, we justify that the EasySMS protocol is able to prevent the transmitted SMS from various attacks over the network. It is assumed that the cryptographic functions used in the paper are not publically available and are secret. The capturing of any secret key SK is not possible because no secret key has been transmitted in any phase of the proposed protocol and always a delegation key DK1 is being transferred in the cipher mode whenever is required. Secret keys are also not publically available and are secret.

SMS Disclosure

In the EasySMS protocol, a cryptographic encryption algorithm AES/MAES is maintained to provide end-to-end confidentiality to the transmitted SMS in the network. Thus, encryption approach prevents the transmitted SMS from SMS disclosure.

Replay Attack

The proposed protocol is free from this attack because it sends one timestamp (like T1, T2, T3, T4 and T5) with each message during the communication over the network. These unique timestamp values prevent the system from the replay attack. This attack can be detected if later previous information is used or modified.

Man-in-the-middle Attack

In the EasySMS protocol, a symmetric algorithm AES/MAES is used for encrypting/ decrypting end-to-end communication between the MS and the AS in both scenarios. The message is end to end securely encrypted/decrypted with DK1 key for every subsequent authentication and since attacker does not have sufficient information to generate DK1, thus it prevents the communication from MITM attack over the network.

OTA Modification in SMS Transmission

The EasySMS protocol provides end-to-end security to the SMS from the sender to the receiver including OTA interface with an additional strong encryption algorithm AES/MAES. The protocol does not depend upon the cryptographic security of encryption algorithm (such as A5/1, A5/2) exists between MS and BTS in traditional cellular networks. This protocol provides end to end security to end users. It protects the message content being access by mobile operators as well as from attackers present in the transmitted medium.

Impersonation Attack

There are two cases to evaluate this attack with EasySMS protocol. Both cases are as follows: (a) *When an attacker impersonates the MS:* In Easy SMS ,if an attacker tries to impersonate the MS, he/she will not get success because in scenario-1, the AS calculates the MAC2‘ and compares it with the received MAC2, while in scenario- 2, the AS2 computes MAC2‘ and compares with MAC2. Thereafter, the AS1 computes MAC1‘and checks whether MAC1‘ is equal to the MAC1. Thus, at any stage if the AS finds the above comparison false then the connection is simply terminated. (b) *When an attacker impersonates the AS:* If an attacker tries to impersonate the AS (or AS1/AS2), the attempt to impersonate the AS will be failed as the MS1 computes MAC3‘and compares it with the received MAC3. Thus, an attempt to impersonate the AS terminates the connection

V.FORMAL PROOF OF PROPOSED PROTOCOL

In order to clear statement of our analysis, we use the BAN Logic symbols to formally proof the authentication process of the proposed protocol. (1) $P| \equiv X$: P believes X, or P would be entitled to believe X, (2) $P \_X$: P sees X. Someone has sent a message containing X to P, who can read and repeat X, (3) $P| \sim X$: P once said X. P at some time sent a message including the statement X, (4) $P| \Rightarrow X$: P has jurisdiction over X. P is an authority on X and should be trusted on this matter, (5) $\#(X)$: The formula X is fresh, that is, X has not been sent in a message at any time before the current run of the protocol, (6) $P \overset{K}{\leftrightarrow} Q$: P and Q may use the shared key K to communicate, (7) $P \overset{X}{\Leftrightarrow} Q$: The formula X is a secret known only to P and Q, (8) $(X)y$: This represents X combined with the formula Y that Y be a secret.

The Formal Messages in EasySMS Protocol:

Phase-1:

1. $MS1 \rightarrow MS2 : ID1, Ta,$ ReqNo,f1SK1$(ID1||ReqNo);MS1 \overset{SK1}{\leftrightarrow} AS1$; 2. $MS2 \rightarrow AS2 : ID1, ID2, Tb,$ $ReqNo$,f1SK1$(ID1||ReqNo)$, f1SK2$(ID2||Tb||f1SK1\ (ID1||ReqNo))$; $MS2 \overset{SK2}{\leftrightarrow} AS2$; 3. $AS2 \rightarrow CA/RA : \{ID1, ID2, Tc\}_{SKAS-CA}$; $\forall ASi\ SKASi-CA \leftrightarrow CA$;

