Texting to 9-1-1:

Examining the Design and Limitations of SMS

4G americas™

October 2010

4G AMERICAS TEXTING TO 9-1-1 WHITE PAPER – TABLE OF CONTENTS

EXECUTIVE SUMMARY

A citizen’s ability to send text messages to 9-1-1 emergency services (e.g., PSAP) is a topic that is undergoing significant discussions in the emergency services community, the people with disabilities community, and the wireless industry. The term “text” is used in the general sense during these discussions – “text” signifies everything from the short message service (SMS), to instant messaging (IM), to social networks such as Twitter® and Facebook®. Understandably, the people with disabilities community in particular has expressed interest in text to 9-1-1 using the existing capabilities of their mobile devices, as an alternative to using bulky, cumbersome add-on TTY devices. The wireless industry fully understands the desires of the people with disabilities community and is focused on finding a reliable solution for their needs. This analysis focuses on SMS as a means to contact 9-1-1 emergency services, with a goal to provide a view of the capabilities, limitations, threats and vulnerabilities of this means of communications.

Texting, particularly SMS, has exploded in the past decade. Citizens rely on texting for their social communications needs. There are millions of SMS messages sent each day and there is a perception that SMS is reliable; however, SMS was never designed as a reliable means for life-saving critical communications. SMS was designed to be secondary to voice calls and was never designed to provide the full and robust communications citizens have come to expect with voice calls. SMS has significant limitations and shortcomings that do not make SMS suitable for emergency communications, especially under life threatening conditions.

It is important to understand that SMS is not and never will be a real-time communications service. SMS by its very design is a non-real-time, best-effort, store-and-forward service. SMS is not a session based protocol; without session based communications, SMS makes correlation of multiple messages from a citizen to a particular emergency impossible. With these characteristics, SMS messages may have a delayed delivery, may be delivered in a different order than the sender intended, or may be lost or discarded.

A critical component to providing emergency services in a timely manner to citizens in distress is for the emergency information to be routed to the appropriate PSAP, and for that PSAP to be able to obtain the current location of the citizen who is requesting the emergency services. Routing to the appropriate PSAP is facilitated by the rough location of the subscriber when they initiate a voice call. The ability to obtain more accurate location information is available when there is a voice call; however, there is no location information available for the routing function or for the PSAP to obtain location information when a citizen initiates an SMS message and it traverses the network. While there are applications that make use of location capabilities of the mobile device, locating the nearest pizza restaurant is significantly different from the location accuracy required to direct an emergency response.

Since SMS was never intended for robust mission-critical communications, SMS was not designed with security mechanisms. SMS has a number of security vulnerabilities including SMS spoofing, Denial of Service vulnerabilities, SPAM, Malware, etc. These security vulnerabilities are primarily due to the lack of authentication of SMS messages and the ability to inject SMS messages into the network from external sources.

Related to SMS spoofing are emerging smartphone applications and third party network services commonly called “Free SMS” or “SMS Bypass.” These applications provide SMS capability without using the wireless operator messaging capabilities. These smartphone applications even have screens that look very similar to the “real” SMS services. The wireless operator network has no knowledge or control of these other SMS applications. Some of these special SMS services don’t even require a mobile device. These services can be done via a PC and can totally bypass wireless networks. However, to the recipient, these SMS messages could look like they are coming from a

mobile device.   As a result a PSAP could be subject to massive amounts of SPAM or Denial of Service attacks from what appear to be legitimate SMS messages coming from mobile devices on wireless networks.

Without clear requirements and a standardized design for non-voice emergency communications, the result will be a patchwork implementation that will be a source of confusion to the wireless users since they will have no indication of when they are within a PSAP boundary and served by a wireless operator which supports SMS to 9-1-1 and when they are outside of the area that supports SMS to 9-1-1. There may also be inconsistent vendor-specific implementations across PSAPs and wireless operators. This confusion could result in even further delays in obtaining the emergency services that the user requires.

Current voice emergency services support emergency calls to 9-1-1 for mobile devices that do not have an installed smart card ("SIM" or "UICC") or which may not be authorized for regular voice services in the serving network (for example, a prepaid device that has depleted the funds for service). Mobile devices that don't contain a smart card or are not authorized for use on the serving network cannot initiate SMS messages due to the fundamental design of the network protocols.

The wireless industry recognizes that there are numerous regulatory discussions in progress, and is very engaged in these regulatory discussions. However, the viability of scalable SMS to 9-1-1 service cannot be solved simply by the stroke of a regulator's pen. As will be detailed throughout this white paper, multiple technical issues inherent in SMS design and implementation show that SMS to 9-1-1 is not a rational technical possibility.

Implementation of SMS to 9-1-1 emergency services could have significant impacts on the resources and personnel of the PSAPs. SMS can be originated through a number of sources including wireless devices, the Internet, and third party applications on smartphones. The only way to control the authenticity of these text messages is at the destination, which will require significant SPAM filtering and other protections at the PSAPs.

The National Emergency Number Association (NENA) is currently defining the next generation emergency services requirements and environment. Recent increased cooperation between NENA and the wireless industry, including the Alliance of Telecommunications Industry Solutions (ATIS) and the 3rd Generation Partnership Project (3GPP), is leading to a uniform approach across access technologies (wireline/wireless). This will no doubt benefit both the consumer as well as the PSAPs. These are ongoing, multi-year efforts that will impose significant costs and promise major benefits. Efforts to address the legacy SMS standards will detract from resources that could otherwise be used to advance next generation systems; hence delaying a better solution in order to deploy a limited and constrained one.

In conclusion, there are significant limitations inherent in the design of the current Short Message Services which make it impractical to be used for emergency service. However, the industry is fully aware that it is important to address the requirements for people with disabilities as soon as possible. To that end, it is recommended that techniques which are readily available today, such as silent 9-1-1 calls, along with accelerating research and development into emerging technologies such as TTY Emulation, be undertaken while the next-generation systems are being designed. The following considerations must be taken into account:

- SMS to 9-1-1 is a best effort service with no delivery or performance guarantees, therefore FULL liability protection must be provided for wireless operators and other stakeholders. Liability protections for SMS to 9-1-1 have to be far greater than those for voice because the probability of something going wrong is so much greater and there are more areas where things can go wrong.

- There needs to be an education process for both call takers and consumers on the experience expected as the experience for both the call taker and end user for texting to 9-1-1 will be significantly different than voice or TTY to 9-1-1.

- Routing of a "911" SMS may be provided to a NENA defined central server for handling and routing to a PSAP. The wireless network operator is not responsible for routing.

- No location information is provided by the originating network or mobile device. Location is subject to whatever is put in the message by the originator and subject to mobile device and other functional element capabilities/limitations.

- No priority or special handling is given to SMS messages.

- SMS to 9-1-1 messages should less than 160 characters in length to eliminate the need for segmentation and reassembly of long SMS messages. Long SMS messages are broken into a sequence of independent messages. Each segment can be delayed resulting in out of order delivery of the messages resulting in confusion, and devices are inconsistent in the way they reassemble long messages.

- No acknowledgments of sent, delivered or read SMS messages are provided (by the originating network).

- No security, authentication, or non-repudiation of any SMS message is provided.

- The originating network will not prevent any spam, SMS spoofing, or denial of service (DoS) attacks on messages delivered to the "911" central address.

- An originating network reserves all rights to protect its network from network spikes, DoS attempts and other congestion issues. This must be part of those liability protections.

- SMS is not a session based protocol. Therefore it is a PSAP (E9-1-1 Authority as applicable) function to “manage” routing of all messages to or from the appropriate PSAP call taker for each SMS message. If there is a series of SMS messages in the exchange between the caller and PSAP call taker, then the PSAP is responsible for association of those messages, ensuring routing to the same call taker if that is their desire, and appropriate routing to another PSAP if applicable. Originating networks do not maintain this association.

    - NOTE: If the caller is moving and crosses PSAP boundaries, messages may be sent to different PSAPs based on caller location, cell site boundaries, etc. Management of messages in this environment is not the responsibility of the originating network. It is not clear how this might work at PSAP boundaries.

1. INTRODUCTION

The purpose of this 4G Americas white paper is to examine the use of Short Message Service (SMS) messaging to 9-1-1 emergency services via Public Safety Answering Points (PSAPs). This white paper will provide the reader with the following information:

- A brief history of SMS
- An overview of how SMS works
- Security aspects and vulnerabilities of SMS
- Identified limitations and shortfalls for SMS based emergency services
- Regulatory considerations related to SMS based emergency services
- Wireless subscriber considerations for SMS based emergency services
- PSAP call taker considerations for SMS based emergency services
- Considerations for the people with disabilities
- Conclusions

The ability for a citizen to be able to send SMS text messages to 9-1-1 emergency services (e.g., PSAP) is a topic that is receiving significant interest and undergoing significant discussions in the emergency services community, the people with disabilities community, and the wireless industry. The term "text" is used in the general sense during these discussions – "text" signifies everything from the short message service (SMS), to instant messaging (IM), to social networks such as Twitter® and Facebook®. Understandably, the people with disabilities community in particular has expressed interest in the SMS text to 9-1-1 functionality on using their existing capabilities of their mobile devices, as an alternative to using specialized bulky, cumbersome add-on TTY devices. The wireless industry fully understands the desires of the people with disabilities community and is focused on finding a good and reliable alternative solution for their needs. This analysis focuses on SMS as a means to contact 9-1-1 emergency services, with a goal to provide a view of the capabilities, limitations, threats and vulnerabilities of such means of communications.

Texting, particularly SMS, has exploded in the past decade. Citizens rely on texting for their social communications needs. There are millions of SMS messages sent each day and there is a perception that SMS is reliable; however, SMS was never designed to be used as a reliable means for life-saving critical communications. SMS was designed to be secondary to voice calls and was never designed to provide the level of communications that citizens have come to expect with voice calls. SMS has several significant limitations and shortcomings which do not make SMS suitable for emergency communications especially under life threatening conditions.

SMS is a text-based messaging service and there is a complementary service called Multimedia Messaging Service (MMS). MMS is a multimedia service which supports a variety of multimedia formats including text, pictures, and video clips. The issues and limitations for MMS based emergency communications are similar to the issues and limitations for SMS based emergency communications.

In August of 2010, the American Red Cross published a paper on Social Media in Disasters and Emergencies[1], and the results indicate a shift in the perception of respondents to how they call for help:

- More than half would send a text message to an available response agency if someone they knew needed help.
- 52% of respondents indicated they would send a text message to a response agency, if available.
- 42% would ask other people to help you reach a response agency through a social network like Facebook® or Twitter®.
- 35% would post your request for help on a response agency's Facebook® page.
- 28% would send a direct message via Twitter® to a response agency.
- 86% would use Facebook® to post information about their safety.
- 69% believe emergency response agencies should regularly monitor their websites and social media sites so they can respond promptly to any requests for help posted there.
- 59% feel they should phone the agency to make sure they have seen the request.
- 18% would try to use digital media to ask for help in an emergency if they could not reach 9-1-1, while 4% would use text messaging to ask for help in an emergency if they could not reach 9-1-1.

CNNMoney.com ranked SMS to 9-1-1 in their "101 dumbest moments in business: Tech", highlighting "(t)he year in shenanigans, skullduggery, and just plain stupidity in the world of technology." SMS to 9-1-1 ranked 26th on that list[2]:

> *26. And maybe the cops come three days later and find you stabbed to death on your kitchen floor.*

The debate on texting to 9-1-1 is intense. The wireless industry (e.g., ATIS, 3GPP, 4G Americas) is working with national public safety organizations (i.e., NENA) to define requirements and make recommendations for a non-SMS based non-voice emergency services (NOVES), within appropriate industry fora. The first issue is improving connectivity to 9-1-1 for the hearing-impaired (e.g., TTY Emulation). Viable text to 9-1-1 solutions for the general wireless customer base will need to wait for next generation 9-1-1 ("NG9-1-1") systems, including major wireless network upgrades. The wireless industry continues to be committed to working constructively with public safety on all NG9-1-1 topics. The wireless industry and public safety will continue to investigate potential solutions as demonstrated with the recent standards study activity that has been initiated in 3GPP.

Public education is essential to making sure that consumers understand that today, voice 9-1-1 is the only reliable way of reporting an emergency and summoning help quickly.

The acronyms and definitions used in this white paper are provided in Appendix A.

[1] See http://www.redcross.org/portal/site/en/menuitem.94aae335470e233f6cf911df43181aa0/?vgnextoid=6bb5a96d0a94a210VgnVCM10000089f0870aRCRD

[2] See http://money.cnn.com/magazines/business2/101dumbest/dumbest_category_tech/index.htm

2. SMS OVERVIEW

This section provides an overview of SMS including discussions on the following:

- The history of SMS
- An introduction to how SMS works including concatenation of SMS messages, SMS interconnection with other networks, and common misconceptions about SMS
- A description of how SMS works for SMS messages originating from the mobile devices, for SMS messages being delivered to SMS devices, and for SMS sent via email
- A description of SMS via email or web clients
- A description of SMS aggregators
- A description of Multimedia Messaging Service (MMS)
- A description of Mobile Instant Messaging (MIM)
- A description of SMS via a generic IP connectivity access method
- A discussion of social networking as related to SMS
- A discussion of example texting services and applications and their associated implications

2.1 SMS HISTORY

SMS was originally designed in the 1980s, before more advanced wireless data services existed. The original intent of SMS was to use spare signaling capacity to provide some basic data transfer and information services. SMS transported messages on the signaling paths needed to control the telephony traffic during time periods when no signaling traffic existed (i.e., during the periods of lowest wireless activities), making productive use of idle channels. Subsequently, SMS was expanded to send short blocks of information such as weather, sports, financial, etc., that were neither time-sensitive nor mission-critical.

Voice calls were considered to be the primary service for mobile devices, and even today with the growth of data services, voice is still the primary service. SMS was designed as a secondary service to use signaling channels and other resources when they were not being used for voice calls. Since SMS is a secondary service, there was no intent to support emergency service capabilities (as was done for voice calls), or high reliability, low delay, real-time 2-way messaging, with location, or security capabilities. As a result, the delivery of SMS messages can be delayed when system resources are needed to handle voice calls. As a consequence, SMS was designed as a store and forward service – if the mobile device or system resources are not available, the SMS message is stored until they became available. Unlike voice calls (which setup an end-to-end path from originator to receiver), SMS messages are stored and handed off between the network entities as they traverse from source to destination. If the delivery of an SMS message to a mobile device fails (e.g., if the mobile device is out of coverage or powered off or for whatever reason unable to receive the SMS), that SMS message is stored in the network for a period of time and the delivery of the SMS message is retried at a future time. An undeliverable SMS message will eventually be deleted by the network based upon the number of retries or based upon the age of the SMS message. Also since SMS is a secondary service, there was no intent to support any level of service such as the emergency service capabilities of voice calls. Therefore, the SMS service is not designed with high reliability, low delay, real-time 2-way messaging, location, or security. Because the SMS service was designed and deployed to use only temporarily-vacant capacity in the networks, wireless operators have always described service/reliability levels as "best efforts only" or equivalent. Subscribers know that SMS messages may be delayed, sometimes for lengthy periods; "Happy New Year" SMS messages can be delayed for many hours or even days; Presidential-candidate Obama used SMS to announce Joe Biden as his VP candidate – this message was delayed 12 hours or more after it was sent at 3:00 AM.

By the time that SMS was deployed in the early 1990s[3], voice call minutes were increasing rapidly every year as people acquired more mobile devices. Even when SMS initiation from mobile devices was added as a service to subscribers, it was considered to be an interesting feature that would have limited usage simply because it was viewed to be much easier to make a phone call than it is to type a limited-character message on a mobile device key pad with only 12 keys.

As the SMS service progressed, some viewed SMS as an alternative to the "beeper" or pagers that were then in widespread use. The capability to receive a short text message on a mobile device became more attractive. But again, this was a one-way non-mission-critical service and did not have the reliability of paging services (which uses a significantly different technology designed for a paging purpose).

However, what was not predicted was the massive shift in social behavior that has occurred over the past few years. Well ahead of mobile devices for teenagers, Instant Messaging on PCs shifted the younger generation away from voice calls to text based communications with its own specialized vocabulary. As mobile devices and wireless plans became cheaper, teenagers started getting mobile devices and started accelerating the usage of text messaging. For example, prior to this major evolution in social behavior, the average wireless subscriber had an average of 0.4 SMS messages per month with the vast majority of subscribers not even using the SMS services.

Today, SMS usage has exploded. In the U.S. in 2009, the number of annualized SMS messages[4] was 1.56 trillion, or 152.7 billion monthly SMS messages. Each one of these billions of SMS messages is contending for that "unused" space, which can be viewed as a funnel:

[3] The first SMS message was sent over the Vodafone GSM network in the United Kingdom on 3 December 1992.

[4] Source: CTIA

Figure 1: SMS Traffic Funnel Diagram

2.2 SMS TECHNOLOGY OVERVIEW

Short Message Service, also known as SMS, is a service originally created in the GSM family mobile communications system, using standardized communications protocols that enable the interchange of short text messages between mobile devices. With SMS becoming so widely used in cellular networks, the term “SMS” is often used as a synonym for any text message or the act of sending a text message, though in reality there could be a number of different methods or protocols being used. In this paper we introduce the 3GPP SMS technology, and use the term “SMS” to refer to 3GPP SMS, not any other text messaging applications such as Instant Messaging.

SMS allows the sending of text messages up to 160 characters in length (including spaces), to and from other mobile devices. SMS is supported in other technologies including cdma2000® networks, as well as satellite and landline networks. Support over multiple technologies allows SMS messages to be sent to mobile devices across networks. Most SMS messages are mobile-to-mobile text messages.

The innovation in SMS is to use the telephony-optimized system to transport SMS messages on the signaling paths needed to control the telephony traffic during time periods when no signaling traffic exists. In this way unused resources in the system can be used to transport SMS messages without additional cost. It is because the SMS messages had to fit into the existing signaling formats is why the SMS message length was limited to 128 bytes, which is roughly 140 alphanumeric characters (using a standard 7-bit coding for each alphanumeric character)[5]. However, later improvement increased the capacity to 140 bytes or 160 7-bit characters. It is the fundamental design of SMS to fit the SMS message into the existing signaling slots, as named "SHORT Message Service."

SMS is implemented in mobile devices and in the network, including radio and core components. SMS requires engineering of the radio capacity and network transport infrastructure to transport the SMS messages, as each control channel can only handle the transmission and delivery of a fixed number of SMS messages per second. SMS requires a network element called a Short Message Service Center (SMSC), or "Message Center" or "Message Service Center" for short. The SMSC is the "store and forward" entity in the SMS network.

As the number of SMS message traffic increases, this extra load on the network requires engineering the signaling capacity and potentially adding more SMSCs. With a large base of SMS capable mobile devices, or to enable every mobile device for SMS emergency service, network capacity needs to be planned accordingly to support the SMS.

The resources dedicated to providing cellular service in a particular area are calculated based on a number of variables. Factors including population density, the expected average length of a phone call and the probability that attempts to use the network will encounter a busy signal or "blocking", are all carefully balanced during this phase.[6]

SMS is a point-to-point service as opposed to a broadcast service. A point-to-point service sends a SMS message from point A to point B, as indicated in the following figure:

[5] See why text messages are limited to 160 characters, Los Angeles Times, http://latimesblogs.latimes.com/technology/2009/05/invented-text-messaging.html

[6] 3G Americas White Paper, "Characterizing the Limitations of Third-Party EAS over Cellular Text Messaging Services," Patrick Traynor, Ph.D., September 2008

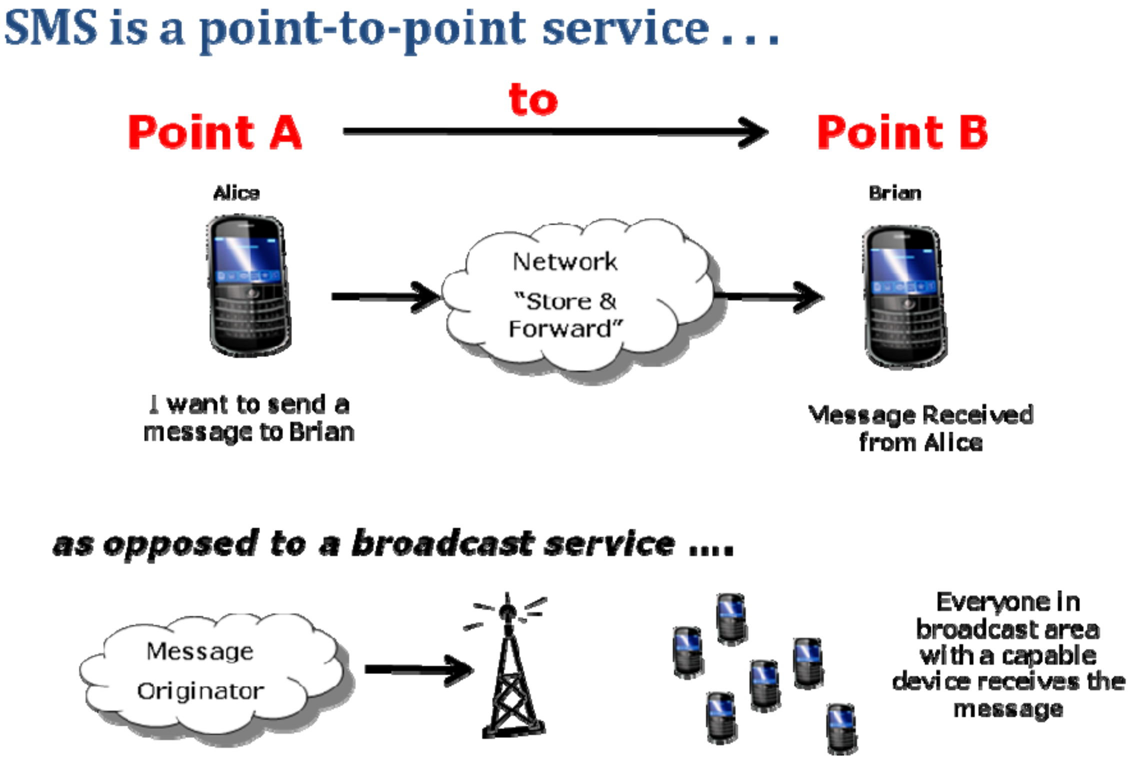

SMS is a point-to-point service . . .
to
Point A
Point B
Alice
Brian
Network
"Store & Forward"
I want to send a message to Brian
Message Received from Alice
as opposed to a broadcast service ....
Message Originator
Everyone in broadcast area with a capable device receives the message

Figure 2: SMS as Point-to-Point Service

A broadcast service also exists in GSM and UMTS and will be used for services such as the Commercial Mobile Alert System (CMAS).

The SMS Point-to-Point service is defined in the 3GPP standard TS 23.040[7]. SMS messages are sent to an SMSC that provides a store-and-forward mechanism to queue the SMS message and forward it to the recipient. If a recipient is not reachable, the SMSC re-queues the SMS message to be re-tried later. Some SMSCs will retry only once (or twice) and then discard the SMS message. SMS message delivery is a "best effort" service; there are no guarantees that a SMS message will actually be delivered to its recipient, and delay or complete loss of a SMS message is fairly common, particularly when sending SMS messages between networks.

An optional feature in the SMS standards (which requires support by the wireless operator network and may be supported by some of the newer mobile devices) enables a user to request confirmation that the SMS message was delivered to its recipients. This trades off the loss of SMS messages with blind re-transmission from the SMS message sender, regardless of the problems this causes and any consideration of network impacts (such as congestion). SMS does not have the ability to handle retransmission in a "good neighbor" way that, in the event of congestion, avoids exacerbating the problem. By contrast, some protocols (such as TCP) have mechanisms that do retransmission with back-off to reduce congestion, and with everyone's SMS messages more likely to get through.

Even though SMS is used extensively by subscribers today, it also is in use by the wireless operator for sending binary content to the mobile device and/or smart card, such as Over-the-Air (OTA) programming or configuration data.

[7] See http://www.3gpp.org/ftp/Specs/html-info/23040.htm

2.2.1 CONCATENTATION OF SMS MESSAGES

Messages longer than what can be sent in this “unused” control channel space can be supported by breaking the message into short segments (which are marked as being linked together but are still sent as individual messages) and re-assembled in the destination mobile device. Segmentation and reassembly is deployed by a wireless operator and must be supported both in the sender’s and recipient mobile devices. This segmentation and reassembly is called “concatenated SMS” messages. An SMS message longer than 160 characters is broken up into smaller segments, each of which can fit into the 160-character field. An additional user data header is added to each segment to provide information to the recipient mobile device for reassemble of the message in the correct order, if that is supported. The receiving mobile device is responsible for reassembling the message and presenting it to the user as one long message. While the standard theoretically permits up to 255 segments, 6 to 8 segment SMS messages are the practical maximum. Each segment of the long message is also treated independently in the transmission, reception, and throughout the network, so delivery to the mobile device in the exact sequence order is not guaranteed.

