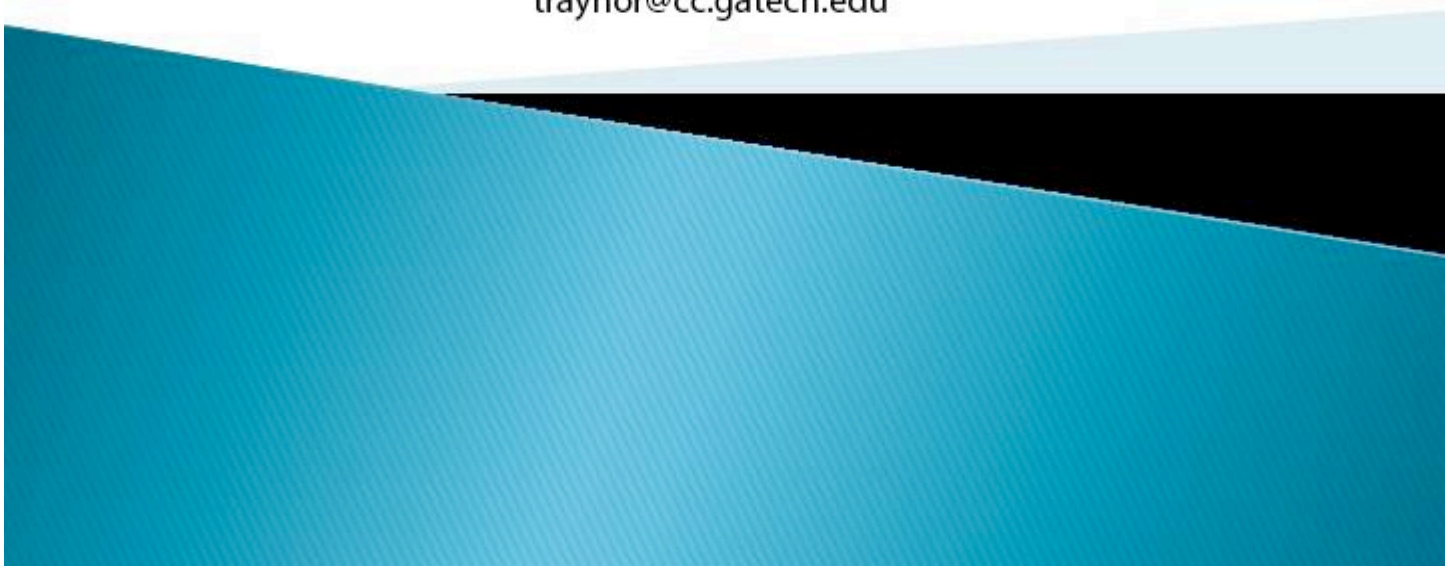
Characterizing the Limitations of Third-Party EAS Over Cellular Text Messaging Services

September 2008

Principal Investigator:
Patrick Traynor, Ph.D.
Assistant Professor
Georgia Institute of Technology

266 Ferst Drive, Room 3138
Atlanta, GA 30332
traynor@cc.gatech.edu



Contents
Table of Contents

1 Introduction

Text messaging allows individuals to transmit short, alphanumeric notes for a wide variety of applications. Whether to coordinate meetings, catch up on gossip, offer reminders of an event or even vote for a favorite contestant on a television game show, this discreet form of communication is now the dominant service offered by cellular networks. In fact, in the United States alone, over five billion text messages are delivered each month [24]. As the mobile phone continues to become more ubiquitous, so too does the use of text messaging.
As the examples above demonstrate, the majority of legitimate uses for SMS can often be characterized as recreational, ranging from social interactions to low priority business-related exchanges. During emergency events, however, the nature of text messaging has proven to be far more utilitarian.

With millions of people attempting to contact friends and family on September 11th, 2001, telecommunications companies witnessed tremendous spikes in cellular voice service usage. Verizon Wireless, for example, reported voice traffic rate increases of up to 100% above typical levels; Cingular Wireless recorded an increase of up to 1000% on calls destined for the Washington D.C. area [27]. While these networks are engineered to handle elevated amounts of traffic, the sheer number of calls was far greater than capacity for voice communications in the affected areas. However, with voice-based phone services being almost entirely unavailable, SMS messages were still successfully received in even the most congested regions because the control channels responsible for their delivery remained available. Similar are the stories from the Gulf Coast during Hurricanes Katrina and Rita. With a large number of cellular towers damaged or disabled by the storms, text messaging allowed the lines of communication to remain open for many individuals in need in spite of their inability to complete voice calls in areas where the equipment was not damaged and power was available.

Accordingly, SMS messaging is now viewed by many as a reliable method of communication when all other means appear unavailable. In response to this perception, a number of companies offer SMS-based emergency messaging services. Touted as being able to deliver critical information during disaster events, such services have been purchased by colleges, universities and even municipalities hoping to protect the general public. Unfortunately, such systems will not work as advertised.

In this paper, we demonstrate the limitations of third party *Emergency Alert Systems* (EAS). In particular, because of the architecture of cellular networks, such systems will not be able to deliver a high volume of emergency messages in a short period of time. Through discussion, modeling and simulation, we show that current systems not only can not widely disseminate such messages quickly, but also that the addition traffic created by third party EAS may disrupt other traffic such as voice communications, including that of emergency responders or the public to 9-1-1 services.