4. $CA/RA \rightarrow AS2 : \{AS1, Tc\}_{SKAS-CA}$; 5. $AS2 \rightarrow AS1 : \{ID1,$ Re$qNo,$ f1SK1 $(ID1 \ || \ ReqNo)\}_{SKAS1-AS2}$; $\forall ASiSKASi-AS\ j \leftrightarrow \forall ASj,$ *where* $i = j$; 6. $AS1 \rightarrow MS1 : Td, Exptime,$ f1SK1$(Td||Exptime||ReqNo)$;7. $MS1 \rightarrow AS1 : \{Td,$ ReqNo$\}$DK1 ; $MS1 \overset{DK1}{\leftrightarrow} AS1$; 8. $AS1 \rightarrow AS2 :$ $\{ReqNo, Exptime,$ f2SK1$(Td||$ ReqNo$)\}_{SKAS1-AS2}$ 9. $AS2 \rightarrow MS2 : \{Te, ReqNo,$ $Exptime,$ f2SK1 $\{(Td||ReqNo)\}_{SKAS1-AS2}\}_{SK2}$; 10. $MS2 \rightarrow AS2 :$ $\{Te\}$SK2;

11. $MS2 \rightarrow MS1 : \{Ta,$ Re$qNo\}$DK1

Phase-2:

1. $MS1 \rightarrow MS2 : \{Ti\ , ID1\}$DK1;
2. $MS2 \rightarrow MS1 : \{Ti\ \}$DK1

VI. CONCLUSION

EasySMS protocol is successfully designed in order to provide end-to-end secure communication through SMS between mobile users. The analysis of the proposed protocol shows that the protocol is able to prevent various attacks. The transmission of symmetric key to the mobile users is efficiently managed by the protocol. This protocol produces lesser communication and computation overheads, utilizes bandwidth efficiently, and reduces message exchanged ratio during authentication than SMSSec and PK-SIM protocols. EasySMS which provides end-to-end secure communication through SMS between end users. EasySMS is executed which makes available the symmetric shared key between both MS and then ciphering of message takes place using a symmetric key algorithm. Short Message Service (SMS) has become one of the fastest and strong communication channels to transmit the information across the worldwide. Sometimes, we send the confidential information like password, pass

code, banking details and private identity to our friends, family members and service providers through an SMS. SMS messages are transmitted as plaintext between mobile user (MS) and the SMS center (SMSC), using wireless network. SMS contents are stored in the systems of network operators and can be read by their personnel. Since, the SMS is sent as plaintext, thus network operators can easily access the content of SMS during the transmission at SMSC.

VII. ACKNOWLEDGEMENT

This research was supported by my guide and supervisors. I thank my faculties and friends who provided insight and expertise that greatly assisted the research, although they may not agree with all of the interpretations of this paper. I thank **Mrs. Chandra Prabha. K**, Assistant Professor, Alagappa Chettiar Government College of Engineering & Technology for commenting that greatly improved the manuscript.

REFERENCES

[1] Press Release. (2012, Dec. 3). *Ericsson Celebrates 20 YearsofSMS*[Online].Available:http://www.ericsson.com/ag/news/2012-12-03-smsen_3377875_c

[2] R. E. Anderson *et al.*, ―Experiences with a transportation information system that uses only GPS and SMS,‖ in *Proc. IEEE ICTD*, no. 4, Dec. 2010.

[3] D. Risi and M. Teófilo, ―Mobile Deck: Turning SMS into a rich user experience,‖ in *Proc. 6th MobiSys*, no. 33, 2009.

[4] K. Yadav, ―SMSAssassin: Crowdsourcing driven mobile-based system for SMS spam filtering,‖ in *Proc. Workshop Hotmobile*, 2011, pp. 1–6.

[5] J. Chen, L. Subramanian, and E. Brewer, ―SMS-based web search for low-end mobile devices,‖ in *Proc. 16th MobiCom*, 2010, pp. 125–135.

[6] B. DeRenzi *et al.*, ―Improving community health worker performance through automated SMS,‖ in *Proc. 5th ICTD*, 2012, pp. 25–34.

[7] M. Densmore, ―Experiences with bulk SMS for health financing in Uganda,‖ in *Proc. ACM CHI*, 2012, pp. 383398.

[8] J. Hellström and A. Karefelt, ―Participation through mobile phones: A study of SMS use during the Ugandan general elections 2011,‖ in *Proc. ICTD*, 2012, pp. 249–258.

[9] I. Murynets and R. Jover, ―Crime scene investigation: SMS spam data analysis,‖ in *Proc. IMC*, 2012, pp. 441– 452.

[10] K. Park, G. I. Ma, J. H. Yi, Y. Cho, S. Cho, and S. Park, ―Smartphone remote lock and wipe system with integrity checking of SMS notification, ‖in *Proc. IEEE ICCE*, Jan. 2011, pp. 263–264.

pp. 137–148. [11] A. Nehra, R. Meena, D. Sohu, and O. P. Rishi, ―A robust approach to prevent software piracy,‖ in *Proc. SCES*, 2012, pp. 1–3.

[12] N. Gligoric, T. Dimcic, D. Drajic, S. Krco, and N. Chu, ―Application layer security mechanism for M2M communication over SMS,‖ in *Proc. 20th TELFOR*, 2012, pp. 5–8.