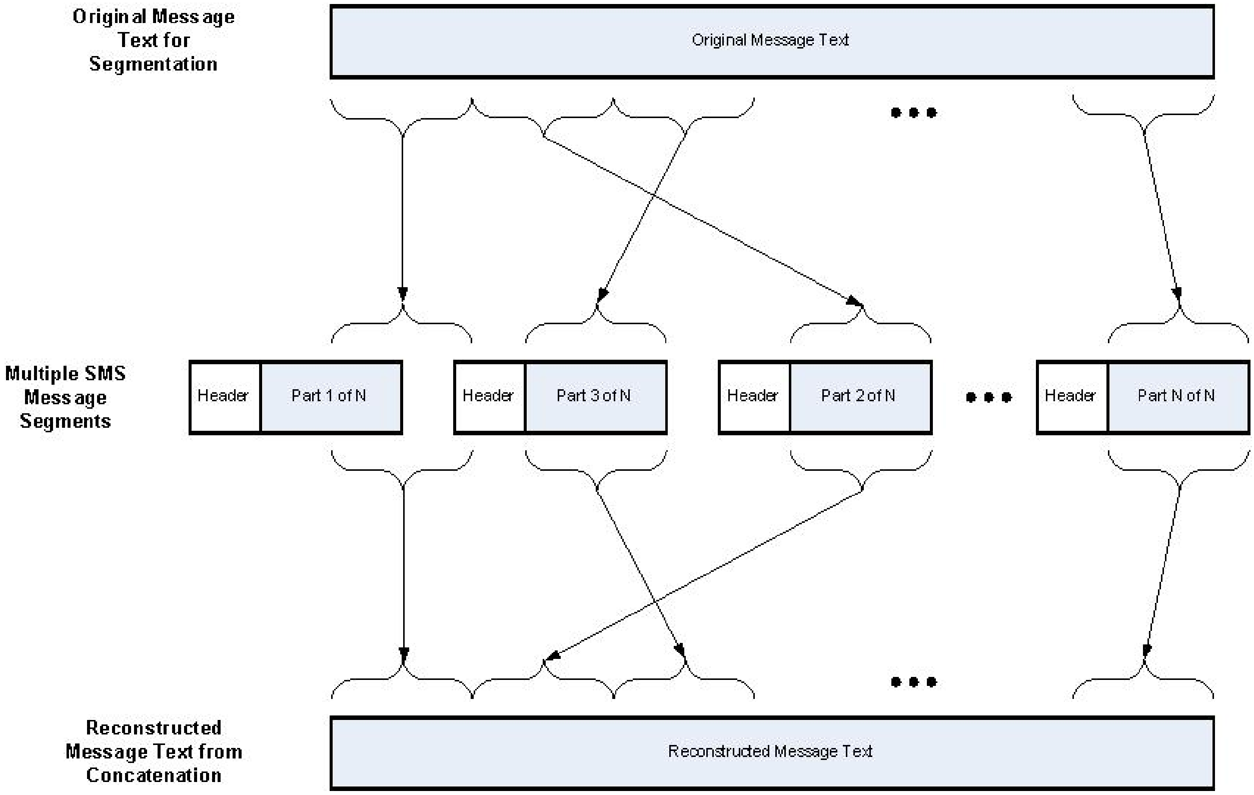

Original Message Text for Segmentation
Original Message Text
Multiple SMS Message Segments
Header
Part 1 of N
Header
Part 3 of N
Header
Part 2 of N
Header
Part N of N
Reconstructed Message Text from Concatenation
Reconstructed Message Text

Figure 3: SMS Message Concatenation

One way of sending concatenated SMS (CSMS) is to split the message into 153 7-bit characters (134 octets of data), and sending each part with a User Data Header (UDH) added to the beginning of the segmented message. The header is used to let the recipient mobile device know how long the header is, a reference number so the recipient mobile device can associate the parts of the message, the total number of parts the message was broken into, and a number sequence indicating where this part falls in the sequence. A sample UDH for a 2-segment message might look like the following:

05 00 03 CC 02 01 [message part 1]

05 00 03 CC 02 02 [message part 2]

2.2.2 INTERCONNECTION WITH OTHER NETWORKS

As described earlier, the original intent of SMS was for a wireless network operator to send information such as a voice mail notification to a subscriber's mobile device. As the service grew, it expanded to provide the capability for sending short text messages between mobile devices. Today, SMS text communications is a service component of phone, web or mobile communications systems, allowing the exchange of short text messages between fixed line or mobile devices.

To achieve this SMS message exchange across networks, Short Message Service Centers must be able to communicate with the Public Land Mobile Network (PLMN) or Public Switched Telephone Network (PSTN) through what are known as Interworking and Gateway MSCs.

When a mobile subscriber originates SMS messages, they are transported from the mobile device, through the cell tower, radio access network (RAN), and Mobile Switching Center (MSC), and on to a Short Message Service Center (SMSC). These "mobile originated' SMS messages may be destined for another mobile user, a, subscribers on a fixed network, or terminated to an "application" also know as a Value-Added Service Providers (VASPs).

SMS messages destined to a subscriber's mobile devices, or "mobile terminated" messages, are transported from the originator (another mobile device, a web site an email client, or a VASP), sent to the SMSC within the destination subscriber's network, through the MSC and cell tower that is presently serving the subscriber's mobile device, and delivered to the destination mobile device. These "mobile terminated" SMS messages may originate from mobile user, from fixed network subscriber (e.g., Internet or email), or from other sources such as VASPs. VASPs which provide the content may submit the SMS message to the wireless operator's SMSC using a TCP/IP protocol such as the Short Message Peer-to-Peer (SMPP) protocol or the External Machine Interface (EMI).

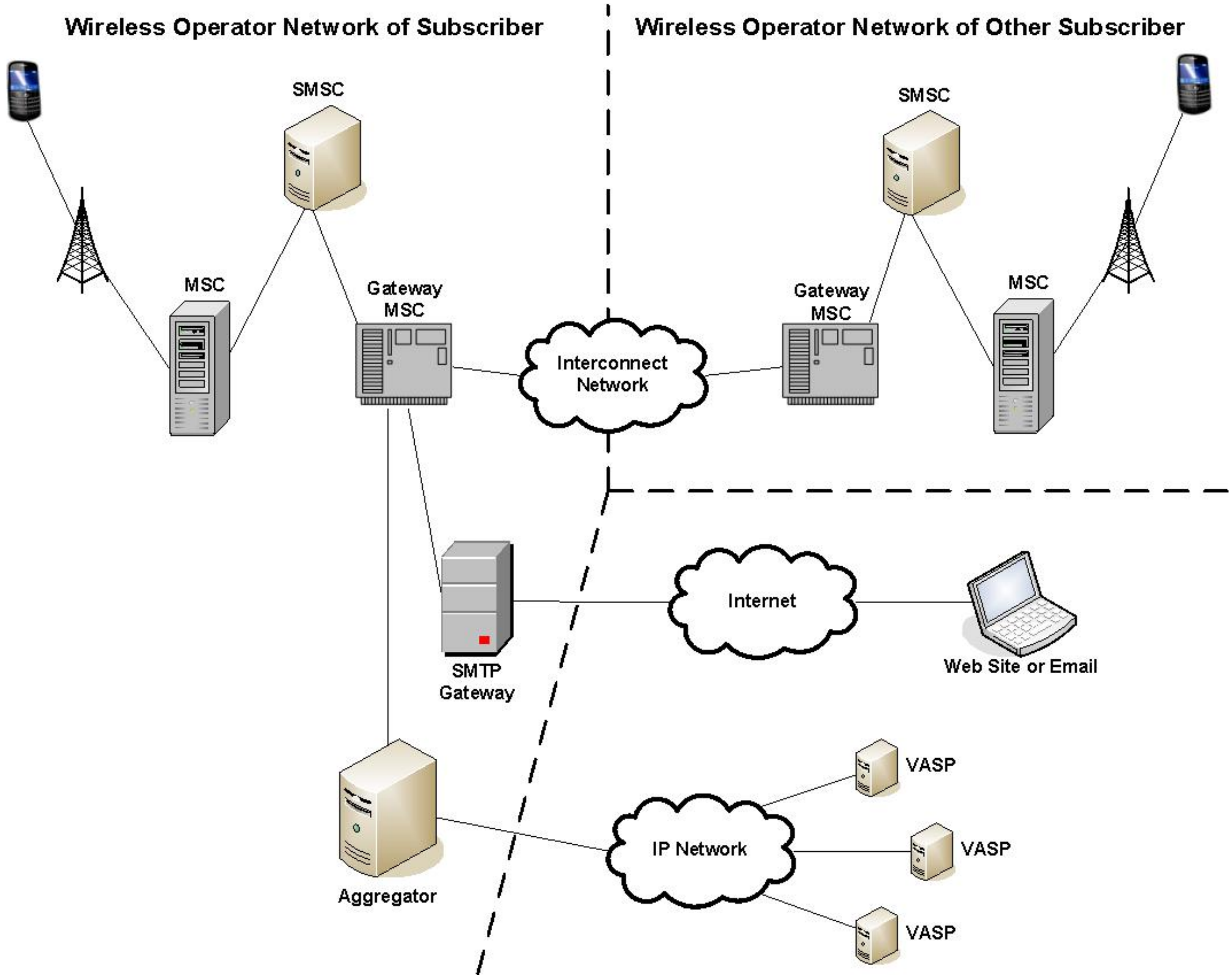


Figure 4: Network Interconnection Architecture

Mobile-to-Mobile SMS messages are sent to the destination mobile device's 10-digit phone number, e.g. 555-555-5555. However, it may be difficult for a subscriber to remember 10-digit phone numbers for value added services or other non-mobile destinations. To help with this, "short codes" have been developed. These allow a VASP to obtain a short code from the wireless operator, and subscribers send texts to that number instead of a 10-digit phone number. When a mobile subscriber originates the SMS message and uses a short code, it is sent to the SMSC, and the SMSC identifies the Short Code as a special or premium service. The SMSC will then direct the content of the text message to the VASP or other service indicated by the short code, typically using an IP protocol such as SMPP or EMI.

The standard lengths for interoperable short codes are five and six digits. Wireless operators use short codes with fewer digits for carrier-specific programs - e.g., "Text 611 to see how many minutes you have remaining on your plan." Codes starting with 1 are not permitted. Common short codes in the U.S. are administered by NeuStar, under an arrangement with Common Short Code Administration - CTIA[8].

Some wireless operators allow non-subscribers the ability send SMS messages to a subscriber's mobile device using what is known as an Email-to-SMS gateway, or may provide the capability to send the SMS message from the

[8] See http://www.usshortcodes.com/csc_press053106.html

wireless operator's website. Many third party websites also offer the capability to send SMS messages to any subscriber through these interfaces; examples of such services are news, weather, and "alert" information sources. For example, an AT&T subscriber whose phone number is 555-555-5555 may receive an SMS message on their mobile device when the sender initiates an email to 5555555555@txt.att.net; this can be done from any source for generating an email. The AT&T subscribers can then reply to this SMS message and the SMS reply is sent back to the original email address of the sender.

2.2.3 SMS MISCONCEPTIONS

The following are some of the common SMS misconceptions that hopefully will be cleared in this paper:

Misconception #1 → Cellular networks constantly keep track of the location of mobile devices

> **FALSE** – All that is known is which MSC and which paging area to try

Misconception #2 → SMS operates over a "separate network"

> **FALSE** – The radio resources are the same, the backhaul is the same, and the signaling network is the same

Misconception #3 → SMS is a reliable, real-time service

> **FALSE** – SMS is a store & forward (non-real-time) best effort service

Misconception #4 → SMS is a two-way session-based service

> **FALSE** – SMS is not session based, and is a one-way point-to-point service

Misconception #5 → SMS can provide 9-1-1 location accuracy

> **FALSE** – SMS cannot provide the location accuracy of a 9-1-1 call because the mobile is on the control channel for a short period of time (network-based TDOA requires up to 30 seconds of measurements on a traffic channel to get required accuracy).
>
> Note also that while some mobile devices have built-in GPS or Assisted GPS where the network assists the mobile device in finding satellite signals that are weak (such as indoors), the GPS is not actively tracking the mobile device and locating the mobile device can still take up to 30 seconds.

Misconception #6 → A cellular network can handle every subscriber that wants to make a call or send a text message simultaneously.

> **FALSE** – The capacity of the cellular network is limited by many factors including the spectrum available. Networks are engineered to handle expected traffic loads at the busiest time of the day, and are physically not able to support every subscriber simultaneously.

2.3 HOW SMS WORKS

As previously discussed, there are two types of point-to-point SMS service: Mobile-Originated-Short Message (MO-SM) service and Mobile-Terminated-SM (MT-SM) service. The architecture and message flow for each are highlighted below.

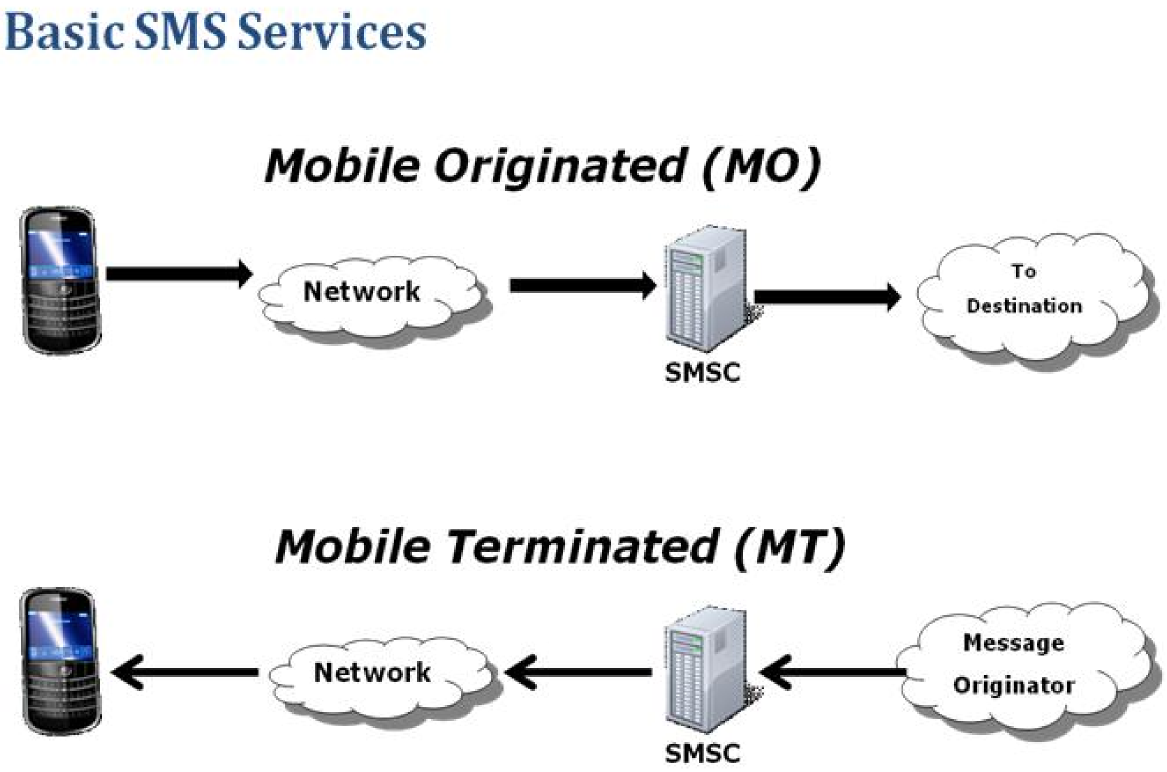


Figure 5: Basic SMS Services

A MO-SM is sent by a subscriber from the mobile device and transported across the cellular network to an SMSC. In a MO-SMS scenario, the originator (“Brian”) has a message to send (“Hi Alice I’ll meet you at Starbucks”). Brian opens the SMS application on his mobile device, types in the message, and “sends” the message. Once Brian’s mobile device gains access to the control channel on the cell tower serving it, the mobile device notifies the network he has a message to send, and the MSC authorizes the ability for Brian’s mobile device to send the message. Brian’s message is then sent as an SMS message over the control channel being used on the cell tower and on to the MSC. The MSC then forwards Brian’s SMS message to the SMSC; the address of the SMSC is provisioned in Brian’s mobile device Subscriber Identity Module (SIM) and that SMSC is located in Brian’s home wireless operator’s network, regardless of what network may be serving Brian at the present time. If Brian was roaming into another wireless operator network outside his home wireless operator’s network, then the MO text message is routed to Brian’s home wireless operator’s SMSC, no matter where in the world that SMSC is located. The SMSC has no knowledge of Brian’s location other then the identity of the particular MSC it received the SMS message from (and since each MSC serves many cell towers over a wide geographic area, an MSC provides no real geographic location of the subscriber). The SMSC acknowledges to the MSC that it received the SMS message, and it is now up to the SMSC to figure out who and where “Alice” is and how to forward that SMS message on to her.

Brian is only aware that the SMS message may have left his mobile device, and has no indication of where it is or what the status of the delivery is.

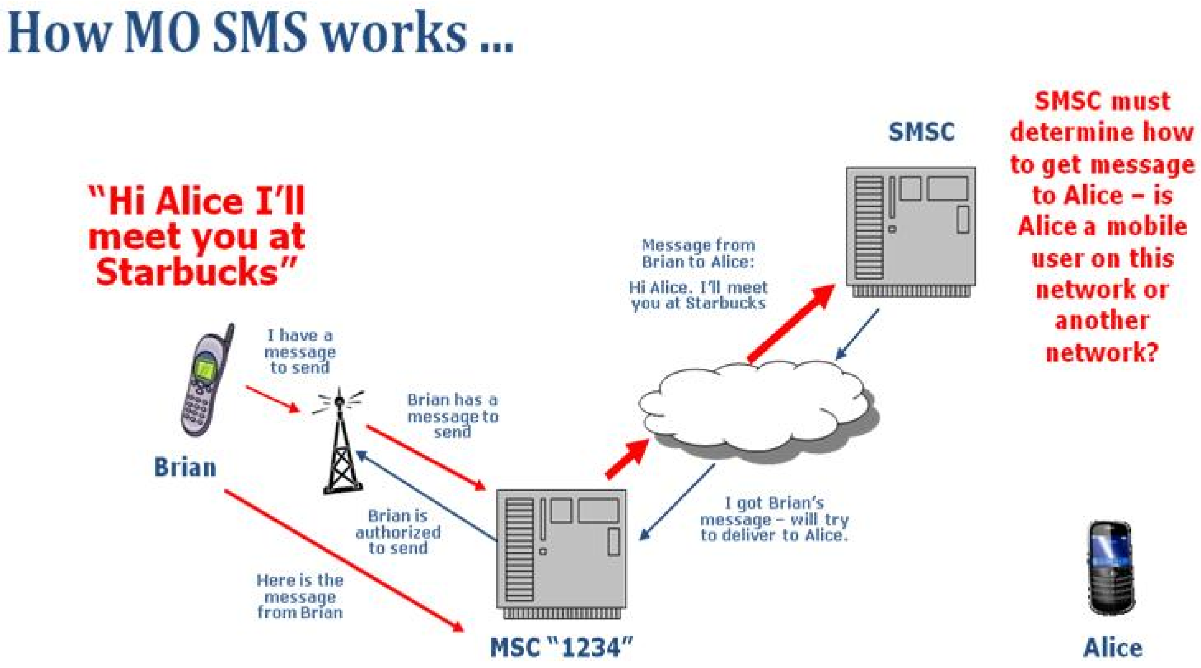
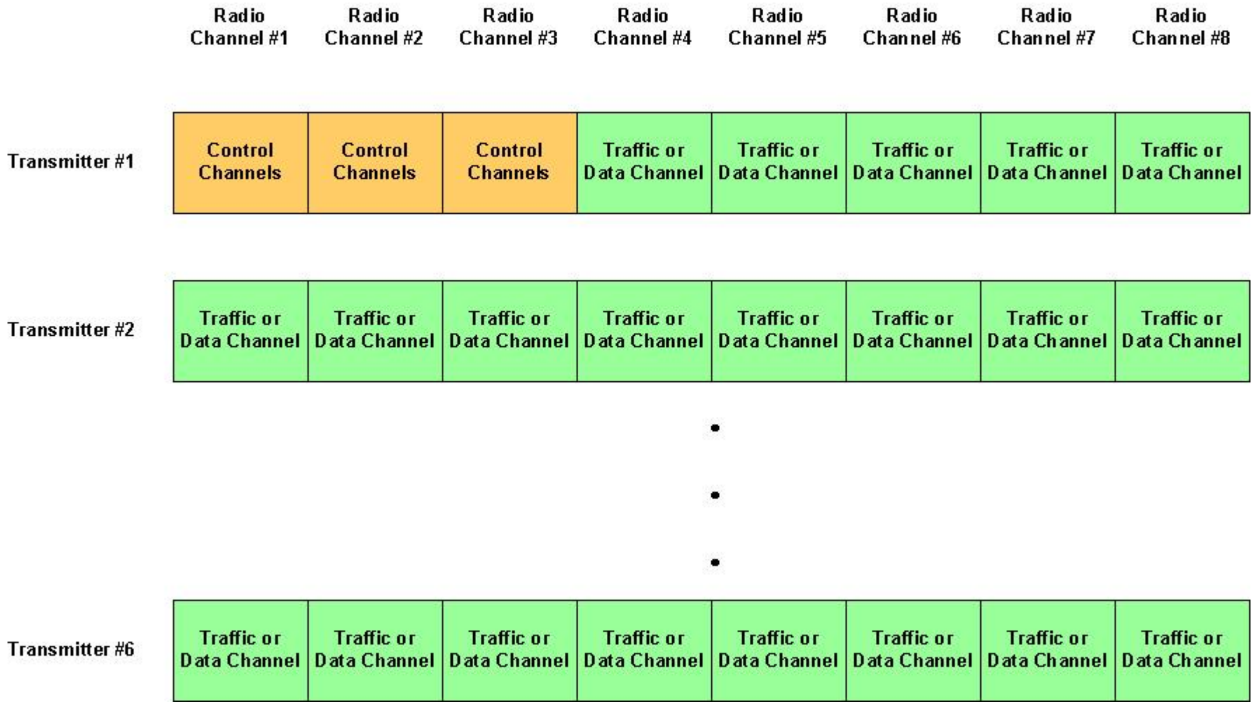

How MO SMS works ...
"Hi Alice I'll meet you at Starbucks"
SMSC
SMSC must determine how to get message to Alice – is Alice a mobile user on this network or another network?
Message from Brian to Alice:
Hi Alice. I'll meet you at Starbucks
I have a message to send
Brian
Brian has a message to send
Brian is authorized to send
Here is the message from Brian
I got Brian's message – will try to deliver to Alice.
MSC "1234"
Alice

Figure 6: Mobile Originated SMS

How does Brian inform the network "I have a message to send"? To understand this, it is important to understand the three basic types of channels in a cellular system – the "control channel", the "traffic channel", and the "data channel". Control Channels (CCH) are used for signaling between cell tower "base stations" and mobile devices. Control channels are used to deliver SMS messages when the mobile device is not engaged in a phone call. Traffic Channels are used to deliver voice traffic to the mobile device, and data channels are used to deliver data to the mobile device. A wireless operator needs to engineer the limited number of channels it has available ("spectrum"). Each wireless operator is allocated a portion of the total frequency band. There is not enough spectrum ("channels") available to allow everyone who has a mobile device to make a voice call or send a text message all at once. The wireless operator's engineering is based on "busy hour" network planning, and the wireless operator deploys transmitters and receivers in the available frequency band into each cell site, and divides these into control, traffic and data channels, as illustrated below:



	Radio Channel #1	Radio Channel #2	Radio Channel #3	Radio Channel #4	Radio Channel #5	Radio Channel #6	Radio Channel #7	Radio Channel #8
Transmitter #1	Control Channels	Control Channels	Control Channels	Traffic or Data Channel	Traffic or Data Channel	Traffic or Data Channel	Traffic or Data Channel	Traffic or Data Channel
Transmitter #2	Traffic or Data Channel	Traffic or Data Channel	Traffic or Data Channel	Traffic or Data Channel	Traffic or Data Channel	Traffic or Data Channel	Traffic or Data Channel	Traffic or Data Channel
				• • •				
Transmitter #6	Traffic or Data Channel	Traffic or Data Channel	Traffic or Data Channel	Traffic or Data Channel	Traffic or Data Channel	Traffic or Data Channel	Traffic or Data Channel	Traffic or Data Channel

Figure 7: Example Channel Configuration

An idle mobile device is monitoring control channels from the cell tower waiting for phone calls, SMS messages, or other system activity. When Brian makes or receives a call, the mobile device is switched over to a "traffic" channel; if engaged in a data session, the mobile device is on a "data" channel. When Brian types in a message and hits "send," the MO-SMS sends the data on the control channel, effectively holding the channel for up to 4-5 seconds (as opposed to a voice call that "holds" a traffic channel for several minutes or more). This short "hold time" of the control channel when sending an MO-SMS is why there is a greater chance of getting a MO-SMS through in a congested network, but this is not guaranteed!

Brian's mobile device may also send or receive an SMS while on a "traffic channel" through what is known as an associated control channel that exists on the traffic channel if the network and handset support it.

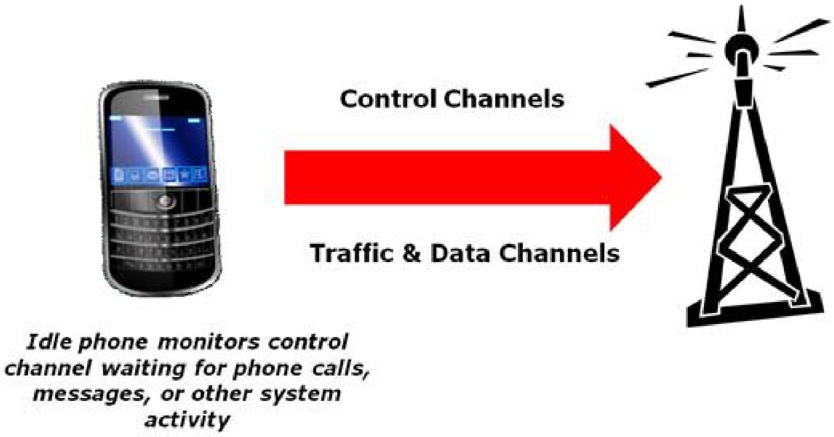

Control Channels
Traffic & Data Channels
Idle phone monitors control channel waiting for phone calls, messages, or other system activity

Figure 8: Mobile Device Channels

On 3G UMTS networks, services are assigned a Quality of Service (QoS) classes for four types of traffic:

- Conversational class (voice, video telephony, video gaming)
- Streaming class (multimedia, video on demand, webcast)
- Interactive class (web browsing, network gaming, database access)
- Background class (email, SMS, downloading)

SMS is sent in the "background" class as it is low priority, non-real-time traffic.

So in the scenario, how do we know where Alice is? Alice could be a subscriber of any wireless operator, roaming on any network in the world, or can be a fixed network email account, or a VASP.

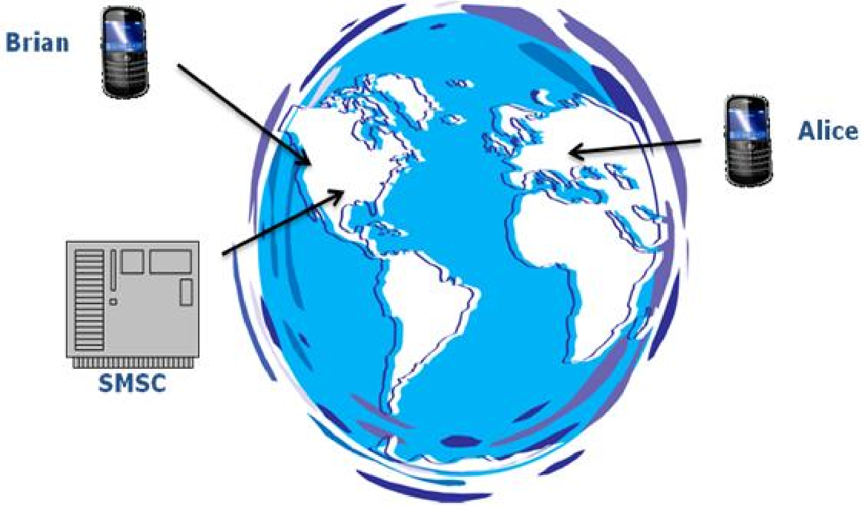


Figure 9: Where's Destination Mobile Device?

For this scenario, assume Alice is using another mobile device. In this case, the delivery of Brian's message to Alice will be a MT-SM that is transported from an SMSC, across the cellular network, and delivered to a mobile device so that it can be viewed by a subscriber.

But how do we find Alice? The simplest case is when both Brian and Alice have the same wireless network operator; in this case, Brian's SMSC also knows about Alice, and can begin to "find Alice" directly. The SMSC in this case will query another network entity known as the "Home Location Register" or HLR, and ask essentially "Where is Alice?" If Alice's mobile device was on the network recently, the MSC serving Alice will have notified the HLR of Alice's whereabouts (down to the MSC level). The HLR can then report back to the SMSC that "Alice last checked in on MSC xyz". The SMSC will then forward Brian's SMS message to MSC xyz and ask it to deliver Brian's SMS message to Alice, who is believed to be on a cell site within MSC xyz's control, and the MT-SMS process will begin.

