ISSN PRINT 2319 1775 Online 2320 7876

Research paper © 2012 IJFANS. All Rights Reserved, UGC CARE Listed (Group -I) Journal Volume 8, Issue 3, 2019

MESSAGE ENCRYPTION USING DICTIONARY BASED COMPRESSION

N. SreeRam

Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, India, sriramnimagadda@gmail.com

Abstract.

Now a days, SMS (Short Message Service) is a very popular service in mobile communication. As SMS is an offline message service which can exchange data from source to destination, a lot of burden on server and memory absorption is being observed. Most of the times, the traffic on the network is also very high and it is again an additional burden to transmit huge messages over the network. To address the above-mentioned problems, this paper has emphasized one of the possible mechanisms which works around a dictionary of Most Frequently Used (MFU) words for the effective utilization of server memory space and network bandwidth.

Keywords: SMS, MFU dictionary, Encryption, memory space.

1. Introduction

Short Message Service (SMS) is a globally accepted wireless service that enables the transmission of alphanumeric message between mobile subscribers and external systems such as electronic mail, paging and voice-mail systems. SMS was originally designed as part of the Global System for Mobile Communications (GSM) digital mobile phone standard, but is now available on a wide range of networks, including 3G networks. At present this SMS also plays a vital role in wireless communication. The wireless network transport short messages between the SMSCs (Short Message Service Centres and wireless stations. By using SMS, an active mobile handset is able to receive or submit a short message at any time, independent of whether a voice or data call is in progress. SMS also guarantees delivery of the short message by the network.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper © 2012 IJFANS. All Rights Reserved, UGC CARE Listed (Group -I) Journal Volume 8, Issue 3, 2019

Normally, each character in SMS occupies one byte or eight bits of memory. If it is possible to represent one word by 8 bits instead of one character by 8 bits, huge amount of server memory can be saved and the data to be transmitted over the network can also be reduced which in turn can reduce the traffic over the network. As SMS is an offline message service and if receiving stations are not identified, the short message is stored in the SMSC until the destination device becomes available. If the large numbers of short messages are stored in the SMSC, obviously there will be huge pressure for SMSC. So, by reducing each word space that it occupies, SMSC will be relieved from huge pressure. The success of this system mainly depends on the effective maintenance and usage of MFU words dictionary. The MFU dictionary has to maintain at both source and destinations. This technique also provides encryption at source and decryption at destination by using MFU words dictionary, so that a third-party person can be able to see only 1's & 0's which cannot be understood by third party

2. HISTORY OF SMS

The idea of adding text messaging to the services of mobile users was latent in many communities of mobile communication services at the beginning of the 1980s. The first action plan of the CEPT Group GSM, approved in December 1982, requested "The services and facilities offered in the public switched telephone networks and public data networks... should be available in the mobile system". This target includes the exchange of text messages either directly between mobile stations, or transmitted via Message Handling Systems.

The SMS concept was developed in the Franco-German GSM Corporation in 1984 by Friedhelm Hillebrand and Bernard Ghillebaert. The innovation in SMS is short. The GSM is optimized for telephony, since this was identified as its main application. The key idea for SMS was to use this telephony-optimized system to transport messages on the signaling paths needed to control the telephony traffic during time periods, when no signaling traffic existed. In this way, unused resources in the system could be used to transport messages at minimal cost. However, it was necessary to limit the length of the messages to 128 bytes (later improved to 140 bytes, or 160 7-bit characters), so that the messages could fit into the existing signaling formats.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper © 2012 IJFANS. All Rights Reserved, UGC CARE Listed (Group -I) Journal Volume 8, Issue 3, 2019

3. SMS Today

In 2008, 4.1 trillion SMS text messages were sent. SMS has become a massive commercial industry, worth over 81 billion dollars globally as of 2006. The global average price for an SMS message is 0.11 USD, while the cost to providers is negligible. Mobile networks charge each other so-called interconnect fees of at least 0.04 USD (£0.03) when connecting between different phone networks. Messages are sent to a Short Message Service Center (SMSC) which provides a “Store and Forward” mechanism. It attempts to send messages to the SMSC's recipients. If a recipient is not reachable, the SMSC queues the message for later retry. Some SMSCs also provide a "forward and forget" option where transmission is tried only once. Both mobile terminated (MT, for messages sent to a mobile handset) and mobile originating (MO, for those sent from the mobile handset) operations are supported. Message delivery is “best effort”, so there is no guarantee that a message will actually be delivered to its recipient, but delay or complete loss of a message is uncommon. Users may request delivery reports to confirm that messages reach the intended recipients, either via the SMS settings of most modern phones, or by prefixing each message with *0# or *N#.