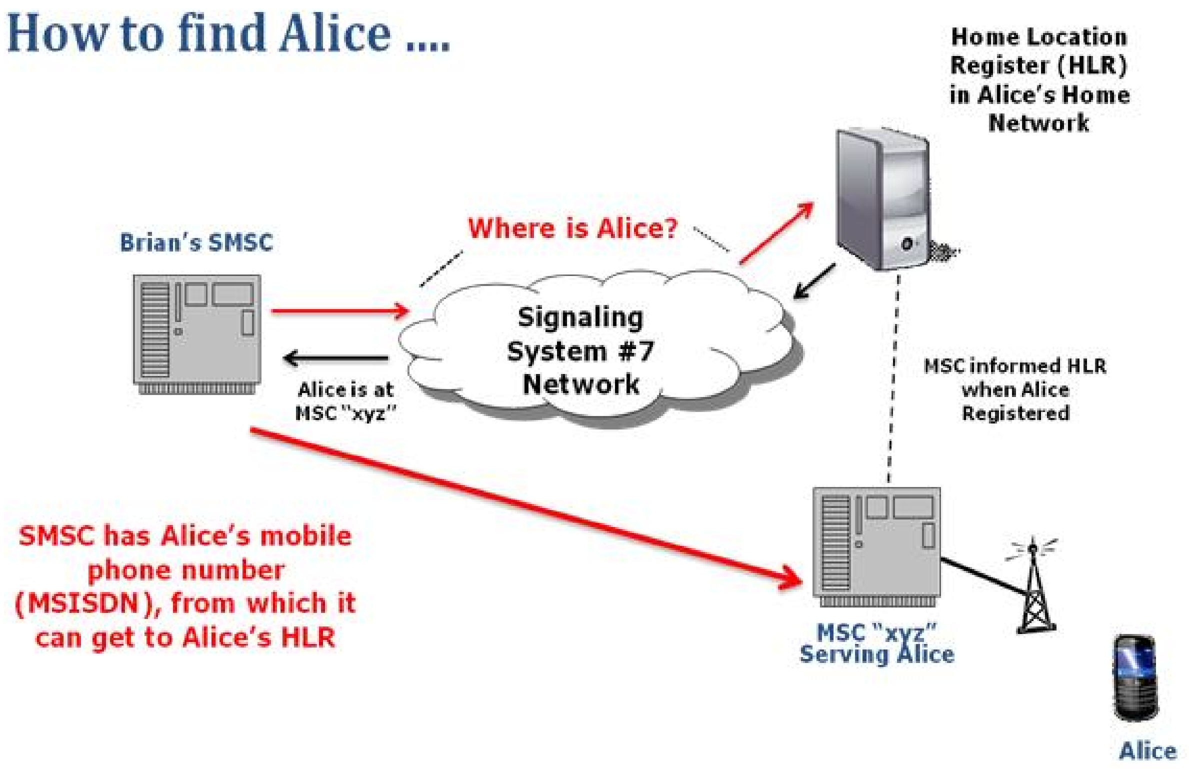

How to find Alice ....
Home Location Register (HLR) in Alice's Home Network
Brian's SMSC
Where is Alice?
Signaling System #7 Network
Alice is at MSC "xyz"
MSC informed HLR when Alice Registered
SMSC has Alice's mobile phone number (MSISDN), from which it can get to Alice's HLR
MSC "xyz" Serving Alice
Alice

Figure 10: Find Destination Mobile Device

If Alice and Brian are not served by the same wireless network operator, finding Alice becomes more complicated. In this case, Brian's SMSC has no knowledge of Alice other then Alice does not receive service by the same wireless network operator as Brian. Brian's SMSC passes his SMS message off to another entity known as the Gateway-SMSC, or G-SMSC. The G-SMSC can determine from Alice's phone number which wireless network operator provides service to Alice, and forwards Brian's SMS message to the Gateway MSC (G-MSC) of the wireless network operator providing Alice's service. The G-SMSC in Alice's home network forwards Brian's SMS message to the SMSC serving Alice. Alice's SMSC then goes through the query of the HLR to identify the MSC where Alice was last reported.

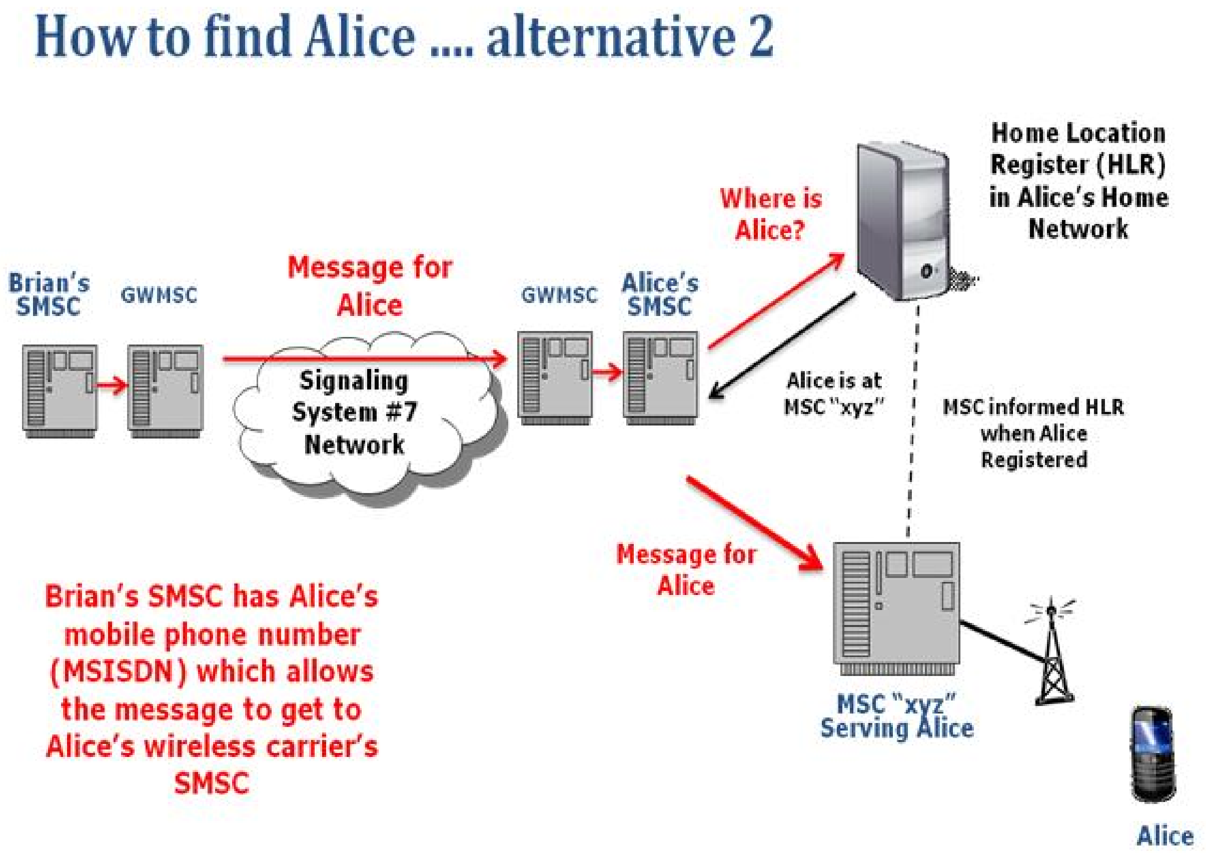

How to find Alice .... alternative 2
Brian's SMSC
GWMSC
Message for Alice
Signaling System #7 Network
GWMSC
Alice's SMSC
Where is Alice?
Home Location Register (HLR) in Alice's Home Network
Alice is at MSC "xyz"
MSC informed HLR when Alice Registered
Message for Alice
Brian's SMSC has Alice's mobile phone number (MSISDN) which allows the message to get to Alice's wireless carrier's SMSC
MSC "xyz" Serving Alice
Alice

Figure 11: Find Destination Mobile Device Alternative #2

If “Alice” (the destination of the MO SMS) is not another mobile device, but a short code, the destination address short code is translated in the home wireless operator’s SMSC to an address where the SMS message is routed for handling the service. Thus, if Alice’s SMSC does not understand the short code used in the roamed-into area, the SMS message may get lost since Alice’s SMSC will not know where to route it. Or worse – if there is the short code used for another service by Alice’s home network, the SMS message will get routed to the wrong destination. This is an important point if a short code is proposed for use for SMS to 9-1-1; there must be consistency across all wireless operators and networks or confusion and potential misrouting of SMS messages will be the result.

When an SMS is delivered to a mobile device, it uses the MT-SMS process. To demonstrate the MT-SMS process, assume Alice desires to send the message “I’ll meet you at 3 pm at Starbucks” to Brian using the previously described MO-SMS process. The SMS message will arrive at Brian’s SMSC as previously described. Brian’s SMSC must now find out if Brian is available on the network, and if so, where? Brian’s SMSC sends a signaling message to Brian’s HLR asking “Where is Brian?” If Brian was recently on the network, the HLR knows which MSC Brian last reported from. That MSC number, “MSC 1234” in this case, is reported back to the SMSC. The SMSC then forwards the SMS message to the indicated MSC, indicating that the SMS message is destined for Brian. However, a single MSC typically has control of a large number of cell towers within a large geographic area. Which cell tower is Brian currently on, especially since in a mobile environment he could be moving from tower to tower? This is the same problem as if a voice call was to be delivered to Brian – he could be on one of a number of cell towers in the area.

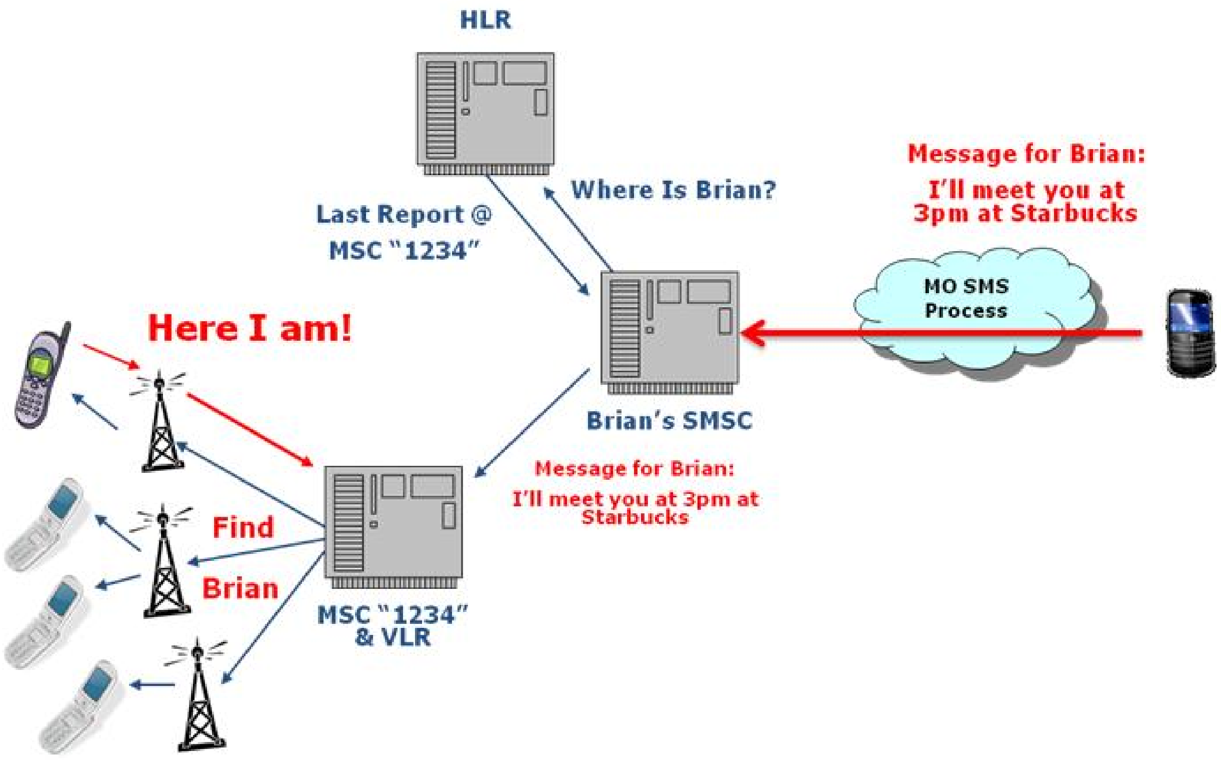


Figure 12: Finding Mobile Device for Mobile Terminated SMS

The method used to locate the particular cell tower Brian is located on is through a process known as "paging." This process is the same whether the MSC is delivering a phone call to Brian, or delivering an SMS message. This is a key point – the same network and radio resources are used in this process regardless of whether this is a phone call or SMS delivery; however, the paging process is prioritized so voice calls are processed first. In a network under high traffic loads, SMS messages will be delayed by design. Also, there are a limited number of paging channels available, based on network engineering of the available spectrum. During extreme busy hour conditions, there may not be enough paging channels to handle both the voice traffic and the SMS traffic. In this event, calls and SMS messages are not delivered and the SMS messages are stored in the SMSC for later retry.

"MSC 1234" sends a message out on a number of cell towers to "find Brian"; this is a "page" message. This paging process starts initially at a group of cell towers in Brian's last known "location area", and if Brian does not answer, the MSC sends out the page to larger areas until either Brian is found, or the MSC assumes Brian is no longer available and gives up. If Brian's device "hears" the page, his device essentially returns a "Here I am!" message to the MSC. The MSC now knows which cell tower Brian is on.

Once Brian's mobile device is located on a particular cell tower, the MT-SM message is delivered to the mobile device. There is a physical limit on the rate at which MT SMS messages can be delivered on the radio channels available – a typical "rule of thumb" rate at which the actual MT SMS message may be delivered is 2 SMS messages per second per sector. If there are a large number of SMS messages going to subscribers on a single tower/sector, SMS messages will be backed up and processed in order until they are delivered.

If Brian's mobile device acknowledges the SMS message was received, the MSC acknowledges to Brian's SMSC that the SMS message was delivered and the SMSC does not have to worry about retrying to deliver the SMS message later.

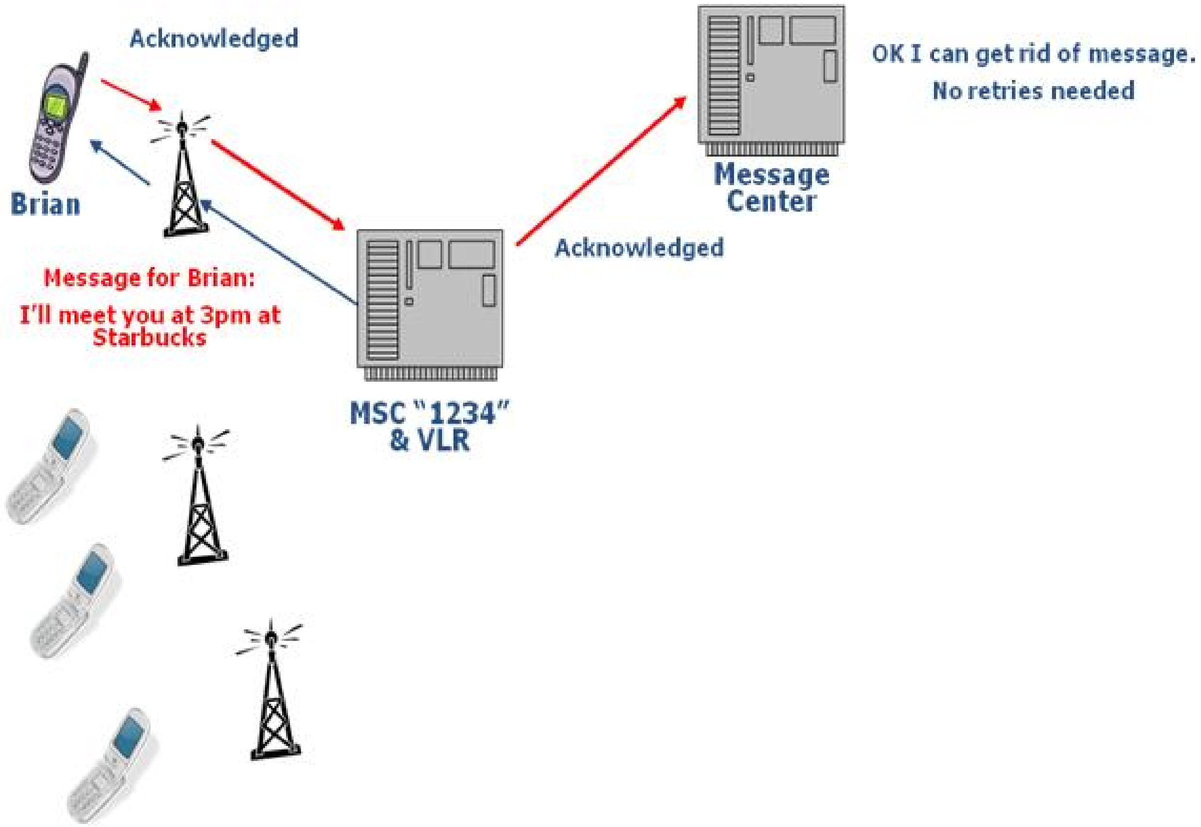


Figure 13: Delivery of Mobile Terminated SMS

Note that no acknowledgment is sent back to Alice so Alice has no indication that Brian received the SMS message.

What happens if Brian's device cannot be found? Brian's device may not respond to the page because of a number of reasons including:

- He is in a poor radio coverage area
- He moved outside the paging area
- He turned off his mobile device
- The cell site is congested with voice call pages

If Brian's mobile device does not respond to the page, an indication is sent to the SMSC that the SMS message was not delivered and is "stored" for later retry – recall by design SMS is a "store & forward" system. The retry period is variable and depends on network configuration, and each retry goes through the same "paging" process. If Brian's mobile device cannot be found after several retries, then the SMSC gives up, stores the SMS message, and asks the HLR to inform it when Brian's mobile device is available on the network. After a period of time, the SMSC may give up entirely and delete the SMS message from it queue. Alice has no indication that this has happened.

An SMSC is able to send only one MT-SM to a subscriber address at a time. The mobile device is able to receive one MT-SM and send one MO-SM at a time.

The following sections describe the SMS signaling flow in more detail.

2.3.1 MOBILE ORIGINATED SMS

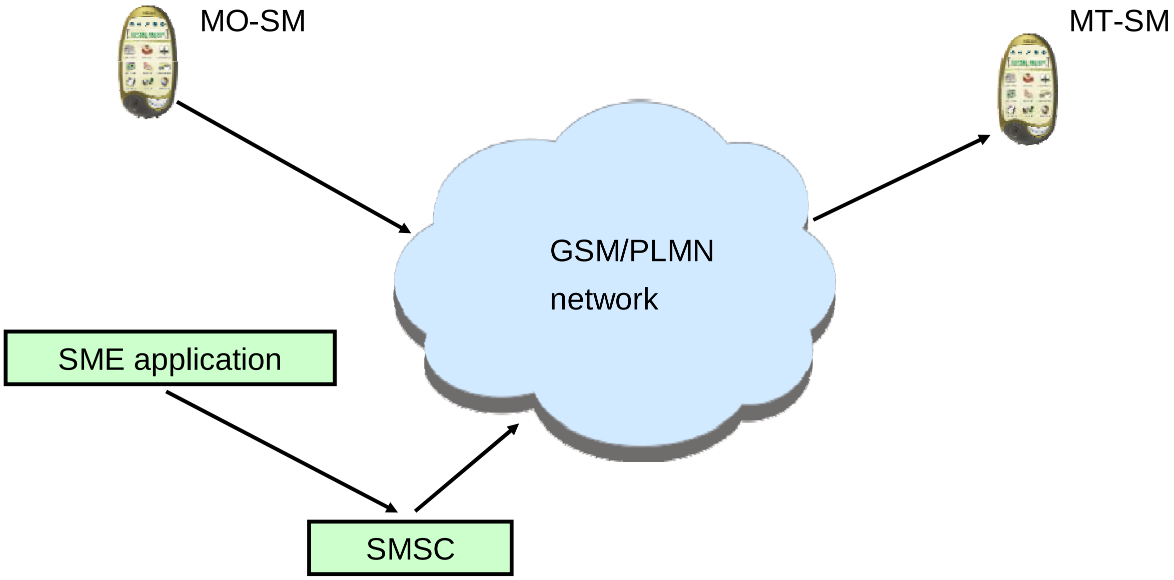


Figure 14: SMS System Diagram

A subscriber can originate a short message to another subscriber even when the recipient's mobile device is switched off or is not reachable. The sender is not sent an acknowledgment when the SM arrives at the recipient. The SM is sent independently of the voice service. SMs can be sent and received during voice calls, but it takes more time.

The following figure depicts the flow of an MO-SM case:

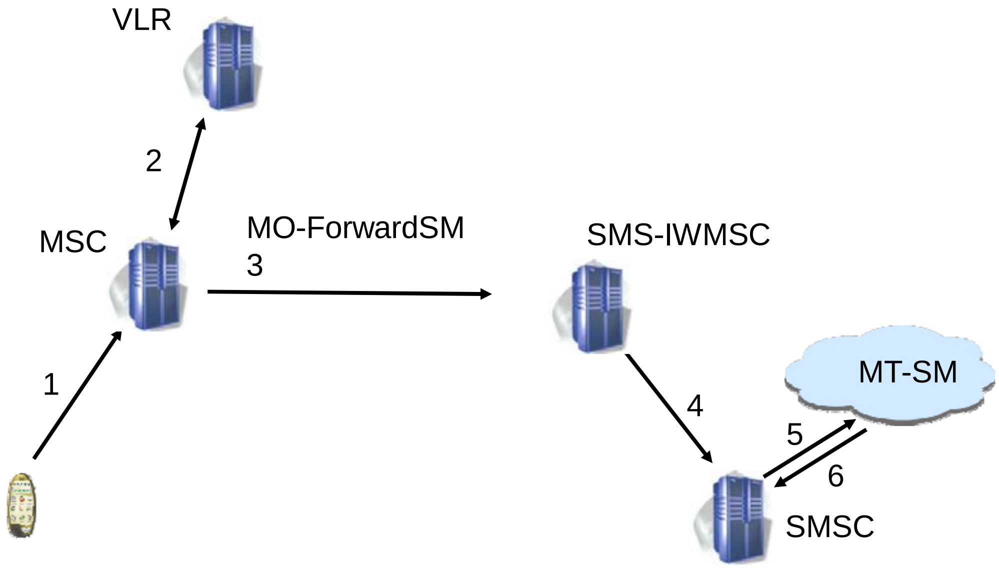


Figure 15: Mobile Originated Short Message Service

1. The mobile device sends an SM via the control signaling channel on the radio interface; the SM includes the address of the SME where the SMSC eventually attempts to forward the SM.
2. The serving MSC checks the data of subscriber from the VLR.
3. The MSC routes the SM to SMS-IWMSC (Interworking MSC).
4. The SM is routed via a special OSI or TCP/IP application to the SMSC.
5. SMSC stores the SM and tries MT-SM when the recipient terminal is connected.
6. MT SM provides SMSC the delivery report to SMSC for any retransmission if needed.

2.3.2 MOBILE TERMINATED SMS

The following figure depicts a MT-SM case:

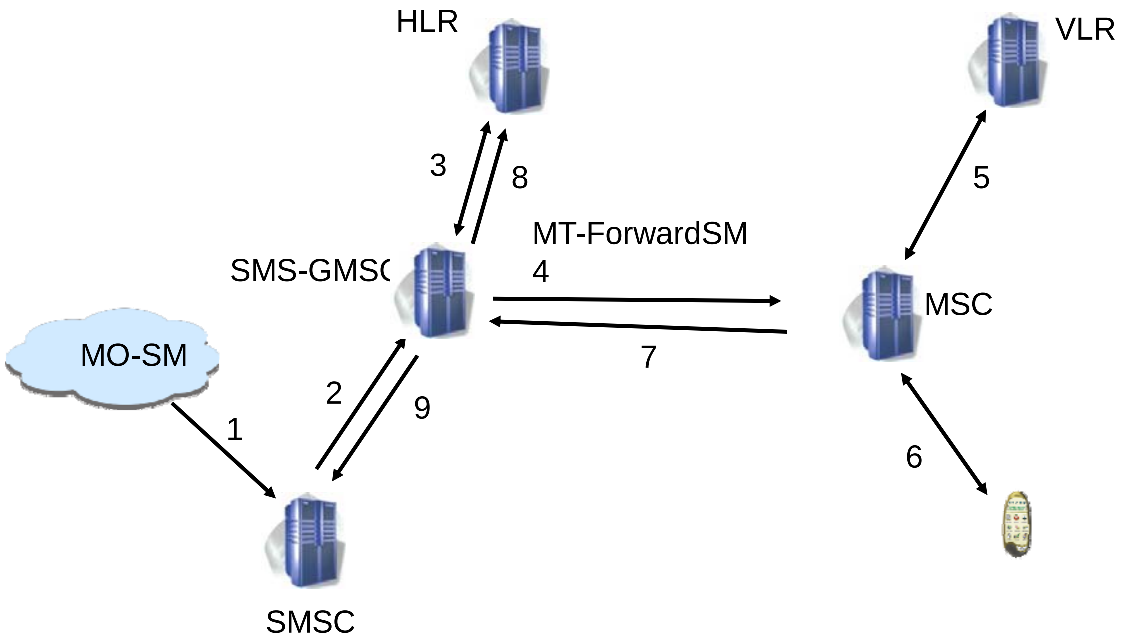


Figure 16: Mobile Terminated Short Message Service

The SMSC receives the short message over the MO-SM service, stores the SMS message, and forwards it to the recipient over the MT-SM service.

The message flow is depicted as below:

1. MO-SM sends the SM to the SMSC.
2. The SMSC sends the SM to the SMS-GMSC.
3. The SMS-GMSC requests the VMSC or SGSN address from the HLR.
4. The SMS-GMSC routes the SM to the VMSC/SGSN.
5. The VMSC asks the VLR for the status and location area of the MS of the recipient.
6. If the recipient is in idle mode, the VMSC starts paging and delivers the SM to it through the control signaling channel of the base station. If the recipient is in busy mode, the VMSC sends the SM through the control channel. The recipient sends a delivery report to the VMSC after receiving the SM.

7. The VMSC sends the delivery report to the SMS-GMSC using global title analysis to find the routing address of the SMSC.
8. If needed, the SMS-GMSC sends the delivery report to the HLR.
9. The SMS-GMSC sends the delivery report to the SMSC either confirming that the MS has received the SM or informing the SMSC the cause why the delivery failed.

No delivery acknowledgement is supported from the SMSC towards the SM sender since there is no signaling mechanism available from the MO-SM.

2.3.3 SMS VIA EMAIL OR WEB CLIENTS

SMS messages may also be initiated from an email client, such as Microsoft Outlook®, or from a web page. Email-initiated SMS uses a protocol called SMTP[9] (Simple Mail Transfer Protocol), which can deliver emails as text messages via SMTP gateways at the entry point into the wireless operator's network. SMTP is a standard for supporting email across IP networks, for example, the Internet. SMTP gateways were never intended to support urgent or time-critical messaging and are not capable of delivering the level of reliability and performance suited to notification services. There is no formal relationship between the sender of the SMS message and the wireless operator when SMS messages are sent to the SMTP Gateway.

There are also add-ons for email programs such as Microsoft Outlook® that facilitate the sending and receiving of SMS messages directly from the email client, as well as web clients that allow sending and receiving SMS messages using a web browser. Instant Messaging applications such as Windows Live Messenger® and Yahoo! Messenger® also support the ability to send and receive SMS messages.

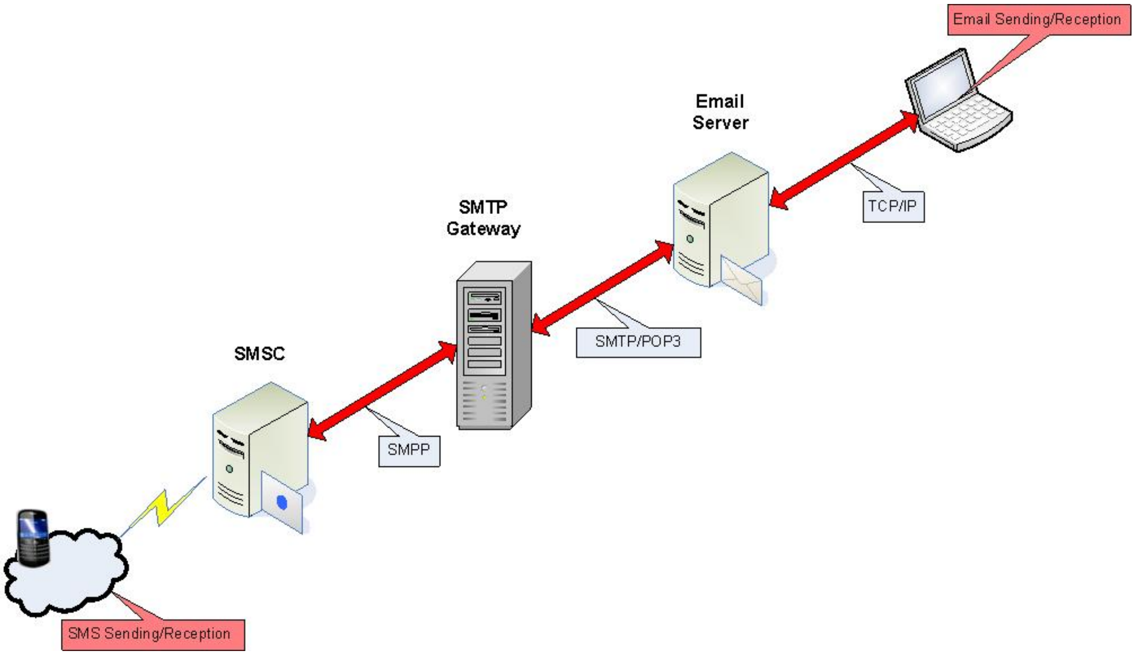


Figure 17: SMS via Email

[9] See IETF RFC 5321, http://tools.ietf.org/html/rfc5321

To initiate an email to SMS, the sender constructs an email message with an address constructed from the 10-digit phone number and the domain name for the email gateway of the wireless operator. The domain names are published by the wireless operators and are readily available on the Internet. An example of an address to an AT&T mobile device is 5555555555@txt.att.net. Email to SMS can also be used to send SMS messages internationally.

As described later, SPAM is a huge concern for wireless operators. SMTP messaging gateways are the target of millions of SPAM messages each day. A significant percentage of SMS requests via email are SPAM. Wireless operators are aggressively managing this problem through sophisticated SPAM detection & filtering. Since there is no formal relationship between the SMS message sender and the wireless operator, SMS messages sent via the SMTP Gateway may be prone to filtering, especially if they appear to be SPAM.

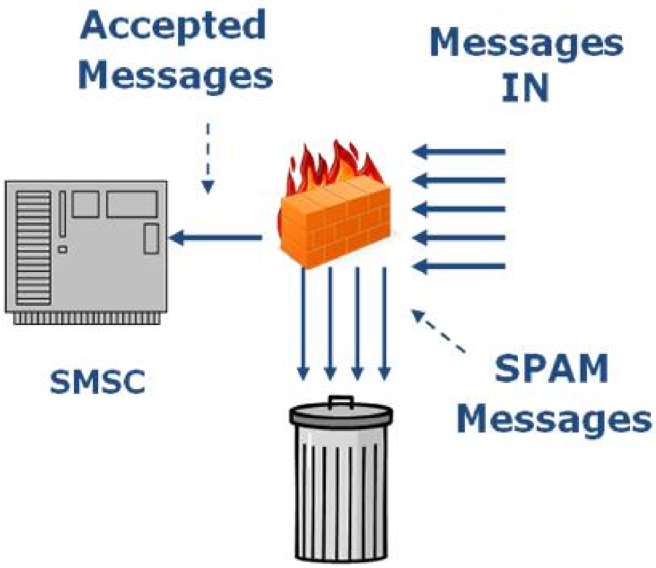


Figure 18: SMS SPAM via Email

2.3.4 SMS AGGREGATORS

Typically, SMS content providers do not connect to a wireless operator network directly, and an SMTP Gateway has challenges especially if the content provider's message has the characteristics of SPAM. Another type of SMS gateway is known as an SMS broker or aggregator. An SMS aggregator provides connectivity with wireless operators by offering a gateway to both send and receive messages and other multimedia or digital content. The aggregator model is based on business agreements between SMS content providers, the aggregator, and the wireless operator. An aggregator is a business entity that negotiates agreements with wireless operators and acts as a middleman providing access to a cellular network for third parties who have no direct relationship with the wireless operator[10]. An SMS aggregator has direct connections to most wireless operators to deliver text messages through their gateways. Such gateways are necessary because it is virtually impossible to connect directly to the wireless operators as a single company. An aggregator can enable the sending of bulk traffic and may also manage the "rental" of short codes to the content providers.

[10] See Jeff Brown, Bill Shipman, Ron Vetter, "SMS: The Short Message Service," Computer, vol. 40, no. 12, pp. 106-110, Dec. 2007, doi:10.1109/MC.2007.440

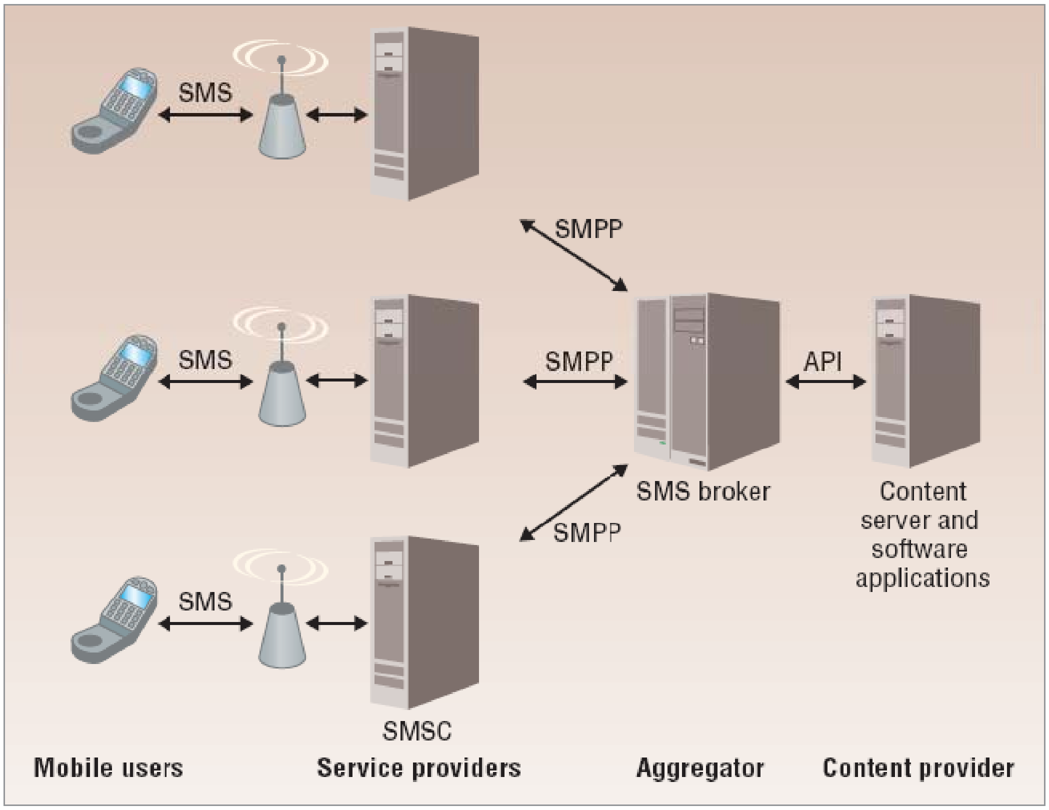
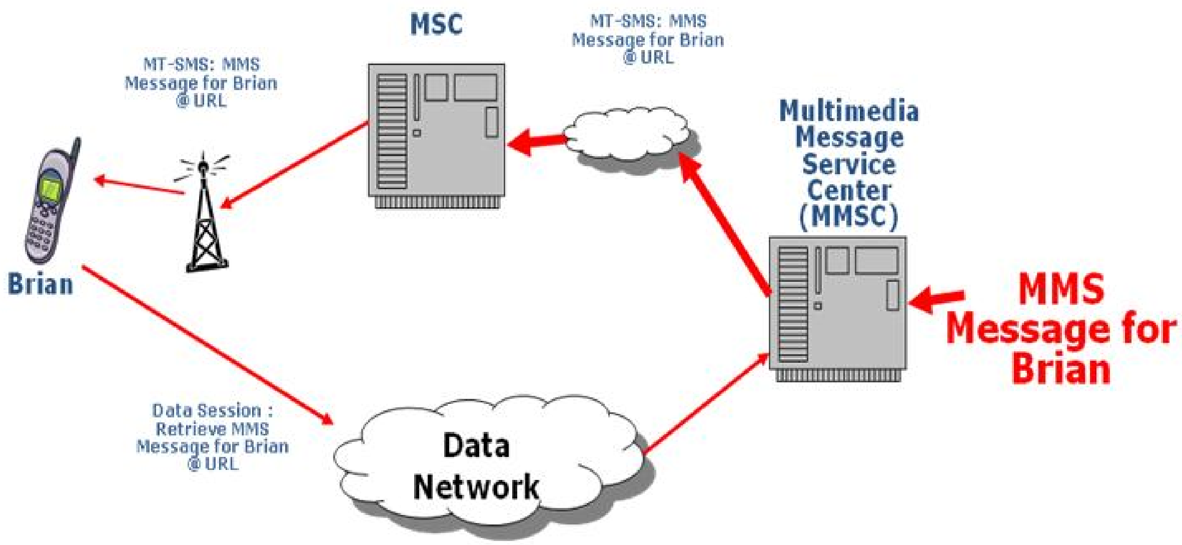


Figure 19: SMS Aggregator Network Architecture[11]

2.4 MULTIMEDIA MESSAGING

The Multimedia Messaging Service (MMS) was developed by 3GPP and is maintained by the Open Mobile Alliance (OMA). MMS supports sending messages that include multimedia content (text, audio, video, pictures, etc.) to and from mobile devices that support the feature. MMS is a subscription service and is functionally different than the SMS service. Technically, multimedia messages are delivered in a completely different way than SMS messages. (MMS is closer conceptually to email than to SMS.) However, MMS uses both SMS and the data network for delivery of the message. Not every mobile device or subscription supports MMS.

[11] See Jeff Brown, Bill Shipman, Ron Vetter, "SMS: The Short Message Service," Computer, vol. 40, no. 12, pp. 106-110, Dec. 2007, doi:10.1109/MC.2007.440


MSC
MT-SMS: MMS Message for Brian @URL
MT-SMS: MMS Message for Brian @URL
Multimedia Message Service Center (MMSC)
Brian
MMS Message for Brian
Data Session : Retrieve MMS Message for Brian @URL
Data Network

MT-SMS triggers browser to open on mobile and retrieve multimedia message from server via data network

Figure 20: Multimedia Messaging Service

To deliver a multimedia message, an SMS "control message" is sent to the device with a URL to trigger the device's browser to open a data connection and receive the multimedia content. Additional SMS messages are exchanged to report status of the retrieval. MMS requires significantly more network resources than SMS.

MMS is a non-real-time delivery system (as is SMS). Prime examples of non-real-time messaging services include traditional email available on the Internet and wireless messaging systems such as paging or messaging.

MMS does not support location determination or routing to the correct PSAP based on the sender's current location.

Multimedia Messaging (MMS) offer no solutions to the limitations of SMS to 9-1-1. Other subsequent text messaging products, such as MMS, may actually use SMS technology as part of the delivery of the message. Thus, all of the existing technical shortcomings with SMS to 9-1-1 will also exist with these messaging methods as well.

MMS also introduces a number of challenges beyond those with SMS[12]:

- **Content adaptation:** Multimedia content created by one mobile device may be incompatible with the recipient's mobile device. In the MMS architecture, the recipient's Multimedia Messaging Service Center (MMSC) is responsible for providing content adaptation (e.g., image resizing, audio codec transcoding), if this feature is enabled by the wireless network operator. When content adaptation is supported by a wireless network operator, its MMS subscribers enjoy compatibility with a larger network of MMS users than would otherwise be available.

[12] See http://en.wikipedia.org/wiki/Multimedia_Messaging_Service

- **Bulk messaging:** The flow of peer-to-peer MMS messaging involves several over-the-air transactions that become inefficient when MMS is used to send messages to a large numbers of subscribers, as is typically the case for VASPs.

- **Mobile Device Configuration:** Unlike SMS, MMS requires a number of mobile device parameters to be set. Poor mobile device configuration is often blamed as the first point of failure for many users. Service settings are sometimes preconfigured on the mobile device, but wireless operators are now looking at new device management technologies as a means of delivering the necessary settings for data services (MMS, WAP, etc.) via over-the-air programming (OTA).

2.5 MOBILE INSTANT MESSAGING

Instant messaging (IM) is a form of real-time direct text-based communications between two or more people using personal computers or other devices, along with shared software clients. The text is conveyed over a network, such as the Internet. More advanced instant messaging clients also allow other modes of communications, such as live voice or video calling. There are numerous IM clients available, and many have proprietary, incompatible protocols. There have been several attempts to create a unified standard for instant messaging: IETF's SIP (Session Initiation Protocol) and SIMPLE (SIP for Instant Messaging and Presence Leveraging Extensions), APEX (Application Exchange), PRIM (Presence and Instant Messaging Protocol), the open XML-based XMPP (Extensible Messaging and Presence Protocol), and OMA's (Open Mobile Alliance) IMPS (Instant Messaging and Presence Service) created specifically for mobile devices.

Most attempts at creating a unified standard for the major IM providers have failed, and each continues to use its own proprietary protocol. For this reason users have to either use the same IM clients, or use a client that supports multiple protocols, or the IM server needs to do the protocol conversion.

In a mobile environment, IM is constrained by bandwidth and the form factor/user interface of the mobile device. Mobile IM (MIM) allows connection to an IM application via the mobile device. There are two distinct methodologies to enable mobile instant messaging:

- **Embedded Clients** - tailored IM client for every specific mobile device with a special back-end server installed within the wireless operator network.

- **Clientless Platform** – a browser based application which enables users to connect to their Internet IM service without the need for any support by the wireless operator.

MIM may use SMS or the data network to provide connectivity to the IM server. SMS may be used as a bearer for MIM. For example, IM applications such as Yahoo! Messenger® offer a client based on SMS[13]. However, SMS does not include alias capabilities nor does it allow for confirmation that the intended recipient is available. SMS makes it impossible for the recipient to receive the MIM message in real-time because SMS is transaction based and not session based. MIM does not “fix” the limitations and vulnerabilities of the underlying SMS transport (if SMS is used for the transport).

3GPP has defined specifications that enable interworking between SMS and IM (at both service level and transport level). In addition, OMA has defined the Instant Messaging and Presence Service (IMPS)[14], which is an OMA enabler

[13] See http://mobile.yahoo.com/messenger/sms

[14] See IMPS Architecture, OMA-AD-IMPS-V1_3-20070123-A, Open Mobile Alliance

that is designed for exchanging instant messages and presence information not only between mobile devices but also between mobile and fixed devices. The following figure shows the IMPS architecture:

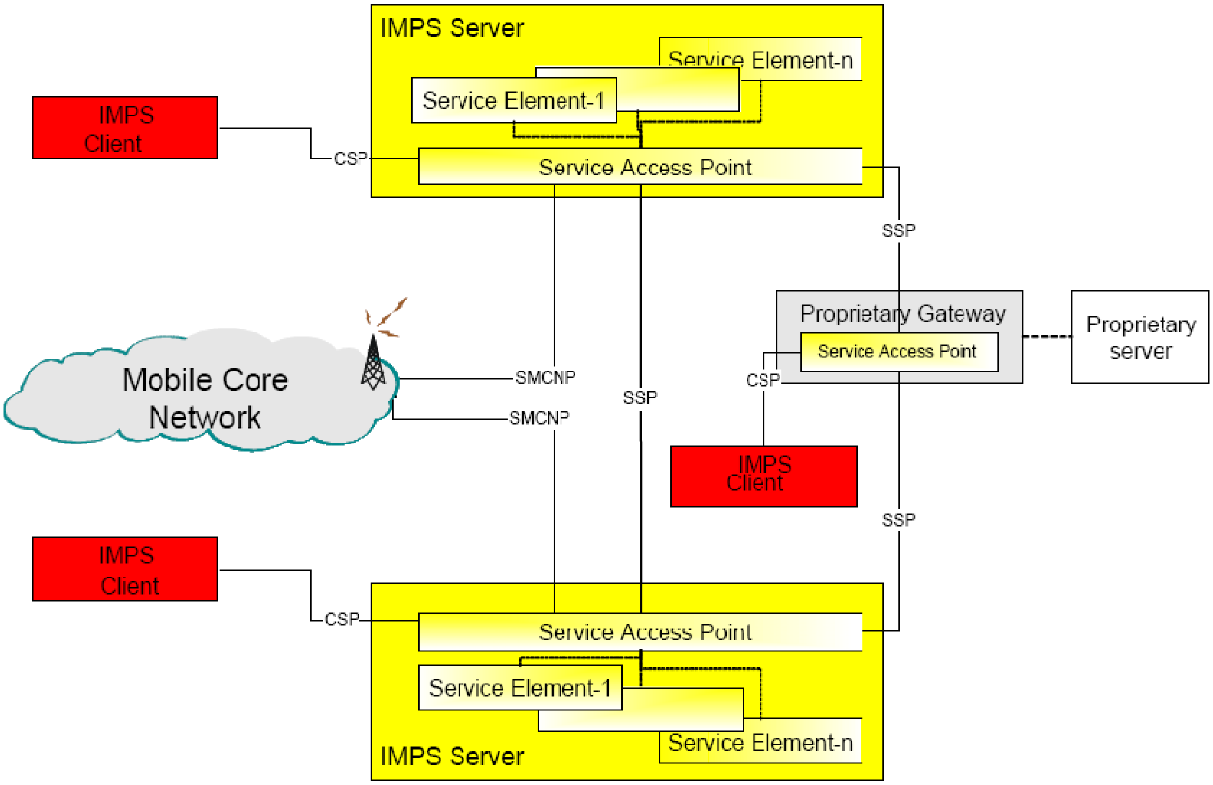


Figure 21: OMA IMPS Architecture

A "clientless platform" MIM allows the community of users to register their presence, allowing for more real-time text messaging and communications than would be possible with traditional mobile messaging. Mobile IM provides "presence" to the IM server which establishes an IM "session". MIM with an "always on" data connection will provide the user with a more real-time IM experience similar to the IM experience from a computer on the Internet. However, since this is a clientless platform, the basic wireless operator provided services (location, routing, etc.) are not available for the IM session.

There are IP relay services offered[15] that allow users to contact emergency services via IM through a relay service. Users select "911" from their IM contact list, and open a session with the relay service. Users have to provide their location to the relay service through the IM session so the relay service knows which PSAP to contact.

Crackers (malicious "hacker" or black hat hacker) have consistently used IM networks as ways for delivering phishing attempts, "poison URLs", and virus-laden file attachments. Hackers use two methods of delivering malicious code through IM: delivery of viruses, Trojan horses, or spyware within an infected file, and the use of "socially engineered" text with a web address that entices the recipient to click on a URL connecting him or her to a website that then downloads malicious code. Viruses, computer worms, and Trojans typically propagate by

[15] See http://www.ip-relay.com/im/

sending themselves rapidly through the infected user's buddy list. Infections may range from nuisance to criminal, and are becoming more sophisticated each year. Consideration of these attacks must be made for any use of IM for emergency services.

IM connections usually take place in plain text, making them susceptible to eavesdropping. In addition, IM client software often requires the user to expose open UDP ports to the world, increasing the threat posed by potential security vulnerabilities.

2.6 SMS OVER GENERIC IP CONNECTIVITY ACCESS NETWORK (IP-CAN)

3GPP has defined the ability to support SMS over a generic IP connectivity access network (IP-CAN)[16]. SMS via IP-CAN requires a mobile device which supports IP Multimedia Subsystem (IMS) data services, and a wireless operator network supporting both an IMS as well as an IP SMS Gateway. These are future capabilities and are not available in networks deployed today.

The reference architecture for providing SMS via IP-CAN is as shown below:

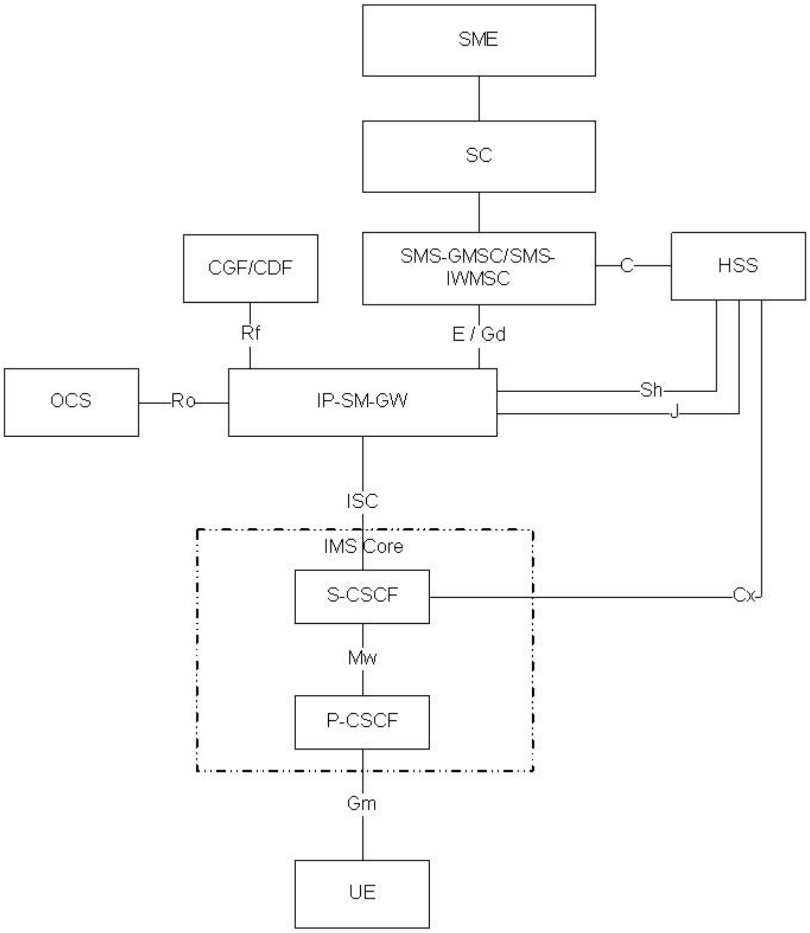


Figure 22: SMS via IP-CAN

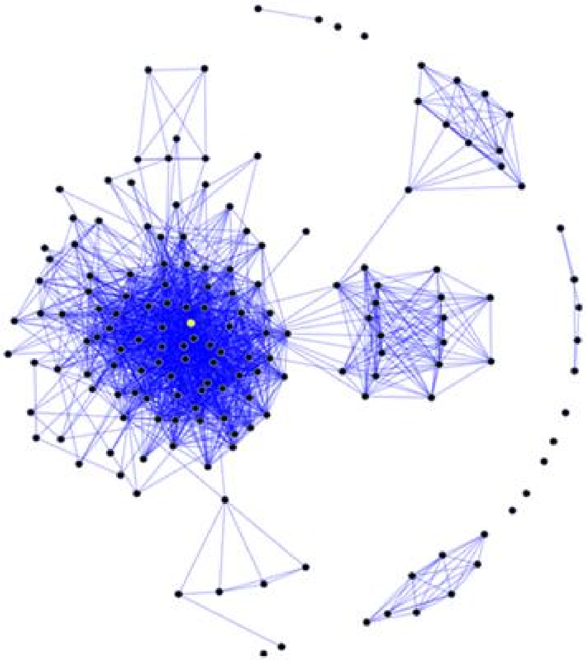
[16] See 3GPP TS 23.204, http://www.3gpp.org/ftp/Specs/html-info/23204.htm

The basic principle is that SMS flows through the traditional SMSC and a Gateway or Interworking MSC to an IP Short Message Gateway. From there, the SMS message is delivered to the mobile device via IP through the IP Multimedia Subsystem (IMS). Note that this is a hybrid architecture, where the legacy SMSC is still used as the store-and-forward entity. Thus, the characteristics of SMS when using SMS via IP-CAN are the same as using SMS on the legacy circuit switched network.

The IP Short Message Gateway has an additional function to provide the capability for service-level interworking between Short Messages and Instant Messages in IMS. In many user-to-user message exchange systems, message senders often wish to know if the human recipient actually received a message or has the message displayed. IETF IMDN (Instant Message Disposition Notification) for delivery notification can be supported as part of the service level interworking with IM.

2.7 SOCIAL NETWORKING

From a technology perspective, social networking applications have similar network impacts as SMS. A Social Network Diagram is made up of numerous point-to-point connections, as indicated in the following figure[17]:



An example of a social network diagram.

The node with the highest betweenness centrality is marked in yellow

Figure 23: Social Network Diagram

Most social networking applications require a data connection to access the application, and may have an SMS component similar to MMS.

[17] See http://en.wikipedia.org/wiki/Social_network

Some social networking applications provide the ability to receive updates via SMS. For example, Twitter® allows a user to receive Tweets through SMS, allows a user to post updates via SMS, and to have defined short codes and text commands that perform specific functions via SMS.

Many social networking applications are adding location capabilities. On specific mobile devices supporting HTML5 and geo-location, there is the capability to "Tweet with your Location" if the user authorizes the application to use the location from the mobile device. The location may be provided at the neighborhood level, the town level, or an exact point. Facebook® has recently launched "Facebook® Places" to their application, again for HTML5 and geo-location supporting mobile devices. "Places" allows a user to "check in" to a specific location to allow their friends see where they are, and can also be used to track friends. The application also gives the user the ability to allow third party applications to obtain your location (with permission) to tailor services to a user's location.