5. SMS ENCRYPTION

Because of the SMS Spoofing, security of message has to be taken care. Now days, SMS is not only being used for just text transfer but for various purposes such as to pay telephone bill, mobile banking, and many other financial transactions. This paper also deals with the concept of storing the messages in an encrypted form so that the middle person cannot understand even if the message is hacked. The words of message are stored in the form of encrypted bit strings; as a result, memory will be saved and message will be encrypted.

A. Encryption Process:

A simple message contains character set {a, b, c, d, ……..,z} ,{A, B, C, D, …,Z}, and some special characters such as ,,.,?,space and numbers 0 to 9 etc.. In SMS, people regularly use same kind of words such as good morning, good evening, congratulations, all the best etc.. For this purpose, a dictionary of the Most Frequently used words will be maintained. The words are assigned with a bit string and are stored in the memory. Every word in the dictionary is placed in alphabetical order and are given bits order in the range of 28 possible bit combinations.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper

© 2012 IJFANS. All Rights Reserved, UGC CARE Listed (Group -I) Journal Volume 8, Issue 3, 2019

Table 1: MFU dictionary format

Word	Binary code	Word	Binary code
A or a	00000000	bad	00001111
About or abt	00000001	boy	00010000
Act	00000010	break	00010001
Action	00000011	bed	00010010
Africa	00000100	bye	00010011
Agree	00000101	C or c	00010100
Aggregate	00000110	cap	00010101
Ahead	00000111	call	00010110
Aim	00001000	D or d	00010111
akash	00001001	dear	00011000
America	00001010	desk	00011001
An	00001011	doctor	00011010
Angle	00001100	E or e	00011011
Auspecious	00001101	eat	00011100
B or b	00001110	F or f	0010000

B. Algorithm:

Step 1: Identify the list of most frequently used words of mobile messages.

Step 2: Arrange all the words in alphabetical order and form it as a Dictionary.

Step 3: Assign numbers to the words of Dictionary in a sequence and the assigned index/number of a particular word will be stored in the form of its equivalent binary number.

C. Most Frequently Used Words Dictionary (Mfud):

MFU words dictionary contains the more frequently used words and special characters in SMS. Each word in this dictionary is defined with a 8 bit code in alphabetical order. The words in the dictionary are not case sensitive. This MFU dictionary is defined for most of the frequently used words comprises of 26 alphabets, numbers and special characters. This MFU

ISSN PRINT 2319 1775 Online 2320 7876

Research paper © 2012 IJFANS. All Rights Reserved, UGC CARE Listed (Group -I) Journal Volume 8, Issue 3, 2019

dictionary has to be maintained in both sender node and receiver nodes. The business logic of encoding and decoding of SMS is also provided in both sender and receiver mobile sets. When a sms is typed by the sender, the encoding module of the node automatically breaks the sms into words and identifies the equivalent 8 bit binary code of the words from dictionary and encode that sms with that binary code. If any word in sms in not matched with any of the words in the MFU dictionary that word was transmitted over the network without any encryption.

For each word, one separate frame is created whether the word was matched with the word in dictionary or not. Each frame consists of a 8 bit header. When a sms was encoded by 8-bit binary code, automatically its size was reduced and security is also provided. This technique can reduce the wastage of memory space on the server machine and network bandwidth can also be used in efficiently. The presence of a blank space in sms indicates the starting of new word. If there is more than one blank space in between two words, then they are truncated to a single blank space.

There are two types of headers that can be used in this sms system. Each frame consists of an 8-bit header and encoded data as shown below.