Some agencies have started looking at incorporating Facebook®, Twitter®, MySpace®, etc. into their emergency communications systems. However, these sites are typically used for general information sharing and not for emergencies[18]. Most police agencies do not monitor the social networking sites constantly from their PSAPs. Social networks are increasingly becoming the first way people learn about something happening, and may be beneficial for "word of mouth" information sharing.

There are cases where social networks reportedly played a role in contacting emergency services. In 2009, Atlanta councilman Kwanza Hall used Twitter® on his BlackBerry® in an effort to summon medical assistance at the scene of an accident because he was concerned the mobile device battery was too low to place a call[19]. His Tweet for assistance was picked up by several of his followers, who called 9-1-1 and reported it. However, it was not clear if the Tweet resulted in the medic dispatch or was a result of other bystanders making a call to 9-1-1. This scenario does raise several questions, however:

- If the followers are not in the same geographic location, how do they know whom to contact for emergency services on behalf of the Tweeter?

- If the Tweeter did not specify the location exactly, will the follower know what city the emergency is even in? For example, Kwanza tweeted "Need a paramedic on corner of John Wesley Dobbs and Jackson St. Woman on the ground unconscious. Pls ReTweet". If a follower in another city received this and he was unaware it was from Atlanta, would that follower call 9-1-1 in his city and report it?

- If the Tweeter has a large number of followers, what if they all called 9-1-1 on his/her behalf? Would this overwhelm the 9-1-1 system?

- Who would keep a record of Tweets for use in investigations and/or litigation?

While these social networking tools may seem valuable for emergency services, significant security issues exist. As these applications incorporate location features, significant security and privacy concerns are raised. SMS-based social networking applications do not overcome the limitations of SMS. Browser based social networking applications require an always-on data connection, and newer applications require mobile devices that support HTML5 and geo-location.

[18] See "Police: Use 911 instead of Twitter, Facebook", http://www1.whdh.com/news/articles/local/12001917838482/police-use-911-instead-of-twitter-facebook/

[19] See "Twitter Trumps 911", http://www.wired.com/epicenter/2009/05/twitter-trumps-911/

2.8 EXAMPLE IMPLICATIONS OF TEXTING SERVICES AND APPLICATIONS

This section provides two examples of other texting services and applications which could have implications for the support of emergency text messages to PSAPs. The first example describes the implications of an existing smartphone based alerting application. The second example describes the implications of the variety of existing "Free SMS" and "SMS bypass" applications and services.

2.8.1 SMARTPHONE ALERTING APPLICATION

Availability of a third-party emergency alerting application for a popular smartphone platform started in March 2010. Even though this particular version of an emergency alerting application is targeted for a specific smartphone, future versions of this application or other similar smartphone applications could be developed for any other type of smartphone.

When the subscriber installs this emergency alerting application for their smartphone, they configure it with phone numbers for SMS messages and email addresses for whom they wish to notify if they need help. In an emergency situation, this application can be activated without alerting onlookers or the potential attackers. When this emergency alerting application is activated, it will send SMS and/or email messages to the configured list of contacts approximately every 60 seconds until deactivated by the subscriber. The emergency alert message that is sent every 60 seconds identifies the subscriber indicates that they are having an emergency, and provides approximate location information in the form of a URL to Google® Maps.

This emergency alerting application has been receiving numerous rave reviews on various Internet blogs, online user journals, and online newspaper articles. This application has also received several endorsements. All of these reviews and endorsements are encouraging subscribers to acquire and install this application.

At this time, this application does not send these emergency alert messages to PSAPs because SMS or email interfaces to do so currently do not exist. If a PSAP defines an SMS or email address whereby citizens can send messages, there is nothing to restrict the use of this application for sending messages to that address.

For the purpose of this analysis, the following assumptions will be applied:

a. The environment is the campus of a large university (e.g., 20,000 students).
b. A mechanism has been defined for the students to send SMS emergency messages to the PSAP supporting that university, such as a specific short code.
c. Smartphones are very popular with college students and, therefore, a large number of university students have smartphones with the emergency alerting application installed and configured. For example, the university might give the emergency alerting application to the students for free with the SMS address for the university PSAP preconfigured.
d. Three wireless operators provide wireless coverage for the university campus with each wireless operator covering the campus with 5 sectors each.

An emergency situation such as a campus shooting occurs on the university campus. Hundreds and potentially thousands of students activate the emergency alerting application on their smartphones. Assume that mobile originated SMS messages are processed by each of the three networks at the rate of 2 mobile originated SMS messages per second per sector. Based upon the coverage assumption, the wireless networks covering the university campus have a maximum capacity of 30 mobile originated SMS messages per second. With the large number of activations of the emergency alerting application on the student's mobile devices, the wireless networks covering the university campus will reach this maximum capacity very quickly. Due to the 60 second retransmission capability of the emergency alerting application, the wireless networks will remain at this maximum level until the application is deactivated on the smartphones by the students. As described above, SMS does not have the kind of smart retransmission back-off included in protocols such as TCP, which could avoid each application making the situation worse.

Based upon the assumption that the PSAP is one of the preconfigured recipients of the SMS based emergency messages from this smartphone application, the PSAP will be receiving these emergency alert messages at the rate of 30 SMS alert messages per second which equates to a rate of 1,800 SMS messages per minute or 108,000 SMS messages per hour. The PSAP will continue to receive these alert messages at this rate until the students deactivate the emergency alerting application on their smartphones.

Many of these alert messages will be repeated alert messages, but these repeated alert messages may not be exact duplicates because the student may have moved and consequently the location information portion of the message could be different.

Also, the alert messages for any other emergency incident that is occurring at the same time would be intermingled with this massive queue of alert messages and could be overlooked by the PSAP system and/or the PSAP call takers.

Due to movement of the students and due to the propagation characteristics of RF radio coverage, these emergency alert messages may also be sent to PSAPs that are serving the surrounding neighborhoods.

2.8.2 "FREE SMS" AND "SMS BYPASS" APPLICATIONS AND SERVICES

There are a significant number of applications and services available to wireless subscribers which are advertised as "Free SMS" or "SMS Bypass" services. These are web-based and smartphone applications which provide texting services without using the messaging capabilities of the wireless operator's network. These applications, when downloaded to smartphones, may even have screens that look very similar to the embedded SMS services on the mobile device.

To get a sense of the number and availability of these services and applications just enter "Free SMS" or "SMS Bypass" in your favorite Internet search engine or in your favorite smart device app store.

The texting capabilities provided by the wireless operator SMS based messaging services are defined by industry standards and are completely separate from these other types of text messaging services even though they may appear on the surface to be the same.

Since these are Internet-based applications, the wireless operator network has no knowledge or control of these third party "Free SMS" or "SMS Bypass" data services and applications. Consequently, as with SMS, the wireless operator networks cannot perform the functions such as PSAP determination, PSAP routing, and call back information. The support of these emergency services functions by these third party "Free SMS" or "SMS Bypass" data services and applications will be impossible.

Some of these third parties "Free SMS" or "SMS Bypass" services don't even require a mobile device. SMS-like messages can be sent via a PC over any network (e.g., WiFi, cable, DSL) and will totally bypass the wireless networks. However, to the end recipient, these third party SMS-like messages could appear as if they are coming from a mobile device. As a result, PSAPs could be subject to massive amounts of SPAM and Denial of Service attacks from what appear to be legitimate messages coming from mobile devices on wireless networks.

These SMS-like messages from "Free SMS" or "SMS Bypass" services are completely anonymous and cannot be traced back to an originating mobile device or subscriber.

3. SECURITY ASPECTS AND VULNERABILITIES

SMS does not provide any type of authentication or security. Millions of spam SMS messages hit the wireless operator's networks every day, and protections are put into place to protect the customers from these messages. Therefore, it is very easy to transmit malicious SMS messages either to a 9-1-1 center or to a subscriber. "Fraudsters" can use this fact to create denial of service attacks on 9-1-1 centers; international trials of text to 9-1-1 functions resulted in very high percentage of fraudulent/hoax messages, including the delivery of pornographic content to the PSAP. In addition, virus software and malware is now being seen delivered via SMS.

Additionally, terrorists or other criminals can send fraudulent SMS messages to 9-1-1 call takers produce some reaction (e.g., "Am held by men with machine guns inside store at corner of 5th and Main. They say they are going to kill me. HELP!"). The resulting first responder reaction can then be targeted for malicious exploitation.

SMS is subject to malicious attacks that would affect SMS access to 9-1-1 emergency services, and would create new problems for PSAPs and potentially for wireless networks. The use of smartphones that can be programmed to repeatedly send SMS messages also creates the potential for inadvertent transmission of a large number of short messages that could flood a PSAP.

3.1 SMS SPOOFING

SMS Spoofing (also known as "Blow-back" and "Joe-Job") occurs when a sender manipulates address information to impersonate a subscriber and send a short message. It is possible to spoof SMS messages and make them appear to come from other people's mobile devices. Senders transmitting SMS messages from online computer networks normally "spoof" their own number in order to properly identify themselves. SMS spoofing can be conducted at the national and international level.

An SMS Spoofing attack is often first detected by an increase in the number of SMS errors encountered during a bill-run. These errors are caused by the spoofed subscriber identities. Wireless operators can respond by blocking different source addresses in their Gateway MSCs, but fraudsters can change addresses easily to bypass these measures. If fraudsters move to using source addresses at a major interconnect partner, it may become unfeasible to block these addresses, due to the potential impact on normal interconnect services.

An example of SMS spoofing is that messages sent from Google® are sent with the Sender ID "Google". Skype® sends messages from its users with the mobile number they registered with. In this case, when a user attempts to "reply" to the SMS message, the local system may or may not allow the replying message to be sent through to the spoofed "origin". Another example is to send a spoofed SMS message to Twitter®. Twitter® uses the SMS originator to authenticate the user. Hoax Mail is used to spoof the SMS message and therefore could trick Twitter® to post the message on the victims Twitter® page.

If SMS messages could be sent to 9-1-1, a fraudster could use spoofing to impersonate a valid subscriber and send a malicious message to 9-1-1. Many problems could then arise for PSAPs and for valid subscribers including:

- Invalid SMS message contents received by the PSAP;

- PSAP response messages would be sent to the valid subscriber who did not send the original SMS message (which could then start a an "exchange" of SMS messages between the PSAP and the valid subscriber);

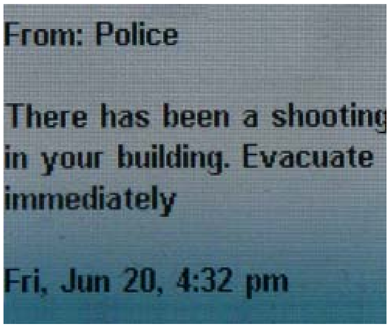
- The PSAP may dispatch a first responder to a location specified in the SMS message;

- PSAP resources diverted to handle "incidents" triggered by spoofed messages;

- Potentially blocking legitimate SMS messages at the PSAP to defend against spoofing.

Wireless network resources would be wasted in transporting "spoofed" SMS messages to 9-1-1. Any tools employed by a wireless service provider or the PSAP to detect and block spoofing could block legitimate SMS messages to 9-1-1.

The following example from the 3G Americas white paper, "Characterizing the Limitations of Third-Party EAS over Cellular Text Messaging Services,"[20] illustrates the issue of distinguishing fraudulent messages from legitimate messages.



From: Police

There has been a shooting
in your building. Evacuate
immediately

Fri, Jun 20, 4:32 pm

Figure 24: Example of Forged Emergency Message

This is a forged emergency message warning the user of an on-campus shooting and claims to be sent by the Police.

There are significant implications to this shortfall. For instance, in the event of an emergency such as a chemical leak, it would be easy for a malicious party to send an "all-clear" message before the situation was deemed safe. Because it would not be possible for users to verify the source of the information, maliciously induced confusion is a real threat.

Examples of SMS spoofing are common and can be expected with any SMS based service (including emergency services) due to the lack of security.

In 2009 following an earthquake in Indonesia, a hoax text messages began circulating warning of a "new, stronger earthquake"[21]. It was claimed to have been sent from a legitimate government agency.

[20] 3G Americas White Paper, "Characterizing the Limitations of Third-Party EAS over Cellular Text Messaging Services," Patrick Traynor, Ph.D., September 2008

Also in 2009, a hoax Amber Alert message was circulated[22] saying “a 3-year old boy was kidnapped by a man in a 2003 Mitsubishi Eclipse with Oregon license plate 98B351”. “Amber Alerts from unknown sources could lead to a delayed response from the public and jeopardizes the integrity of the entire Amber Alert plan,” said State Police Lt. Molly Cotter, Oregon Amber Alert coordinator.

SMS spoofing has resulted in panic -- hoax text messages were used to spreads tsunami terror in Indonesia (June, 2007[23]). Thousands of people fled their homes in panic on the Indonesian coast after hoax text messages spread warning them that a tsunami will hit the region. ”The possibility is that a tsunami may take place on June 7,” said part of a short telephone text message (SMS) that is widely circulating in various coastal areas of Nusa Tenggara province.

In May 2005, an SMS tsunami rumor hits Sumatra[24]. Rumors that a volcanic eruption had sent a tsunami crashing toward the coast spread through a seaside town on Indonesia's Sumatra Island early Tuesday, prompting thousands of panicked residents to flee to high ground. It was unclear how Tuesday's rumor began, but it quickly spread by word of mouth and SMS text message, the state news agency Antara reported. By about 2 A.M., almost all the mosques in the town were broadcasting tsunami warnings from their loudspeakers along with religious verses, it said.

Section 2.8.2 describes “Free SMS” and “SMS Bypass” services and applications which are outside the control and knowledge of the wireless operators and which might be capable of being used as sources of SMS spoofing and denial of service attacks.

3.2 SMS FLOODING

SMS Flooding occurs when a very large number of SMS messages are sent to one or more destinations. Flooding is a denial of service attack that can congest elements in the wireless network. If SMS messages could be sent to 9-1-1, flooding could congest the PSAP elements used to respond to SMS messages. The tools used by wireless service providers to detect and filter flooding could block legitimate SMS messages to 9-1-1. Any tools potentially used by a PSAP to combat SMS flooding could also block legitimate SMS messages to 9-1-1.

SMS Flooding may occur if a smartphone or web application can be programmed to repeatedly send SMS messages to 9-1-1 (see section 2.8.1). Although the subscriber’s intent may not be malicious, the repeated sending of SMS messages to 9-1-1 may create a congestion problem.

Voting with SMS messages can also generate a very large amount of SMS traffic and, in fact, record level of SMS traffic levels have occurred from SMS voting activities (e.g., voting for favorite performer on American Idol™). However, SMS voting is not the same as SMS Flooding for the following reasons:

1. SMS voting is originated only from mobile devices and the radio configuration limits the number of SMS messages that can be sent from any cell site.

[21] See “SMS Earthquake Warnings an 'Irresponsible' Hoax: Indonesian Officials”, http://thejakartaglobe.com/home/sms-earthquake-warnings-an-irresponsible-hoax-indonesian-officials/327986

[22] See “State police chase Amber Alert hoax”, http://www.theoutlookonline.com/news/story.php?story_id=125478497579981700

[23] See “Hoax text message spreads tsunami terror in Indonesia”, http://www.breitbart.com/article.php?id=070606101917.31jf2eyb&show_article=1

[24] See “SMS tsunami rumor hits Sumatra”, http://www.textually.org/textually/archives/2005/05/008318.htm

2. SMS voting typically occurs across very large geographic areas (e.g. multiple states or national). Consequently, the SMS voting messages are distributed across tens of thousands of cell sites.

3. The SMS voting messages are sent to specific SMSCs which are pre-configured to handle the volume of SMS voting messages.

4. There is no impact to personal safety if the SMS voting message is queued before being processed.

5. SMS voting is typically done with the wireless operator knowledge, cooperation, and coordination including allocation of additional resources.

6. SMS voting may use a special SMSC with the store and forward capability disabled, in order to prevent congestion at the SMSC. This may result in an increase in the number of "lost" messages.

There is no threat to life or property if a SMS voting message is lost or delayed.

3.3 SMS SPAM

SMS Spam is any unsolicited message delivered to a mobile device as an SMS message. Wireless service providers employ filters to block SMS spam. If SMS messages could be sent to 9-1-1, spam filters may block some SMS messages. An unintended blocking may occur because of the configuration of the spam filter, or unintended blocking may occur as a normal aspect of the spam filter operation.

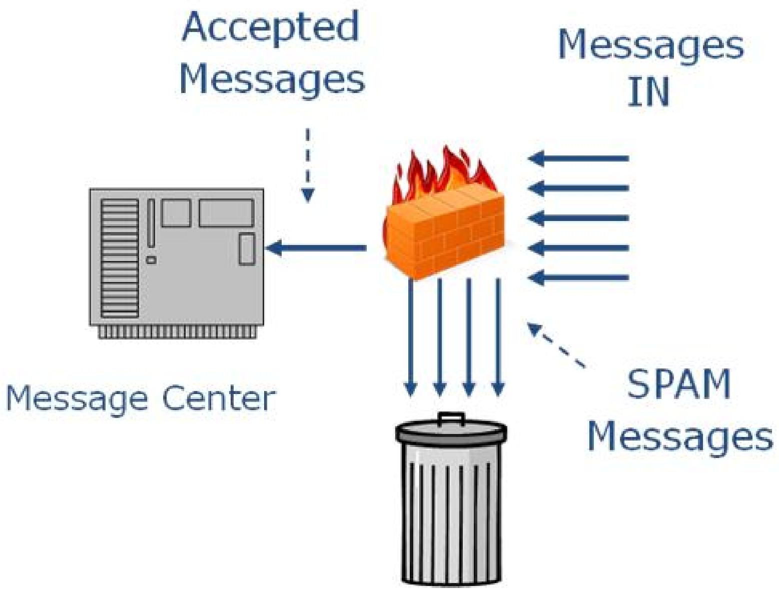


Figure 25: SPAM Messages

SPAM detection mechanisms include:

- Looking at the number of messages sent from a single originator
- Detection of X messages over a Y period
- Source of message, e.g. from a known "spammer"

3.4 DENIAL OF SERVICE ATTACKS

The security vulnerabilities open the door to denial of service attacks from resulting network and radio interface congestion to the point of blocking voice calls. The National Communications System (NCS) studied the threats of SMS[25], and one conclusion is:

> *"By examining the Washington, DC, and Manhattan scenarios, it can be concluded that, if SMS were used extensively during a crisis, a significant SMS load could be placed on a network. Individually, the voice load and SMS load are multiple times higher than the engineered capacity at each sector. This analysis has not considered several factors that might increase load, such as messages originating from other sources (e.g., the Internet) and terminating in the congested area. It has also not considered message re-send attempts after failures, which add to network load."*

Such an attack could be initiated against one or more PSAPs in the U.S. and could come from domestic or international sources.

Another report from ETSI [26] highlights that SMS Lacks Security resulting in vulnerabilities to spoofing and denial of service attacks:

> *"For mobile terminated national emergency messages it would be possible for spam either from a mobile phone or from the Internet to create malicious emergency messages and cause a panic reaction for many mobile subscribers."*

Once you fill up the control channels with SMS messages, voice call setups (as well as additional SMS messages) are blocked.

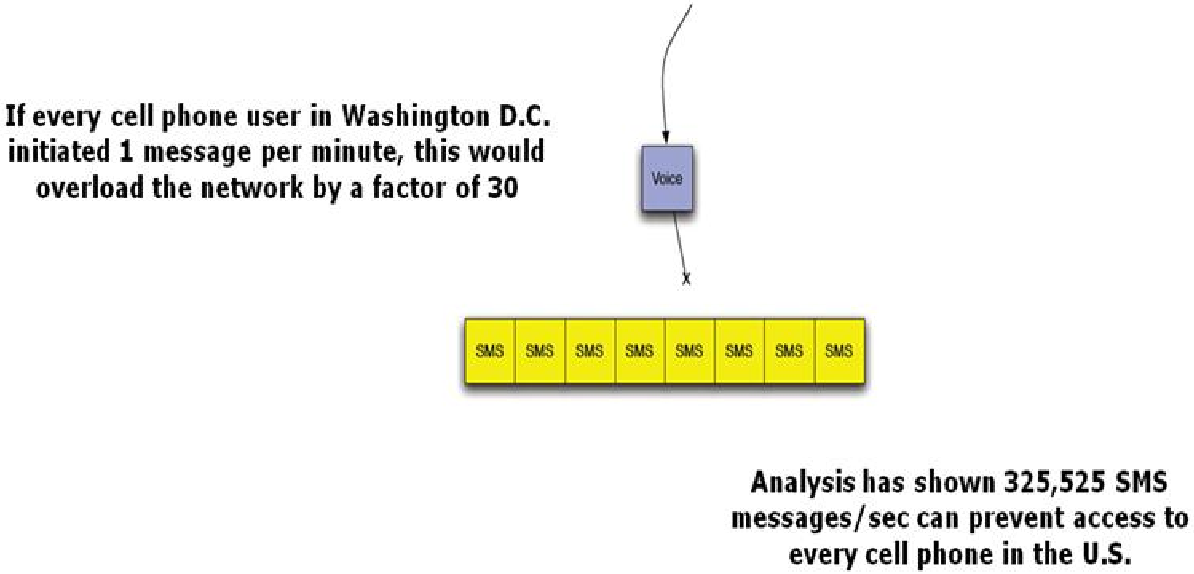

If every cell phone user in Washington D.C. initiated 1 message per minute, this would overload the network by a factor of 30
Voice
X
SMS
SMS
SMS
SMS
SMS
SMS
SMS
SMS
Analysis has shown 325,525 SMS messages/sec can prevent access to every cell phone in the U.S.

Figure 26: Exploiting Open Functionality in SMS-Capable Cellular Networks[27]

[25] See NCS SMS over SS7, TECHNICAL INFORMATION BULLETIN 03-2, December 2003

[26] See ETSI TR 102 444 V1.1.1 (2006-02)

3.5 FRAUDULENT PSAP

It is extremely easy for a person with malicious intent to create what looks to be a “real” PSAP address but in reality is a fraudulent address. This can be an issue not only for SMS but also any texting solution, including IM and social networks. A fraudster could advertise a phony account and post misleading information. If these methods are used to contact 9-1-1, the fraudster could engage in a conversation making the victim believe they are actually conversing with the police.

These fraudulent attacks are not speculation. In 2010, a Twitter® account with no ties to Portland Oregon police was using the police bureau's badge and operating under the name "pdxpolice."[28] This account posted crude information and poked fun at police officers. In 2009, @AustinPD appeared on Twitter®. It advertised itself to be a Twitter® link to the Austin (Texas) Police Department. However, it was not a real link to the Austin PD and was a prank. "Although some may dismiss the site as a simple prank or minor irritant, the fact is that the information presented was false and misleading, and could lead to unwarranted concern by the public," Austin police chief Art Acevedo said in a statement[29].

Creating fraudulent SMS addresses, Twitter® accounts, Facebook® accounts, and IM addresses is very simple and could be a significant problem if and when these services are widely used to contact emergency services.

3.6 PRIVACY

SMS messages do not have cryptographic protection for confidentiality and integrity. Thus SMS messages could be intercepted and snooped during transmission. This is especially true if the SMS messages go through a third-party network during the transmission process.

There are also spyware programs such as FlexiSpy[30] that enable intruders to record all incoming and outgoing SMS messages to/from a mobile device and upload them to a remote server for later viewing.

3.7 SMS PHISHING

Phishing attacks are common on the Internet. Phishing is the criminally fraudulent process of attempting to acquire sensitive information (such as usernames, passwords and credit card details) by masquerading as a trustworthy entity in an electronic communications. Phishing attempts via SMS (also called SMiShing) may also occur directing a user to a fraudulent website or to download malware to their mobile device. Using a combination of SMS Spoofing and SMiShing, a victim may believe they are providing information to the police or other emergency service agencies. Extensive public education must be undertaken to counter this threat.

[27] “Text Hackers Could Jam Cellphones, a Paper Says,”, http://www.nytimes.com/2005/10/05/technology/05phone.html?_r=1

[28] “Fake Police Twitter Account Boasts Crude Tweets,” March 2, 2010, http://www.kptv.com/news/22715236/detail.html

[29] “Austin 911! Fake police Twitter account gets busted,” cnet News, March 25, 2009, http://news.cnet.com/8301-13577_3-10204228-36.html

[30] See http://www.flexispy.com/news-flexispy-blackberry-windows-mobile.htm

4. IDENTIFED SMS AND NETWORK SHORTFALLS

To characterize the key limitations and shortfalls of SMS for use in emergency calls, it is useful to understand what is available in voice emergency calls. "Voice" 9-1-1 callers provide 9-1-1 centers with:

- Automatic routing of the voice call to the PSAP without the need for the subscriber to provide any information;
- Priority of the emergency voice call;
- Callback information;
- Actual location information especially that provided by the caller when asked by the 9-1-1 call taker, including details of hard-to-find locations and the caller's location in relation to the incident (e.g., "I'm hiding in the upstairs bedroom closet and the burglar is in the kitchen");
- Ability for 9-1-1 call takers to determine the caller's emotional state and capabilities;
- Ability to rapidly exchange information when the 9-1-1 call taker needs to ask questions and get clarifications;
- Background sounds and other information transmitted as part of the voice call, which can help 9-1-1 call takers learn more about the caller's situation and possible risks to first responders; and
- Possible deterrence of prank calls via PSAP recordings of voice 9-1-1 calls, which may allow malicious callers to be identified.

Phase II wireless E9-1-1 service allows the public to call local 9-1-1 centers for help. Some states have 100% Phase II deployed for all wireless operators. The 9-1-1 call takers get the emergency caller's callback number and approximate geographic location, along with real-time voice connections with the person seeking help. This real-time dialogue provides benefits impossible to replicate with any sort of text communications. These benefits are essential to effective 9-1-1 responses.

SMS to 9-1-1 provides none of the benefits inherent in Voice 9-1-1 service. It is virtually impossible to guarantee a real-time two-way text communications exchange using SMS technology. Given how SMS is designed and network configurations, SMS emergency messages will not receive any sort of "priority treatment". There is no indication of failed SMS to 9-1-1 message attempts, both at the 9-1-1 center and to the 9-1-1 caller – Did my message get through? There is no viable means of providing location information, thus no way to route the SMS message to the correct PSAP. SMS does not provide any type of authentication or security; risks from "spoofing" and denial of service attacks are high. Multimedia Messaging (MMS) or Mobile Instant Messaging (MIM) offers no solutions to the limitations of SMS to 9-1-1.

SMS was designed as a method of handset-to-handset or automated service-to-handset messaging, with the message sent from one phone number (or an automated service) to another phone number. Over time, SMS was enhanced so that the endpoint of an SMS message could be an email address. In order for SMS to be delivered to a 9-1-1 center in a way that permits it to be a quality method of emergency communications, there are a number of identified shortfalls, both in the wireless operator's network and in the PSAP systems, that provide significant operational challenges and limitations for the use of SMS for emergency communications to PSAPs.