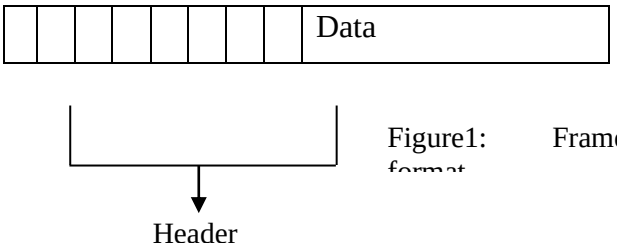

Figure1: Frame format

The frame format consists of two parts. Header and data part.The header length is 8 bits. If the data in the data part is matched with the MFU dictionary, it contains all ones. Data: The data part contains the encoded data. If any word in the sms was not matched in with any word in the MFU dictionary, then a separate frame was created with a separate header. The header used in this case is also having the length of 8 bits.

D. Algorithm

Step 1: The MFU words dictionary is stored in the both source and destination mobile sets.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper © 2012 IJFANS. All Rights Reserved, UGC CARE Listed (Group -I) Journal Volume 8, Issue 3, 2019

Step 2: The words of a message will be searched from MFU dictionary and the matched words will be encoded with their equivalent bit sequence.

Step 3: If a particular word of message fails to find its match in MFU dictionary, then that word will be stored in conventional method.

Step 4: The encoded sms will be transmitted over the network.

Step 5: when the sms arrived at destination the decoding module decode the sms by searching the same MFU dictionary.

By this process, the message can be encrypted as well as squeezing. In turn, network bandwidth problems, security problems and server memory overhead problems can be addressed.

6. Results and Discussion

BEST CASE

If the message text contains all the words from the MFU word dictionary, then it will be the best case. For example, the text is ‘good morning and How are you’, Here, the text contains altogether 28 characters.

Normally one character occupies 8 bits or one byte of memory space. To send the above text as per the existing method, it requires 28 X 8 = 244 bits of memory.

By using present encryption method to send the above text, it requires just 6 bytes for 6 headers and 6 more bytes to represent equaling code of each word i.e totally 12=8=96 bits only.

So it is possible to save 244 – 96 = 148 bits of memory space i.e. around 60 % of memory space can be saved.

WORST CASE

When the words of the given message do not match with any of the MFU words, the entire message has to be transmitted untouched. But every word has to be prefixed with the header. For example: the words of the message ‘sutn moion eergg ’ will not match with the words of MFU dictionary. At this stage, the message will be saved in the original format; but, additional overhead of introducing header2 for each word of the message will be observed.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper © 2012 IJFANS. All Rights Reserved, UGC CARE Listed (Group -I) Journal Volume 8, Issue 3, 2019

7. Conclusions

The developed Short Message Squeezing method not only helps in reducing the memory overhead on the server; but it also helps in encrypting the message. And hence, the developed methodology will help a lot to have more secured way of sending SMS over mobile networks. The developed methodology is based on the conventional dictionary-based compression. More sophisticated compression techniques and encryption techniques can be adopted to have more effective Message Squeezing and Encryption process. In this paper, there is an assumption that all the transmitted frames will be reached in same order as that of the sending order. But the same cannot be ensured in wireless communication. So, there is a need to address the problem of message sequencing as well.

References

1. MohammadReza Gholami, Seyyed Mohsen Hashemi and Mohammad Teshnelab "A Framework for Secure Message Transmission Using SMS-Based VPN" IFIP International Federation for Information Processing, 2008, Volume 254, Research and Practical Issues of Enterprise Information Systems II Volume 1, Pages 503-511
2. Toorani M.Bhesti shirazi A.A Iran university of Sci. & Technology, Tehran " A Secured SMS messaging protocol for the m-payment systems" Computers & Communications 2008 ISCC 2008. 6-9 july 2008 pages 700-705
3. Tarek M. Mahmoud, Bahgat A. Abdel-latef, Awny A. Ahmed, Ahmed M. Mahfouz "Hybrid Compression Encryption Technique for Securing SMS" International Journal of Computer Science and Security (IJCSS), Volume (3): Issue (6)
4. www.d2vozd.org
5. www.wikipedia.org
6. Andrew S Tanenbaum "Computer Networks" 4th Edition Pearson Education.