4.1 SMS TO VOICE EMERGENCY CALL COMPARISON

The following table identifies the key characteristics of SMS as related to voice based emergency calls:

Table 1: SMS to Voice Emergency Call Comparison

Characteristics	Voice Emergency Call	SMS (evaluated from mobile device, MSC, SMSC GSM standards)
Transport	CS call with allocated traffic channel	No channel allocation
Connectivity	Caller and call taker establish a connection	No connection established
Emergency indication	Mobile device and all network elements must support it	Not supported
Priority	High priority	Not supported
9-1-1 call routing based on caller's location	Different routing than normal call	Not supported
Local breakout for 9-1-1 call	Roaming user's call directed to the local PSAP	Not supported -- Roaming user's SM directed to home SMSC, not the local SMSC
Call delivered within 6 seconds	Required and standardized	Not supported ("best effort" service)
Location information sent to PSAP	Required and standardized	Not supported
Callback information sent to PSAP	Required and standardized	Not supported
High availability and high reliability (five 9)	Required	Not supported ("best effort" service)
Mobile devices that do not have a SIM inserted or are unable to obtain normal service for other reason, can still initiate emergency calls	Required (in some jurisdictions, including North America) and standardized	Not supported

4.2 IDENTIFIED SHORTFALLS FOR SMS

This section discusses the following shortfalls of using SMS for the use of SMS for emergency communications with PSAP:

- Callback information for wireless subscriber

- Routing of SMS message to appropriate PSAP
- SMS is only a “best effort” service
- Subscriber is mobile during messaging with PSAP
- No location capabilities for SMS messages
- No SMS delivery acknowledgements to the users
- Address of “911” not a valid SMS destination address
- International roaming subscribers have different international emergency numbers
- Handling of unauthorized or fraudulent mobile devices

4.2.1 CALLBACK INFORMATION

SMS is capable of providing the caller’s identification to the recipient provided the SMS uses the wireless operator’s network. The sender’s identification is signaled to the SMSC in the MO-SM and the SMSC sends the identification to the recipient over the MT-SM. A SMS can be spoofed to hide the real sender’s identification (see section 3.1 for a more detailed discussion of spoofing).

4.2.2 ROUTING SMS MESSAGE TO APPROPRIATE PSAP

Over the past 10 years, wireless operators have developed sophisticated systems to estimate the location of a wireless caller to 9-1-1, and use those location estimates as the basis for routing that voice call to 9-1-1. Furthermore, in some countries (e.g., US), specific location accuracy requirements for voice calls to 9-1-1 are mandated. Similar geographically-based routing systems for the SMS message to 9-1-1 would need to be developed.

The SMSC has a standardized functionality to forward the SMS message to another SMSC to handle/route the SMS message to the requested email address or phone number.[31] However, when the customer enters a non-specific endpoint for the SMS message, such as “911”, a method of determining the appropriate geographic PSAP does not exist.

An emergency voice call is routed to the appropriate PSAP based on the caller’s rough location that is available from the call set-up. However, SMS does not include any location information in its signaling. Therefore the routing to the correct PSAP based on the SM sender’s location is not supported.

With a voice call to a PSAP, if the subscriber moves the call is maintained with that PSAP. Consider an example where a mobile subscriber sends an SM to a PSAP. The subscriber may move out of the PSAP's jurisdiction or service area. From the PSAP point of view, a subsequent SM from the same subscriber for the same incident must be sent to the same call taker at the same PSAP. However, neither the mobile device nor the network have any association between two SMs sent from the same mobile device, since SMS is a discrete message, not session, service. It is possible that SMS routes subsequent messages to a different PSAP if the subscriber moves to another location. Each message is handled by the SMS individually.

[31] See Section 2 of this document for further details on how an SMS message is routed in existing systems.

4.2.3 BEST EFFORT SERVICE

Wireless operators, SMS users and the industry standardized SMS solution expectations for real-time message delivery delay varies greatly. There are no defined or standardized SMS latency and delay requirements because the SMS service is designed as a background, non-conversational, and low priority service. (It was designed as an add-on to allow unused signaling channels to carry a secondary service.)

It is virtually impossible to guarantee a real-time two-way text communications exchange using SMS technology. SMS is a store-and-forward messaging technology operating over a shared network. As such, SMS was never designed nor deployed to provide any time-sensitive, mission-critical service. There is no guarantee of delivery -- immediate or otherwise -- of an SMS message, whether for commercial or emergency purposes. Also, there is no guarantee of delivery of the proposed response or interaction from the PSAP to the initiating sender. Significantly, most wireless operators do not make level-of-service representations to SMS customers beyond “best efforts”.

In voice networks, wireless operators have the capability of prioritizing voice calls to 9-1-1 over other calls. There is not a capability in SMS systems that allows for prioritization of any SMS messages based upon any criteria. This has been identified in an ETSI Technical Report[32] and a prior 3G Americas analysis of Texting to 9-1-1.[33] Thus, “emergency” SMS messages would have to contend with the other hundreds of millions of daily SMS messages.[34]

Given how SMS is designed and network configurations, SMS emergency messages will not receive any sort of “priority treatment”. SMS does not provide “priority handling” at the air interface nor on the network. SMS messages always contend with other traffic on the control channels, both voice and messaging, with voice calls always having priority over SMS. Thus, delays are likely in the origination and delivery of SMS emergency messages at the air interface. In addition, all SMS emergency messages will go into the queue with the tens of thousands of other non-emergency SMS messages being processed at any given time.

A highly visible example of the ‘best effort’ nature of SMS was when then Presidential candidate Obama announcing his choice for a running mate; this announcement was made in the middle of the night via SMS. The news reports in the following days highlighted the limitations of SMS[35]:

> *"It was the text message read 'round the country. But many had to wait minutes, and some for hours, to receive the announcement of Sen. Joseph Biden as Sen. Barack Obama's running mate... some awaiting word were complaining on various blogs and social networking sites ... as of 3 p.m. Saturday, nearly 12 hours after it was originally sent, Micah Sifry [co-founder of TechPresident, a group blog covering the intersection of politics and technology] still hadn't gotten the text. 'I didn't really mind not getting it, but I do know people who got it at 3 a.m. An older friend of mine e-mailed me at 4 a.m., saying he couldn't sleep and asking, 'Why wasn't this thing sent at 5 p.m.?'.”*

Studies have shown that with an addition of SMS to 9-1-1, wireless operators would need to consider the addition of capacity expansions to their existing SMS systems.[36]

[32] ETSI Report TR 102 444 V1.1.1 (2006-02) “Analysis of the Short Message Service (SMS) and Cell Broadcast Service (CBS) for Emergency Messaging applications”

[33] 3G Americas White Paper, “Characterizing the Limitations of Third-Party EAS over Cellular Text Messaging Services,” Patrick Traynor, Ph.D., September 2008

[34] Based upon CTIA SMS statistics reported at http://www.ctia.org/media/industry_info/index.cfm/AID/10323.

[35] Source: WashingtonPost.com, August 23, 2008. “Obama's Text: Message Received, With a Few Garbles”, Jose Antonio Vargas

4.2.4 SUBSCRIBER MOBILE DURING MESSAGING WITH PSAP

When an SMS user moves across a PSAP service boundary, the wireless network does not support the routing of the SMS messages to the same destination PSAP, as there is no built-in notion of an on-going conversation. There is no ability for the wireless network operator to notify the user or PSAP that the SMS message is sent to a different destination.

4.2.5 NO LOCATION CAPABILITIES FOR SMS

There is no existing method for communicating subscriber location to the PSAP, since the architecture of SMS does not support either determining or delivering location information. Any new development would require substantial redesign of network systems as well as the design of such functionality into new mobile devices.

Wireless networks do not have the ability to locate a user sending an SMS to 9-1-1. The existing emergency call location service is standardized for voice connections and not for a user sending an SMS, which is delivered by two independent services known as MO-SM (Mobile Originated-Short Message) and MT-SM (Mobile Terminated-Short Message). In order to locate a user, the terminal and/or the network needs to collect the measurements for the positioning calculation, the pre-condition of these measurements sometimes require a co-existing voice connection for location purposes with all existing deployments.

The location determination functional deployment for voice calls cannot be used for SMS without a standardized solution and significant wireless infrastructure re-engineering, as well as new mobile devices being deployed to users. It is also unclear whether any new location enabled form of SMS, if even feasible, will introduce any adverse impacts to the existing version and vice versa – e.g., if a legacy mobile device attempted to send an SMS emergency message over an SMS enhanced network or an enhanced mobile device attempted the same over a legacy network. Avoiding such adverse impacts might further increase the cost and complexity of any enhancements.

The lack of location capability for SMS can have impacts to user experience for both the wireless subscriber and for the PSAP call taker (see section 5.1.4).

4.2.6 NO DELIVERY ACKNOWLEDGEMENTS

In SMS, there is no indication of failed SMS to 9-1-1 message attempts. In a conventional voice 9-1-1 call, if the call is not completed for some reason (e.g., trunk congestion, wireless channel unavailability, etc.), the 9-1-1 caller is immediately informed of that fact via the voice call treatment (e.g., fast busy signal, wireless call attempt failure announcement, etc.). However, if an attempted SMS to 9-1-1 transmission were to fail, there may be no immediate indication to the user of that failure on many mobile devices. For example, certain devices deposit a failed SMS message into an "outbox" with no clear indication to the user that the SMS message was not successfully sent. In such cases, the 9-1-1 caller will learn of the failed attempt only when she looks in the message outbox of her mobile device. In addition, there is no indication a SMS message sent from the PSAP is ever delivered to or read by the 9-1-1 caller.

[36] National Communications System. SMS over SS7. Technical Report Technical Information Bulletin 03-2 (NCS TIB 03-2), December 2003

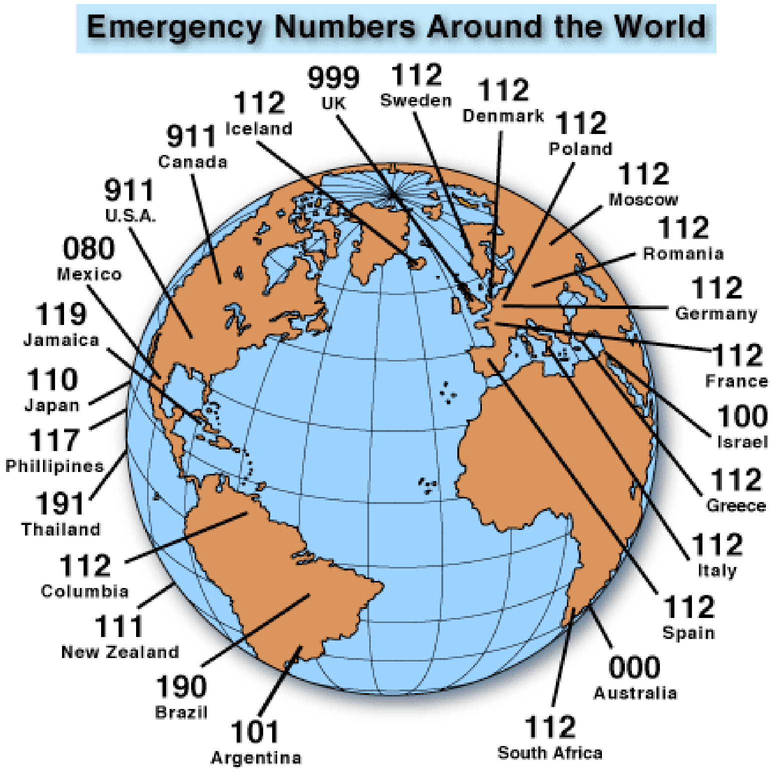
4.2.7 RECOGNITION OF "911" AS VALID SMS DESTINATION

Wireless networks may have "911" configured in the SMSC as an invalid destination for an SMS message. Depending upon the network, the wireless operator might ignore the message to 9-1-1, send some type of error response and/or send a response message indicating that text messaging to 9-1-1 is not currently supported.

Wireless operators would need to modify their SMS systems to support messages to "911", or any other emergency dial string. Such emergency dial strings would need to be recognized by the SMSC as a valid endpoint for SMS messages.

4.2.8 INTERNATIONAL EMERGENCY NUMBERS

Wireless subscribers roaming to United States or Canada from other parts of the world use different telephony numbers for contacting emergency services and may not be familiar with the use of "911" or any other identity that would be used for a text to 9-1-1 service. If the home jurisdiction of these roaming subscribers support text messaging to emergency services, these subscribers may try to use that capability whenever they are in the United States or Canada to contact emergency services. Their text messaging request may be routed to the emergency services of their home jurisdiction instead of the local emergency services.



DISPATCH Monthly graphic

Figure 27: International Emergency Number[37]

[37] See http://www.911dispatch.com/911/911_world.html

4.2.9 UNAUTHORIZED OR FRAUDULENT MOBILE DEVICES

As required by the FCC, unauthorized or fraudulent mobile devices and mobile devices that do not have a SIM inserted are all able to make emergency services voice calls. However, existing wireless systems do not permit unauthorized or fraudulent mobile devices to originate SMS messages for any use, including potential emergency services.

Furthermore, if a service provider offers SMS as a subscription service, a mobile device that is not authorized for SMS will not be able to initiate an SMS message to 9-1-1.

Major wireless system changes would be required to enable all mobile devices to initiate SMS messages to 9-1-1. However, it is not possible for a PSAP to send an SMS message back to a fraudulent mobile device or to mobile devices that are not registered in the serving wireless network. SMS is a connectionless[38] service and a PSAP cannot send an SMS message to a mobile device that does not have a valid identity or to a mobile device that is not authorized for service in a wireless network.

4.3 CONSIDERATIONS FOR PSAP SYSTEMS

This section discusses the following topics that the PSAP should consider for the support of SMS to 9-1-1 messages:

- Connectivity of subscriber to a specific call taker/dispatcher at the PSAP
- Assembly of multiple SMS messages into a logical sequence
- Forwarding of SMS messages to appropriate PSAP
- Spamming of PSAP via SMS messages

4.3.1 CONNECTIVITY OF SUBSCRIBER TO SPECIFIC CALLTAKER/DISPATCHER AT PSAP

When subscribers initiate the SMS message, they will be sending the SMS message to “911”. Assuming that the wireless operator has developed a capability to route the SMS message to the geographically relevant PSAP, this PSAP will need to determine a destination call taker to handle these text messages, as the wireless operator will need a single destination endpoint to route the SMS-to-9-1-1 messages.

4.3.2 ASSEMBLY OF MESSAGES INTO LOGICAL SEQUENCE

As a consequence of section 4.3.1 above, the PSAP would also need to have a method of assembling the SMS to 9-1-1 messages into a logical sequence. As SMS is a store and forward system, the PSAP point of logical sequence assembly would need to take into account various delays in SMS message delivery and establish a system that puts the SMS messages in the proper order so that the message sequence makes logical sense.

[38] In telecommunications, connectionless describes communications between two network end points in which a message can be sent from one end point to another without prior arrangement. The device at one end of the communication transmits data addressed to the other, without first ensuring that the recipient is available and ready to receive the data. See http://en.wikipedia.org/wiki/Connectionless_protocol.

There is no “end” of SMS based logical sequence (e.g., neither end is aware of when the text based conversation has ended). Consequently, neither the user nor the PSAP will be able to determine when the SMS-based text conversation has completed. Since SMS is not a session-based service, SMS messages do not contain any sort of sequence or order information; hence, PSAPs lack a basis for determining if a SMS message was dropped, was missed, or was out-of-sequence. In addition, any attempt to present SMS messages in order would require that received SMS messages be held for some period, waiting to see if a SMS message with an earlier or out-of-order timestamp arrives. This adds additional delay to handling an emergency situation.

4.3.3 MESSAGE FORWARDING TO PROPER PSAP

Assuming that the wireless operator might have developed a capability to route the SMS message to the geographically appropriate PSAP, it is possible, and indeed likely, that the first SMS message from the caller to the PSAP could be delivered to a PSAP that is not the PSAP which would handle a response (Police, Fire, EMS) to the SMS to 9-1-1 request for service. PSAPs would need technical enhancements to be developed and operational methodologies in place to handle a text message that had been forwarded from another PSAP (to include the dissemination of history and re-ordering and assemblage of prior messages between the original PSAP and the customer).

If the SMS message is forwarded, there is no technical capability that will allow the MO-SMS messages to “follow” the forwarding to an alternate PSAP. With a voice call, transfer of the circuit switch path is possible and allows an orderly transfer of the voice call to alternative PSAPs. This capability cannot be done with SMS.

4.3.4 SMS SPAMMING TO PSAP

The possibility exists that certain individuals would want to spam a PSAP with large volumes of messages for purposes of abuse, or potentially sending false messages for help to occupy PSAP response assets (Police, Fire, EMS), or to harass or harm an innocent subscriber by directing police response to the subscriber's location, or to cause an innocent subscriber to be blamed for sending false emergency requests. As the wireless operator does not have the capacity to analyze each individual SMS, nor will they block any mobile originated SMS including an SMS to 9-1-1, the PSAP will likely need to develop technical enhancements and operational methodologies on spam or potential spam abuse of the PSAP. It is possible for individuals with malicious intent to generate SMS to 9-1-1 messages without using a wireless network.

4.4 CANADA — REPORT TO CRTC BY EMERGENCY SERVICES WORKING GROUP (ESWG)

On January 21, 2010, the Emergency Services Working Group (ESWG) of the Canadian Radio-television Telecommunications Interconnection Steering Committee (CISC) provided a report to the Canadian Radio-television and Telecommunications Commission (CRTC) on Text Messaging to 9-1-1 (T9-1-1) Service[39].

The following limitations of SMS were highlighted in the report:

- SMS 9-1-1 text messages cannot be prioritized over regular SMS text messages, exposing them to the same latency and delays as regular SMS text messages.

[39] Text Messaging to 9-1-1 (T9-1-1) Service, Canadian Radio – television and Telecommunications Commission Interconnection Steering Committee (CISC) Report to the CRTC by the Emergency Services Working Group (ESWG), Report Number: ESRE0051, January 21, 2010.

- The mobile device must have a valid subscription to support the SMS service.
- A prepaid mobile device must have sufficient funds to support multiple text messages with the T9-1-1 service.
- Wireless systems have a limitation of 160, 140, or 70 characters per SMS message, depending on the deployed network equipment and handset used. In order to reach all mobile devices on all networks and to ensure the message is not broken in parts that could be received in wrong order.
- SMS messages are based upon a “store and forward” principal. They have no guaranteed delivery times or quality of service associated with it.
- The SMS service may be affected by high SMS text volume, e.g. during New Year’s Eve, when there is a surge of SMS messages. It has been estimated that on New Year’s Eve in 2007, 4.6 SMS messages per capita were sent.
- SMS message senders do not receive confirmation of messages sent.
- Likewise, error messages are not sent to the mobile device when a SMS message has not been received by the destination.
- Some wireless mobile devices cannot accommodate a 3-digit short code, e.g. 9-1-1. As a result, the Short Code made available for a SMS to 9-1-1 service must be at least five digits long.
- SMS infrastructure may not have “5 nines” reliability (i.e. 99.999% uptime). In other words, the SMS service may not have the same availability as the remainder of the wireless network.
- The SMS service is unable to automatically provide a location. Currently, there is no standard for the Interworking of SMS subsystems and wireless Phase II E9-1-1 systems.
- The base of mobile devices within each wireless service provider need to be audited to ensure that they can transmit both voice and SMS text at the same time.
- SMS “spoofing” of the embedded telephone number may occur when a fraudster manipulates address information in order to impersonate a mobile user. Some short codes Application Service Providers (ASPs) have mechanisms to prevent spoofing.
- SMS messages may be sent from a web page and would contain a 10-digit dummy number. [It is not understood by the ESWG at this point in time whether or not this method can support two-way text messaging.]
- SMS to 9-1-1 messages may contain abbreviations not understood by the message receiver.
- Foreign roamers would not be supported because their text messages would be routed back to their home networks. Domestic Roamers are supported if network interconnectivity permits it, e.g. the case of one wireless service provider’s subscriber roams onto the network of another wireless service provider. SMS messages are normally routed back to the home wireless service provider’s network; therefore this is the route that a SMS T9-1-1 message would take.

The recommendations of this report to the CRTC can be summarized as follows:

- A near-term solution for T9-1-1 service consisting of SMS messaging preceded by a silent wireless voice call with a "DHHSI" indicator for PSAPs, may be developed and trialed by the ESWG. (Note: DHHSI is the EWSG acronym for Deaf, Hard of Hearing, or Speech Impaired)
- This solution for the technical trial is confined to the DHHSI community and pre-registration for the T9-1-1 service is required.
- The technical trial is expected to span approximately 12 to 18 months.
- DHHSI persons wishing to use this service must pre-register their wireless handsets prior to using the T9-1-1 service.
- If the CRTC wishes the service to become available to the general population, the T9-1-1 service will require redesign by the ESWG.
- A long-term solution for the DHHSI community and perhaps for the entire Canadian population using text methods such as IM or RTT will depend on the maturation level of IP networking and NG9-1-1.

4.5 CONSIDERATIONS FOR MIGRATION TO NEXT-GENERATION

The wireless industry has started the migration to next-generation systems. This is an ongoing, multi-year effort that imposes significant costs and promises major benefits. Inherently, any re-engineering of legacy SMS standards, along with upgrades to wireless operator networks and mobile devices, to support emergency SMS will detract from resources that could otherwise be used to advance next-generation, hence delaying a better solution in order to deploy a limited and constrained one. Next-generation promises to support both voice and non-voice (including text and video) emergency services, on an equal basis, with the same signaling, routing, location determination, location disclosure, and other critical aspects of 9-1-1.

In other words, a complex and fundamentally limited solution for 9-1-1 text may displace much better solutions that are not fixated on SMS. It should further be noted that even a limited SMS based solution will probably require users to obtain new mobile devices, making any such solution less attractive in many ways to the user than a better solution that also requires new mobile devices.

5. USER CONSIDERATIONS FOR EMERGENCY SERVICES

This section describes the considerations for the user experience that would occur for SMS to 9-1-1 functionality. These considerations are discussed for both the wireless subscriber and for the PSAP call taker. A simple SMS to 9-1-1 scenario is also presented with the associated considerations that will occur for both the wireless subscriber and for the PSAP call taker.

5.1 CONSIDERATIONS FOR WIRELESS SUBSCRIBER

The first voice 9-1-1 system became operational in early 1968 in Alabama and adoption by other communities soon followed. Deployment of voice 9-1-1 in the United States is almost ubiquitous. Consequently, the citizens have developed a set of expectations about the availability, reliability, and security of voice 9-1-1.

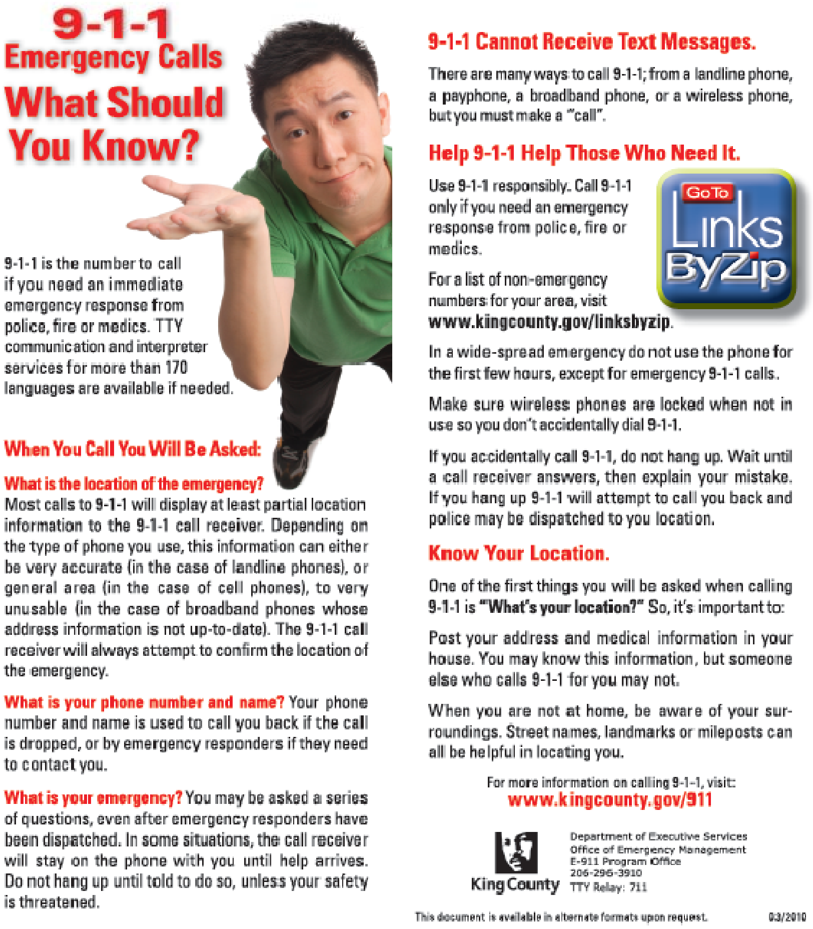
5.1.1 AVAILABILITY

The citizen users have the expectation that help from emergency services will be available whenever they dial 911 on their wireline or wireless telephony device. The expectation from the wireless user is they can reach 9-1-1 no matter what their location as long as they have adequate cellular coverage. It is a rare occurrence when the wireline or wireless services are unable to comply with this expectation.

For any potential SMS-based, or more generally, text-based emergency services, wireless users may automatically assume that the ability to text to 9-1-1 exists in all locations, based upon their experiences with voice based emergency services. However, it is likely that not all PSAPs would support SMS based emergency communications. It is possible that all serving PSAPs in a metropolitan area may not support SMS based emergency communications. Consequently, as the wireless user roams to other cities or moves within the same metropolitan area, the wireless user may roam in and out of different PSAP coverage areas with different capabilities for the support of SMS based emergency communications. The wireless user will have no indication of when they are within a PSAP boundary which supports SMS based emergency communications and when they are outside of the area that supports SMS to 9-1-1.

For example, in 2009, there was significant press related to the launch of an SMS to 9-1-1 service in Blackhawk County, Iowa. This announcement made national news, and as a result, many citizens assumed that SMS to 9-1-1 was available “everywhere”. Due to the high level of misconceptions this announcement caused, King County Washington had to issue a public statement that SMS to 9-1-1 was not supported in King County and that the citizens should dial 9-1-1 to access voice based emergency services[40].

[40] See http://www.kingcounty.gov/safety/E911/PublicEducation.aspx



9-1-1 Emergency Calls What Should You Know?

9-1-1 is the number to call if you need an immediate emergency response from police, fire or medics. TTY communication and interpreter services for more than 170 languages are available if needed.

When You Call You Will Be Asked:

What is the location of the emergency? Most calls to 9-1-1 will display at least partial location information to the 9-1-1 call receiver. Depending on the type of phone you use, this information can either be very accurate (in the case of landline phones), or general area (in the case of cell phones), to very unusable (in the case of broadband phones whose address information is not up-to-date). The 9-1-1 call receiver will always attempt to confirm the location of the emergency.

What is your phone number and name? Your phone number and name is used to call you back if the call is dropped, or by emergency responders if they need to contact you.

What is your emergency? You may be asked a series of questions, even after emergency responders have been dispatched. In some situations, the call receiver will stay on the phone with you until help arrives. Do not hang up until told to do so, unless your safety is threatened.

9-1-1 Cannot Receive Text Messages.

There are many ways to call 9-1-1; from a landline phone, a payphone, a broadband phone, or a wireless phone, but you must make a "call".

Help 9-1-1 Help Those Who Need It.

Use 9-1-1 responsibly. Call 9-1-1 only if you need an emergency response from police, fire or medics.

For a list of non-emergency numbers for your area, visit **www.kingcounty.gov/linksbyzip**.

In a wide-spread emergency do not use the phone for the first few hours, except for emergency 9-1-1 calls.

Make sure wireless phones are locked when not in use so you don't accidentally dial 9-1-1.

If you accidentally call 9-1-1, do not hang up. Wait until a call receiver answers, then explain your mistake. If you hang up 9-1-1 will attempt to call you back and police may be dispatched to you location.

Know Your Location.

One of the first things you will be asked when calling 9-1-1 is **"What's your location?"** So, it's important to:

Post your address and medical information in your house. You may know this information, but someone else who calls 9-1-1 for you may not.

When you are not at home, be aware of your surroundings. Street names, landmarks or mileposts can all be helpful in locating you.

For more information on calling 9-1-1, visit:
www.kingcounty.gov/911

King County

Department of Executive Services
Office of Emergency Management
E-911 Program Office
206-296-3910
TTY Relay: 711

This document is available in alternate formats upon request. 03/2010

Figure 28: King County Washington Brochure on 9-1-1 Emergency Calls

5.1.2 ACCESSIBILITY

Based upon decades of educational programs, signs, and banners, citizens have been taught to dial 911 from wireline or wireless telephony devices to request emergency services. Therefore, it is natural for citizens to assume that "911" would be the address for any SMS based emergency services.

However, "911" is not a valid short code for SMS communications. SMS short codes require 5 or 6 digits.

Carriers use short codes with fewer digits for carrier-specific programs (e.g., "Text 611 to see how many minutes you have remaining on your plan"). Common short codes in the U.S. are administered by NeuStar, under a deal with Common Short Code Administration (CSCA) under CTIA. Short codes for commercial purposes are leased by the wireless operators from the CSCA.

Also, there is no national short code defined for SMS based emergency communications. As a result, the user may be required to know the individual SMS short codes on a per metropolitan area basis.

5.1.3 RELIABILITY

Whenever citizen users have an emergency and need assistance, they expect to be able to contact the PSAP for help. The telecommunications industry, in conjunction with the PSAPs, is able to comply with the user's expectation of being able to call 9-1-1 for assistance under emergency conditions. Calls to PSAPs are completed quickly and have a very high percentage of successful call connections. If the call is prematurely disconnected, the PSAP call taker has the information to be able to call back the citizen, if the call was made from an initialized (subscribed) device.

For any potential text based emergency services, the wireless user would automatically assume that their message would be delivered quickly and that the PSAP call taker would take immediate action. However, SMS is not a real-time, nor even a necessarily reliable, service. SMS is a store-and-forward, "best effort" service and, consequently, there could be delays or loss in the delivery of the SMS message to the PSAP or in the delivery of any subsequent SMS messages from the PSAP call taker back to the wireless user, assuming that the wireless user is within the boundaries of a PSAP that supports SMS based emergency services.

5.1.4 USER LOCATION

Citizen users have the expectation that emergency services know their location when they call emergency services and, therefore, know where to send assistance. For wireline services, this assumption is generally correct. For wireless services, it depends on the PSAP capabilities, wireless operator network capabilities, and mobile device capabilities and upon the requirements of the FCC for location as part of 9-1-1 calls.

However, for any potential SMS based emergency services, there is no location information available in the SMS message and signaling protocol. Unlike voice 9-1-1 calls over wireline and wireless networks, current wireless telephone networks do not have the ability to determine and deliver caller locations for SMS messages. Therefore, the wireless user would have to provide that location information to the PSAP as part of the SMS text (however, there is still the problem of routing the text to the PSAP).

Some proposed third party solutions require that wireless users enter the zip code of their current location in the text message to the PSAP. An exchange may be as follows:

1. Emergency caller sends emergency text: "I need help"
2. Message automatically generated back to the caller: "What is your zip code or city?"
3. Emergency caller has to send another message with this location information
4. Initial message is then routed to a 9-1-1 center serving that zip code

One flaw in this method is that, except for a few locations such as home, office, or school, the wireless subscriber may have no idea of the zip code of their current location. It is also easy for users to forget to do, as well as easy to get wrong. Furthermore, even when a zip code is provided and is correct, a zip code indicates an area that will generally be far too large for public safety dispatch to find the user. Additionally, because zip codes and PSAP boundaries are independent of each other, it is unreliable to use zip codes for routing to the correct PSAP.

Some of the latest generation devices have A-GPS capabilities. As described in the example smartphone application in section 2.8.1, A-GPS location information could be included in the text of the emergency SMS message if the mobile device manufacturer includes the capability to include the A-GPS data within an SMS message. However, the generic text messaging applications on many mobile devices do not support the automatic inclusion of A-GPS information in text messages. Either a special application such as the one described in section 2.8.1 has to be used or the wireless user has to find the A-GPS information on their mobile device for manual inclusion into the text message.

Another important consideration is that the A-GPS data is not continuously updated in the mobile device in order to minimize the impact to the battery life. Thus, if the mobile device were able to put the x,y location coordinates in the message, or if the user were able to obtain them from the mobile device, it can take up to 30 seconds for the A-GPS data to “refresh” with accurate data.

Any solution that adds data to an SMS necessarily increases the amount of text, and hence reduces the characters available for the user to describe the emergency, or makes it more likely that the SMS message will exceed length limits and will need to be segmented. Support for segmentation is not universal. Even when supported, segmented messages inherently increase the risk of loss, delay, and out-of-order receipt.

The lack of location support by SMS will have two major consequences. The first and less important is that an SMS message will likely be delivered to a PSAP that does not have jurisdiction over the area the user is located in. The second and by far the more important is that the PSAP call taker may not be able to dispatch public assistance to the user. Unless the user provides precise location information in the SMS message itself (e.g. a street address together with town or city) or the PSAP call taker can somehow communicate further with the user (e.g. by calling back the user using normal voice service or by establishing an SMS dialogue with the user), the PSAP call taker may be able to do little more than log the message and put public safety in the assumed area of the user on some kind of alert. The probability that a user under stress in an emergency situation where SMS has to be used will fail to include sufficient location information in a relatively small message is likely to be high. This deficiency may be doubly dangerous because having sent what the use thought to be a valid SMS appeal for help; the user may be lulled into a false sense of security and make less of an attempt to summon help by other means. Experience with the existing voice call related E9-1-1 service has shown that the availability of reliable and accurate location information can often be critical in summoning help in time-critical situations.

5.2 CONSIDERATIONS FOR PSAP CALL TAKER

The PSAP call taker is trained and experienced in the handling of voice based requests for emergency services. However, an SMS based emergency service would have different characteristics and consequently would have different considerations for the PSAP call taker and the PSAP systems.

5.2.1 EVALUATION OF CALLER

With voice based emergency services, the PSAP call taker can perform an evaluation of the calling party and validate the emergency situation. For example, on voice based emergency services, the PSAP call taker can do the following types of evaluations:

- Is the caller genuinely stressed or is the caller joking?
- Is the caller a child potentially playing a game?
- Is the caller potentially inebriated or mentally impaired?

With any potential SMS or text based emergency services, the PSAP call taker will not be able to do any evaluation of the caller. In fact, it may not even be the person in need of emergency services that makes the "call". Consequently, the PSAP call taker would have to assume all communications are valid and may have to dispatch the limited first responder responses even to false emergency situations.

5.2.2 ANCILLARY INFORMATION

In addition to the direct verbal information that is being provided to the PSAP call taker by the caller, the PSAP call taker can collect additional ancillary information. For example, the PSAP call taker can hear any background noise. This background noise could be of assistance in the evaluation of the caller as discussed above or in the preparation of the first responders for the environment that they will be encountering. For example, is the event an isolated occasion or is the event happening in a crowded environment.

However, with any potential SMS or text based emergency services, the PSAP call taker would not have access to any of this ancillary information.

5.2.3 OVERLOAD POTENTIAL

In recent months, there have been reports of application software under development for smartphones that would automatically dial 911 and continue dialing on a repeated basis. An example use of these applications would be wireless users attempting to get their stolen smartphone located and returned. Some of these occurrences have caused 9-1-1 emergency services to be unavailable to other citizens due to either a saturation of all of the 9-1-1 voice call lines to the PSAP or an overload of the PSAP systems. In some cases, this situation was cleared only after the PSAP call taker determined the location of the smartphone and dispatched first responders to that location to stop the operation of the smartphone.

In any potential SMS based emergency services environment, a similar SMS based program could be programmed for smartphones that could generate repeated SMS based emergency messages (see section 2.8.1). A small number of smart devices could easily generate enough SMS messages to overload the PSAP systems and call takers.

However, as opposed to voice based emergency service requests, the PSAP call taker has no location information for this smart device unless the location information was included in the text of the SMS message. Of course, a person with malicious intent would not include the smart device location information in the SMS message. The only way to stop this flood of SMS messages is to locate the smartphone and discontinue the transmissions; but this action is not possible since the location of the smartphone is not known.

5.2.4 LANGUAGES AND TERMINOLOGY

Most metropolitan areas have citizens who use a variety of languages. PSAP call takers are trained to process voice based emergency calls in languages other than English. Even if the PSAP call taker does not understand the language of the caller, the PSAP call taker could have some idea of the situation by evaluation of the caller's state and background noise information (as discussed above) to determine the validity of the emergency in order to dispatch emergency services.

Most the issues of multiple languages with text-based communications are even more complex. Many languages have their own character sets and language symbols (e.g., Cyrillic, Hebrew, Arabic, Chinese, and Japanese).

Internationalization of Internet protocols to support character sets other than ASCII has been a difficult process (fraught with unexpected technical and social challenges) that has been ongoing for over two decades. The PSAP systems receiving SMS based messages in languages other than English would have to be able to interpret and present the characters and language symbols to the PSAP call taker. Many character sets require more bits per character, further reducing the number of characters than can be sent in a single SMS message. Of course, even with proper presentation of the language characters and symbols, the PSAP call taker may not be able to interpret the contents of the SMS based emergency services message.

In addition to the formal languages of the various countries and regions of the world, there is also the specialized terminology of the Internet user community; especially the user community associated with text messaging and social networking. These types of users have developed their own terminology for the message content, typically 3, 4, or 5 letter acronyms. Much of this terminology is specific to the user's unique social networking community. The PSAP call taker may or may not be familiar with these acronyms and their associated meanings.

5.2.5 POTENTIAL IMPACT OF VIRTUAL REALITY

Virtual reality based games and social interactions are very popular on the Internet and have been traditionally associated with PC based connectivity. However, advancements in smart device applications are facilitating the expansion of the virtual reality world to smartphones, wireless tablets, and wireless netbooks. This virtual reality environment supports communications between members via their avatars. Depending on the implementation of the virtual reality environment, some of these communications could be SMS based.

There are members of the emergency services community who believe that any system that supports communications between citizens must also support communications with emergency services. Based upon this belief, the virtual reality gaming environment would need to support the capability to do SMS based emergency communications with the real world PSAP. This raises the possibility of false emergency requests from the virtual reality games to the real world emergency services. For example, the user's avatar in the virtual world has an emergency in the virtual world but the request is accidentally sent to the real world PSAP for the current location of the wireless device.

It is also not clear that users would expect to use a virtual reality or other specialized device or application for emergency communications.

5.3 "SIMPLE" SMS TO 9-1-1 SCENARIO

Consider the following scenario:

- Brian is home alone late at night and hears a noise at his back door. Someone has just entered his house.
- Brian investigates and sees the intruder, grabs his mobile device and hides in the upstairs closet.
- Not wanting to give his presence away with a voice call, Brian enters an SMS message "Someone broke into my house" on his mobile device, enters a destination of "911", and hits send…

Problem #1 → Brian entered "911" but "911" is not a valid common short code for sending an SMS. A common short code in the U.S. must be a 5 or 6 digits (i.e. "91156").

- Brian expects to get a reply that "Help is on the way", but let's explore exactly what happens…

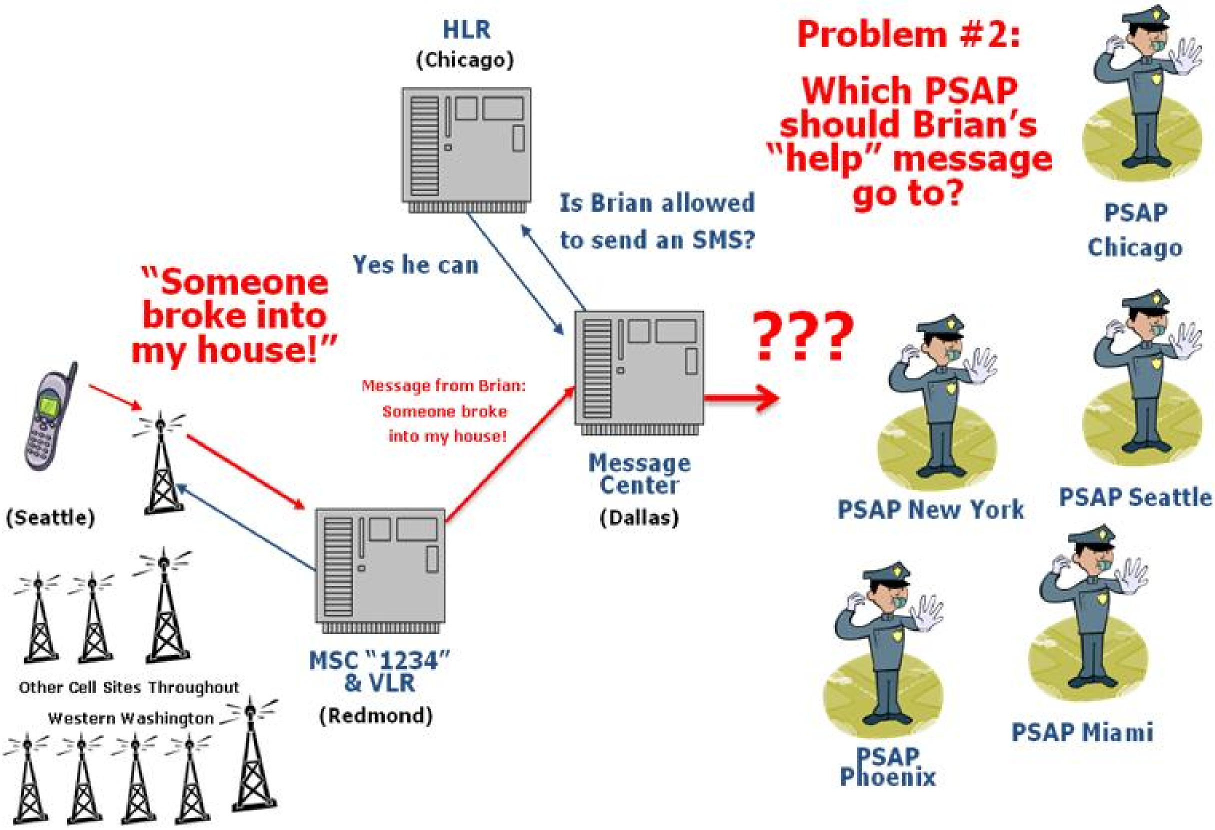
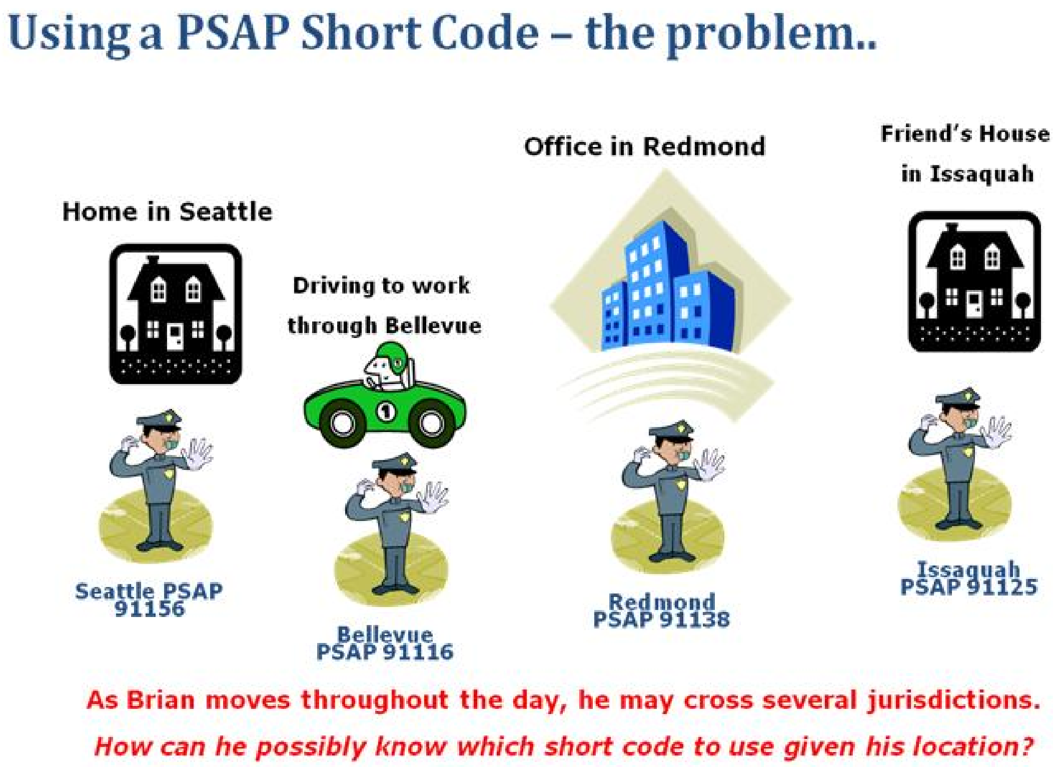

HLR
(Chicago)
Problem #2:
Which PSAP should Brian's "help" message go to?
PSAP Chicago
Is Brian allowed to send an SMS?
Yes he can
"Someone broke into my house!"
Message from Brian: Someone broke into my house!
???
Message Center
(Dallas)
PSAP New York
PSAP Seattle
(Seattle)
Other Cell Sites Throughout Western Washington
MSC "1234" & VLR
(Redmond)
PSAP Phoenix
PSAP Miami

Figure 29: "Simple" SMS Scenario

The first and immediate problem is which PSAP should Brian's request go to? The Message Center does not know where Brian is sending the message from, as there is no need for it to know for regular SMS services. The Message Centers typically support a wireless operator's entire network. For a nationwide wireless operator, Brian can be anywhere in the country. Without knowing where Brian is, the message center cannot route to the appropriate PSAP. Suppose that Brian did not send the message to "911" but to a special short code that Brian knows is for his local PSAP. Say that short code is "91156". Now, the Message Center can route the SMS message to the PSAP associated with the short code "91156". However, the problem (#2) with this is that every PSAP in the country would have to have a special short code so it is uniquely identified, and users would have to know the code for not only their home area, but also all areas they may be traveling to...



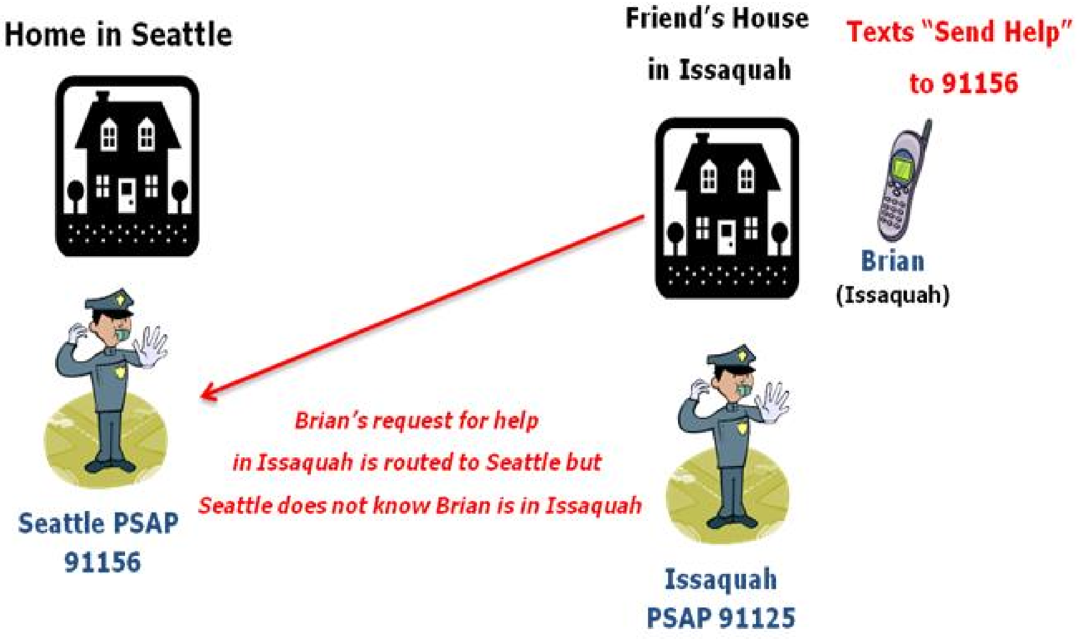
Using a PSAP Short Code – the problem..

As Brian moves throughout the day, he may cross several jurisdictions.

How can he possibly know which short code to use given his location?

Figure 30: PSAP Short Code Problem

What could happen is If Brian is outside his immediate home area and uses his home PSAP short code, the SMS text message for help would be routed to his home PSAP and not the PSAP for his location:



Brian's request for help in Issaquah is routed to Seattle but Seattle does not know Brian is in Issaquah

Figure 31: PSAP Short Code Problem When Away From Home PSAP Area

What would the Seattle PSAP do with this information? The Seattle PSAP has no idea Brian is in Issaquah.

Let’s suppose somehow we are able to figure out which PSAP to route to…

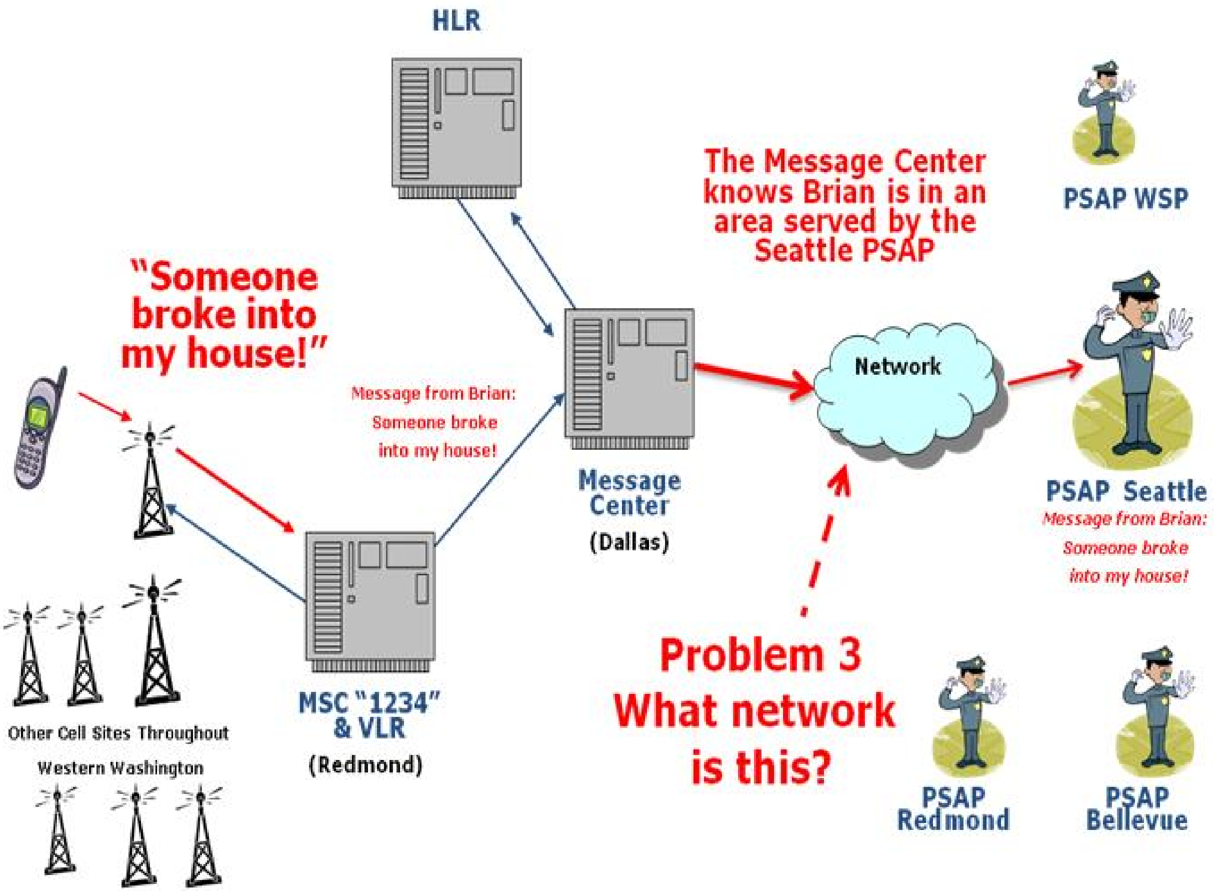

HLR
The Message Center knows Brian is in an area served by the Seattle PSAP
PSAP WSP
"Someone broke into my house!"
Message from Brian: Someone broke into my house!
Network
Message Center
(Dallas)
PSAP Seattle
Message from Brian: Someone broke into my house!
Problem 3
What network is this?
Other Cell Sites Throughout Western Washington
MSC "1234" & VLR
(Redmond)
PSAP Redmond
PSAP Bellevue

Figure 32: Which Network Problem

Problem #3 → What network is between the Message Center and the PSAP? To provide reliable and “near real-time” routing of the message from the Message Center to the PSAP, what network is used?

- Internet?
    - Reliability issues
    - Routing Delays
    - Privacy Issues
    - Security Issues
    - Denial of Service (DoS) attacks
    - “Man in the Middle” (MiM) attacks
- Maybe a private network to be developed and managed by the “PSAP” community?

Assume we have a network between the SMSC and the PSAP. Brian's SMS message is received at the Seattle PSAP…now what? All the Seattle PSAP has is "Send Help", but there are vital unanswered questions at the PSAP:

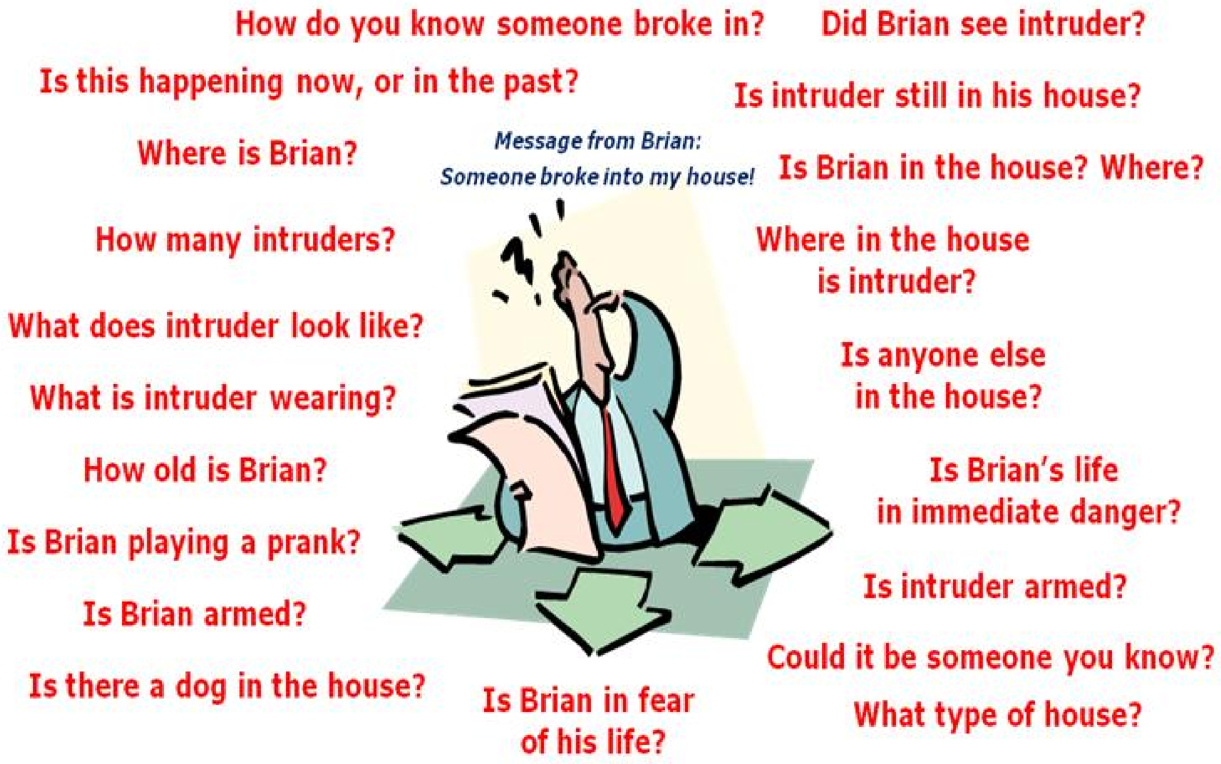

How do you know someone broke in?
Did Brian see intruder?
Is this happening now, or in the past?
Is intruder still in his house?
Where is Brian?
Message from Brian:
Someone broke into my house!
Is Brian in the house? Where?
How many intruders?
Where in the house is intruder?
What does intruder look like?
Is anyone else in the house?
What is intruder wearing?
How old is Brian?
Is Brian's life in immediate danger?
Is Brian playing a prank?
Is intruder armed?
Is Brian armed?
Could it be someone you know?
Is there a dog in the house?
Is Brian in fear of his life?
What type of house?

Figure 33: Unanswered PSAP Call Taker Questions

Answers to these questions will dictate type of response needed:

- One police unit? Several police units?
- Medics?
- No response?
- Urgent response?
- Routine response?

Answers to these questions are essential to protect the public safety personnel responding to the scene, as well as the public. The PSAP cannot rely only on information in one SMS. Lack of information may result in inappropriate response:

- Too little of a response
- Too big of a response
- May impact someone else that can't get help because resources are tied up

- Too late

Problem #4 → A Public Safety issue to resolve: Without a real-time dialog, the PSAP call taker will not be able to get all the answers needed for an appropriate response. This will require the development of a comprehensive policy on how to handle and respond to SMS to 9-1-1 messages; a short SMS text message by John Q. Public is not guaranteed to provide the information the PSAPs need to determine an appropriate response.

So why doesn't the PSAP call taker just send questions back to Brian to ask these vital questions prior to initiating the response using SMS? But first, what information does the PSAP have available from this incoming SMS? The PSAP has:

- A text message
  - "Someone broke into my house!"
- A phone number of the mobile device that "apparently" sent the text message
  - Maybe can be used to send a message back to Brian
  - Maybe can also be used make a standard voice call to Brian
- Maybe, if the solution can be provided, a rough location of the user
  - Which cell the user is in

Each Question from the PSAP is delivered as a separate MT-SMS (see section 2.3):

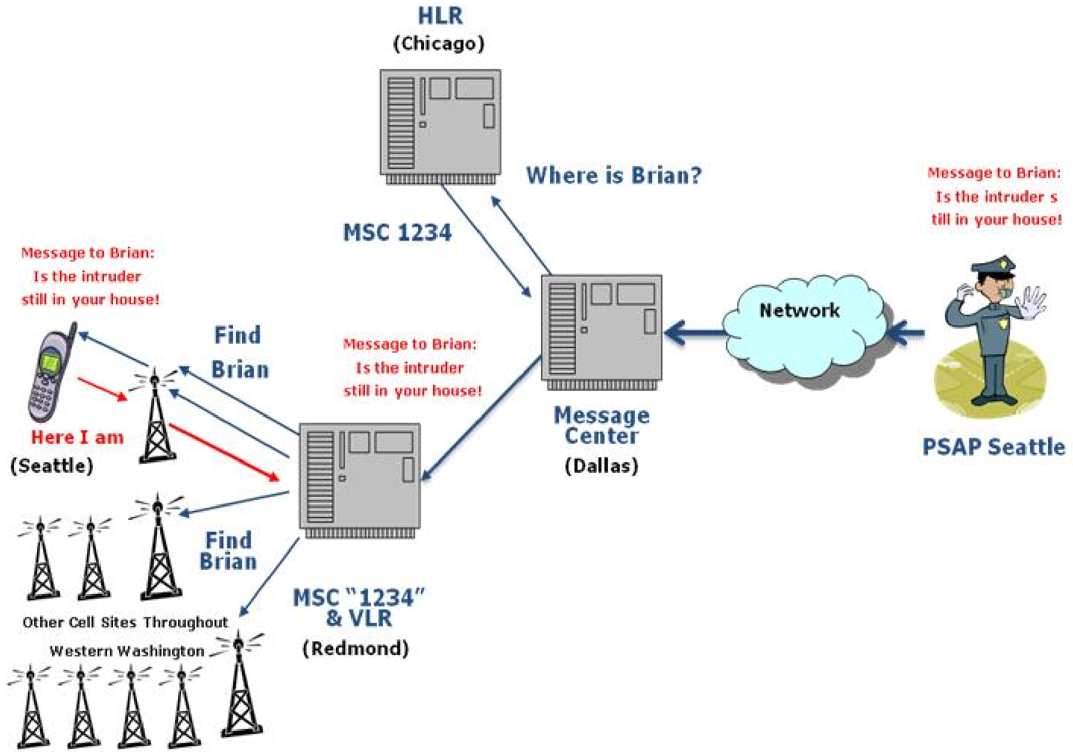


Figure 34: Each PSAP Question as Separate MT-SMS

Each response back to the PSAP from Brian is a separate MO-SMS (see section 2.3):

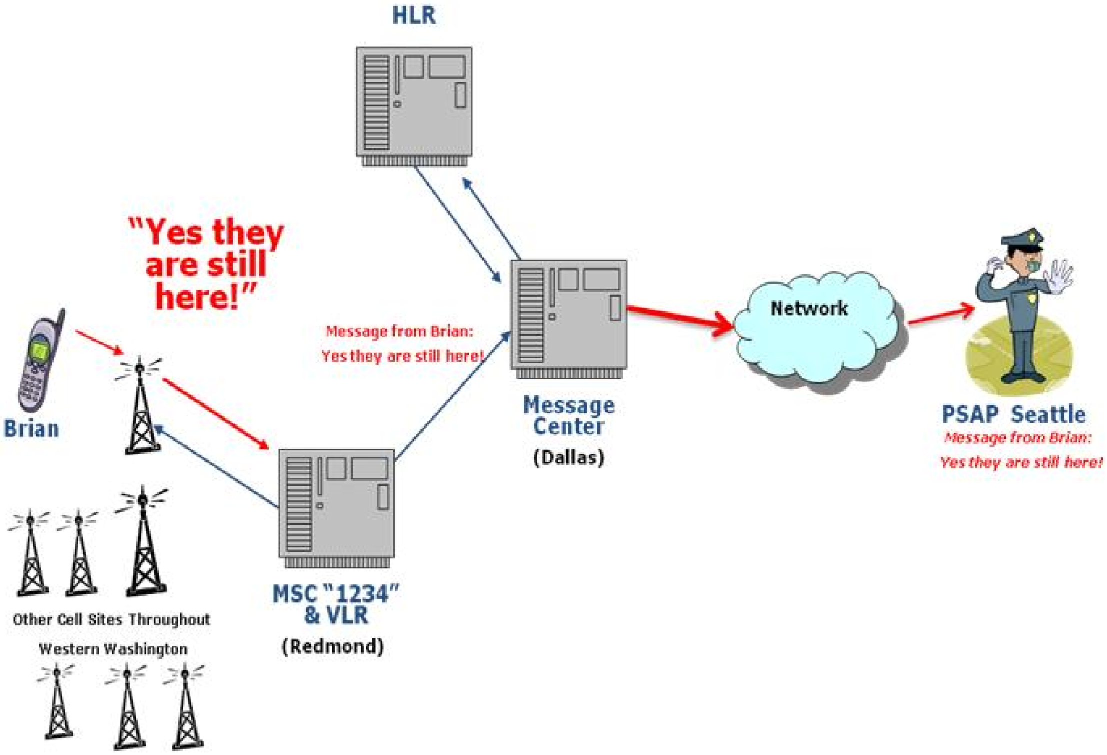


Figure 35: Each Response to PSAP as Separate MO-SMS

If the PSAP has a lot of questions to ask Brian, there is the potential for significant delays in the store-and-forward SMS network. It also takes time for each SMS message to be sent and a SMS response received. Also, SMS messages and SMS responses are not guaranteed to arrive in sequence, especially if there are concatenated SMS messages in the sequence. Thus it is possible for the responses to be incorrect as they may have come out of sequence; this could potentially be a significant issue. Consider the following simple example:

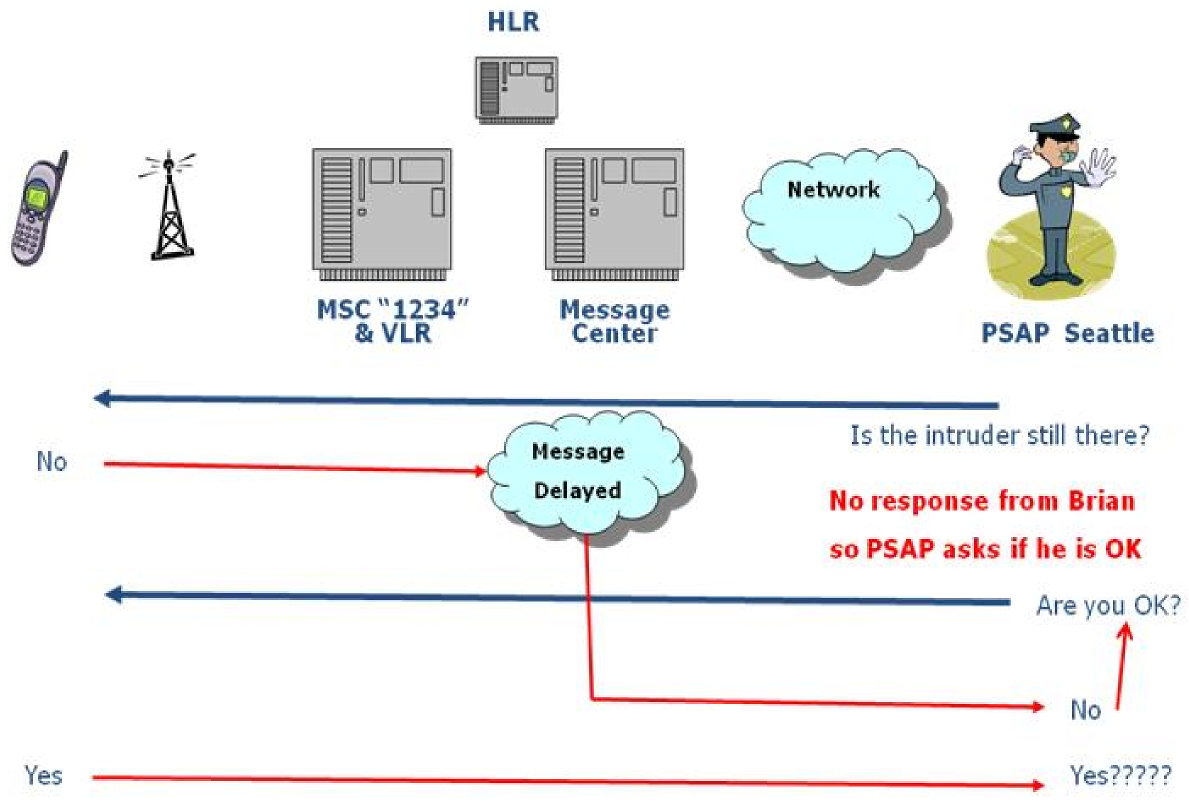


Figure 36: Out of Sequence Responses to PSAP

In response to Brian's original SMS message, the PSAP sends a SMS message to see if the intruder is still there. Brian responds to this SMS message to say "no", but the SMS message for whatever reason is delayed and does not reach the PSAP. The PSAP waits for a response and does not see one, so out of concern sends a second SMS message to see if Brian is OK. Brian receives the second SMS message and responds back "yes" indicating he is OK. After the second SMS message is sent, Brian's response to the first PSAP SMS message finally makes it back to the PSAP. There are no 'sequence numbers" contained in SMS, so the "no" response is assumed to be for the second question ("Are you OK?"). The PSAP call taker incorrectly believes Brian is not OK and may initiate a response based on that. At some later point, the response to the PSAPs second question arrives, and the call taker may not know which response goes to which question.

6. PEOPLE WITH DISABILITIES

People with disabilities are understandably interested in the SMS to 9-1-1, or more generally "text to 9-1-1" capability, especially for individuals with hearing or speech impairments. Wireless operators and manufacturers also understand this need. While mobile devices support connection to external TTY devices, people with disabilities have expressed that they find it burdensome to carry a TTY device with them as they go about their daily activities (as any of us would). Consequently, these users are looking for a solution that can be used with the mobile devices that they carry with them, using applications resident on the mobile device. People with disabilities use existing applications such as SMS, instant messaging (IM), and email in their everyday routine communications, and believe these communications tools may be of value for contacting emergency services. However, dependence on communications methods such as SMS, that can adequately handle normal day-to-day communications but were not designed for critical life-safety communications, may have devastating implications to the user. It is important to have a thorough understanding of the limitations of these methods, and of the ultimate user experience, especially when suggested for use in emergency service applications.

3GPP is in the process of studying a long-term solution to address the need for non-voice emergency services (NOVES) for people with disabilities (and potentially the general user population in the future), but it may be several years before this long-term solution is available in the marketplace. Upgrades to support NOVES will likely be required not only in the wireless networks and mobile devices, but also in the PSAPs. This timeframe does not solve the more immediate needs of the people with disabilities.

Part of the reason that the people with disabilities desire a near-term solution is because there are third-party providers who have been touting "solutions" for SMS to 9-1-1 communications. Some of these latest "solutions" were presented to the people with disabilities community at the NENA Annual Conference in June 2010.

The issue with the SMS to 9-1-1 solutions being touted by these third-party providers is that these solutions are primarily focused on the upgrades to support interactions on the PSAP side of the communications interface and do not address the end-user devices, the originating wireless networks, and ultimately the SMS shortcomings and limitations (e.g., location, security, latency, routing) that are discussed in the other sections of this white paper. However the people with disabilities community has been led to believe that these solutions will be sufficient to provide emergency communications without regard to an end-to-end evaluation of the user experience, and thus are strongly lobbying the industry to implement one or more of these third party solutions.

A potential alternative to these near-term SMS to 9-1-1 solutions is for the people with disabilities community to be able to use TTY communications with the PSAP without requiring users to attach a separate TTY terminal to their mobile devices. This alternative is commonly called "TTY Emulation". This solution not only benefits the end user by removing the burden of carrying a TTY terminal and does not require expensive upgrades to the PSAP, as most can handle TTY communications today. It also can be used immediately, without requiring wireless operator network upgrades. The Wireless Rehabilitation Engineering Research Center (RERC) has been conducting a research project on TTY Emulation and has developed a prototype on an open-source mobile device. The significant challenge to implementation of TTY Emulation is the development of a solution that is compliant with the FCC regulations for TTY latency and bit error rates, and is available on multiple mobile device platforms.

TTY Emulation establishes a standard circuit-switched emergency voice call, and uses the media path to transmit and receive characters as TTY tones (typically Baudot tones). TTY emulation re-uses emergency voice services, including high reliability, low latency, priority handling, immediate location estimation, location-based routing to the correct PSAP, location determination, location transmission to the PSAP, and other features.

There are some challenges with TTY Emulation that make a standardized solution with involvement by device vendors and wireless operators desirable. For example, it is generally more reliable to transmit and receive signaling between the handset and base station instead of audible tones, but this is a well-established technique that is widely understood within the industry.

Although there are a number of research activities in the area, there are no known commercially available mobile devices which are "TTY Emulation" capable, nor are there any known plans of any mobile device vendor to implement a TTY Emulation service on their mobile devices. The wireless operator community encourages mobile device vendors to explore this capability on devices to support people with disabilities.

The Canadian Radio-television and Telecommunications Commission (CRTC) has conducted research on text to 9-1-1 functionality and is evaluating a trial project in Canada for people with disabilities (see section 4.4). This trial requires a registered user to establish a "voice" 9-1-1 call. When the PSAP call taker identifies the caller as one who cannot use speech and is registered for SMS, the PSAP call taker initiates an SMS text message to that caller. The SMS message is delivered over the associated control channel that exists as part of the voice call; this eliminates some of the limitations with SMS as the MSC does not have to perform the "paging" process to deliver the SMS message. In addition, since there is a voice call established, the normal routing and location capabilities of the voice call are available, eliminating some of the other limitations with SMS. However, the "store and forward" nature of SMS is still inherent into this method with the possibility of delays. In addition, this capability also requires the user to be able to read and send an SMS message while on a voice call. On many mobile devices, including popular smartphones, this can be complex. For example, the receipt of an SMS message while on a voice call may only bring up a small icon on the screen, with no other indication to the user of the received SMS message. To originate a SMS message, the user may be required to go through menus to get to the SMS screen, all without dropping the voice call. These complications may not make such a "silent voice call" solution practical.

Another solution being advocated for persons with disabilities is Real Time Text, or RTT. RTT is also known as Text over IP, or ToIP. RTT transmits the text character by character as the user types the message. RTT and IM are complementary text services with different capabilities. Real-time text conversations deliver an equivalent mode to voice conversations by providing transmission of text character by character as it is entered, so that the conversation can be followed closely and that immediate interaction takes place. Store-and-forward systems like email or SMS on wireless networks, or non-streaming systems like instant messaging, are unable to provide that functionality. RTT requires an IP data connection, as the messages are transported over IP protocols. Capabilities such as automatic routing and location are not defined, although the IETF ECRIT has defined protocols that in future next generation networks may enable these functions from generic IP endpoints with support from the mobile devices and the wireless operator network. ITU-T Recommendation F.700[41] defines RTT, and IETF RFC 5194[42] defines the Framework for Real-Time Text over IP Using the Session Initiation Protocol (SIP).

It is important to address the requirements for people with disabilities as soon as possible. It is recommended that techniques which are readily available today, such as silent 9-1-1 calls, while the next-generation systems are being designed.

7. CONCLUSIONS

As described in this white paper, there are significant limitations for the use of SMS for texting to 9-1-1. The following considerations must be taken into account:

- SMS to 9-1-1 is a best effort service with no delivery or performance guarantees, therefore FULL liability protection must be provided for wireless operators and other stakeholders. Liability protections for SMS to 9-1-1 have to be far greater than those for voice because the probability of something going wrong is so much greater and there are more areas where things can go wrong.

- There needs to be an education process for both call takers and consumers on the experience expected as the experience for both the call taker and end user for texting to 9-1-1 will be significantly different than voice or TTY to 9-1-1.

[41] See ITU-T Recommendation F.700, "Framework Recommendation for Multimedia Services", November 2000.
[42] See http://tools.ietf.org/html/rfc5194

- Routing of a "911" SMS may be provided to a NENA defined central server for handling and routing to a PSAP. The wireless network operator is not responsible for routing.

- No location information is provided by the originating network or mobile device. Location is subject to whatever is put in the message by the originator and subject to mobile device and other functional element capabilities/limitations.

- No priority or special handling is given to SMS messages.

- SMS to 9-1-1 messages should less than 160 characters in length to eliminate the need for segmentation and reassembly of long SMS messages. Long SMS messages are broken into a sequence of independent messages. Each segment can be delayed resulting in out of order delivery of the messages resulting in confusion, and devices are inconsistent in the way they reassemble long messages.

- No acknowledgments of sent, delivered or read SMS messages are provided (by the originating network).

- No security, authentication, or non-repudiation of any SMS message is provided.

- The originating network will not prevent any spam, SMS spoofing, or denial of service (DoS) attacks on messages delivered to the "911" central address.

- An originating network reserves all rights to protect its network from network spikes, DoS attempts and other congestion issues. This must be part of those liability protections.

- SMS is not a session based protocol. Therefore it is a PSAP (E9-1-1 Authority as applicable) function to “manage” routing of all messages to or from the appropriate PSAP call taker for each SMS message. If there is a series of SMS messages in the exchange between the caller and PSAP call taker, then the PSAP is responsible for association of those messages, ensuring routing to the same call taker if that is their desire, and appropriate routing to another PSAP if applicable. Originating networks do not maintain this association.

    - NOTE: If the caller is moving and crosses PSAP boundaries, messages may be sent to different PSAPs based on caller location, cell site boundaries, etc. Management of messages in this environment is not the responsibility of the originating network. It is not clear how this might work at PSAP boundaries.

There is ongoing work in the wireless industry and NENA to develop a non-SMS based solution for non-voice emergency services in the next generation wireless networks. The wireless industry fully understands the desires of the people with disabilities community and is focused on finding a reliable solution for their needs instead of a short term incomplete solution.

In conclusion, there are significant limitations inherent in the design of the current Short Message Services which make it impractical to be used for emergency service. However, it is important to address the requirements for people with disabilities as soon as possible. To that end, it is recommended that techniques which are readily available today, such as silent 9-1-1 calls, along with accelerating research and development into emerging technologies such as TTY Emulation, be undertaken while the next-generation systems are being designed.

8. ACKNOWLEDGEMENTS

The mission of 4G Americas is to promote, facilitate and advocate for the deployment and adoption of the 3GPP family of mobile broadband technologies throughout the ecosystem – including networks, services, applications and wirelessly connected devices – in the Americas.

4G Americas' Board of Governors members include: Alcatel-Lucent, America Móvil, Andrew Solutions, AT&T, Cable & Wireless, Ericsson, Gemalto, HP, Huawei, Motorola, Nokia Siemens Networks, Openwave, Powerwave, Qualcomm, Research In Motion (RIM), Rogers Wireless , T-Mobile USA and Telefónica.

4G Americas would like to recognize the significant project leadership and important contributions of DeWayne Sennett and Brian K. Daly of AT&T as well as the other member companies from 4G Americas' Board of Governors who participated and contributed to the development of this white paper.

APPENDIX A. ACRONYMS AND DEFINITIONS

A.1 ACRONYMS

3GPP	3rd Generation Partnership Project
A-GPS	Assisted GPS
APEX	Application Exchange
ASCII	American Standard Code for Information Interchange
ASP	Application Service Provider
ATIS	Alliance for Telecommunications Industry Solutions
CCH	Control Channel
CISC	Canadian Radio-television Telecommunications Interconnection Steering Committee
CMAS	Commercial Mobile Alert System
CRTC	Canadian Radio-television and Telecommunications Commission
CS	Circuit Switched
CSCA	Common Short Code Administration
CSMS	Concatenated SMS
CTIA	Cellular Telecommunications Industry Association
DoS	Denial of Service
E9-1-1	Enhanced 9-1-1
EAS	Emergency Alert System
ECRIT	Emergency Context Resolution with Internet Technologies
EMI	External Machine Interface
EMS	Emergency Medical Service
ESWG	Emergency Services Working Group
ETSI	European Telecommunication Standards Institute
FCC	Federal Communications Commission
G-MSC	Gateway Mobile Switching Center
G-SMSC	Gateway SMSC
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile communications
HLR	Home Location Register
IMDN	Instant Message Disposition Notification
IETF	Internet Engineering Task Force

IM	Instant Messaging
IMPS	Instant Messaging and Presence Service
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IP-CAN	IP Connectivity Access Network
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication standardization sector
IWMSC	Interworking Mobile Switching Center
MiM	Man in the Middle
MIM	Mobile Instant Messaging
MMS	Multimedia Messaging Service
MMSC	Multimedia Messaging Service Center
MO-SM	Mobile Originated Short Message
MSC	Mobile Switching Center
MT-SM	Mobile Terminated Short Message
NCS	National Communications System
NENA	National Emergency Number Association
NG9-1-1	Next Generation 9-1-1
OMA	Open Mobile Alliance
OSI	Open Systems Interconnection
OTA	Over-the-Air
PLMN	Public Land Mobile Network
PRIM	Presence and Instant Messaging Protocol
PSAP	Public Safety Answering Point
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RAN	Radio Access Network
RERC	Rehabilitation Engineering Research Center
RF	Radio Frequency
RFC	Request for Comments
RTT	Real Time Text
SGSN	Serving GPRS Support Node
SIM	Subscriber Identity Module
SIMPLE	SIP for Instant Messaging and Presence Leveraging Extensions
SIP	Session Initiation Protocol

SM	Short Message
SME	Short Message Entity
SMPP	Short Message Peer-to-Peer
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SMSC	Short Message Service Center
T9-1-1	Text messaging to 9-1-1
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
ToIP	Text over IP
TTY	Teletype
UDH	User Data Header
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
URL	Uniform Resource Locator
VASP	Value-Added Service Providers
VLR	Visitor Location Register
VMSC	Visited Mobile Switching Center
WAP	Wireless Application Protocol
XML	Extensible Markup Language
XMPP	Extensible Messaging and Presence Protocol

A.2 DEFINITIONS

PSAP A PSAP is a set of call takers authorized by a governing body and operating under common management which receives 9-1-1 calls and asynchronous event notifications for a defined geographic area and processes those calls and events according to a specified operational policy.

SMS The Short Message Service (SMS) provides a means of sending messages of limited size to and from mobiles. The provision of SMS makes use of a Service Center, which acts as a store and forward center for short messages.