The paper is organized as follows: Section 2 offers a historical overview of text messaging and emergency alert systems; Section 3 provides a technical overview of SMS delivery in GSM cellular networks and a general third-party EAS provider architecture. Section 4 presents point by point arguments demonstrating the mismatch between current text messaging systems and EAS; Section 5 provides modeling and experimental results; Section 6 discusses how cellular providers intend to address the problem; Section 7 discusses a number of related studies; Section 8 provides concluding thoughts.

2 Historical Context

2.1 GSM Short Messaging

The idea of a text-based communication mechanism as part of a cellular network was discussed as early as the 1980's. However, conversations on how such a service might be used varied significantly. Many within the provider community viewed SMS as a means of notifying customers of personal alerts, including voice mail, or system events, such as network outages. Others wished to create a service capable of competing with one-way numeric pagers ("beepers"). Still another group hoped that such a mechanism could provide service to a range of remote data collection devices (e.g., telemetry). In an effort to allow all of the above applications to be realized, the original SMS standard (1985) [19] described three general functions: Short Message Mobile Terminated (from the network to a device), Short Message Mobile Originated (from a device to the network) and Short Message Cell Broadcast (from the network to all devices in an area).

Such services were made possible through the use of under-utilized "signaling" or control channels.[1] Used primarily to set up voice calls, these channels lay largely unused during normal network operations. Because text-based messaging was never expected to exceed telephony in popularity, designers believed that such services could be added to these channels without noticeably impacting the network. Accordingly, without making any significant changes to the already deployed infrastructure, designers were able to provide a vast array of new services.

Adoption of text messaging was slow. In fact, it was not until 1992 that the first commercial message was transmitted [20]. Customer use remained flat until the end of the decade; however, the introduction of inter-provider messaging agreements, pre-paid user plans and unlimited messaging options significantly boosted the popularity of the service. At the end of the year 2000, approximately 5 billion messages were being sent per month. By 2005, that number increased by nearly two orders of magnitude, with an estimated 1 trillion messages sent worldwide [20], far beyond the original designers' expectations.

Outside of standardization to allow messages to be exchanged by cellular providers across the world, many of the early details of SMS remain. A text-only service, SMS delivers messages containing up to 160 characters. By default, messages are encoded in an alphabet supporting an extended Latin character set known as the "GSM 7-bit default alphabet" [1]. Non-Latin character sets including Arabic, Chinese and Cyrillic can also now be supported by an alternate 16-bit encoding; requiring 16-bits to encode these characters reduces the number of characters by half.

2.2 The Evolution of EAS

An efficient national system for alerting the general populace of emergency events has long been the dream of legislators and public safety officials. However, it was not until the middle of the past century that the technology to enable such a system was widely available. Fears of nuclear attack during the Cold War precipitated the creation of the first such system, known as *Control of Electromagnetic Radiation* (CONELRAD) in 1951. In the event of a national emergency, radios could be tuned to one of two AM frequencies to ensure the delivery of civil defense information. As the threat of attack decreased, the desire to expand such a system for use in local emergency coordination allowed for the better known *Emergency Broadcast System* (EBS) to replace CONELRAD in 1963. Through a combination of analog radio and television broadcasts, warnings for events including severe weather could reach large portions of the population in a short period of time.

Citing the need to improve automation and to expand the range of devices capable of receiving emergency messages, the *Emergency Alert System* (EAS) replaced the EBS in 1996 [29]. Cooperatively managed by the Federal Emergency Management Agency (FEMA)[2], the Federal Communications Commission (FCC) and the National Weather Service (NWS), the EAS uses a unified message type[3] to deliver emergency information in a format readable by all EAS-participating stations with the goal of distributing emergency information to the entire general public in under 10 minutes. As a result of these changes, providers offering services to analog, digital and satellite radios, and cable and satellite televisions can now transmit emergency alerts to their clients.

The area covered by the majority of these services can be extremely large. Accordingly, providing emergency information specific to a particular area (e.g., county, city or neighborhood) is frequently difficult or impossible. Having observed this, the FCC released a *Notice of Proposed Rulemaking* (NPRM) asking whether such problems were the result of a failure to use the most modern means of communications (e.g., email, cellular networks) during times of crisis [14]. As a means of addressing this shortcoming, the FCC also asked for participation from legislators and telecommunications providers in the development of a more capable system.

Congress responded with a number of bills concerning the use of cellular phones for timely notification during a disaster. The House of Representatives passed H.R. 2101, *An Act to Amend the Homeland Security Act of 2002 to direct the Secretary of Homeland Security to develop and implement the READICall emergency alert system* [35], which in 2005 tasked the Secretary of Homeland Security to research, develop and implement a phone-based emergency alert system. In the Senate, the *Warning, Alert, and Response Network* (WARN) *Act* [36], which was eventually passed as part of the *Safe Accountability for Every Port Act of 2006* (SAFE Act), sought to provide similar support for the use of cellular networks.

The WARN Act makes compliance by members of the wireless telecommunications industry voluntary. Nevertheless, most major providers are currently working to assist in the development of technical standards and protocols capable of realizing such infrastructure. To meet this goal the FCC established the *Commercial Mobile Service Alert Advisory Committee* (CMSAAC), a group of service providers, equipment vendors, government representatives and emergency officials, with the expressed goal of providing recommendations to achieve the above goal in both a cost and performance efficient manner [8]. Chief among CMSAAC's extensive conclusions were that currently deployed systems, in particular SMS, were simply not capable of delivering emergency notifications in a timely fashion (i.e., 10 minutes), especially on a large scale. Moreover, CMSAAC concluded that the development of new protocols and systems capable of achieving these goals would be required.

3 Technical Overview

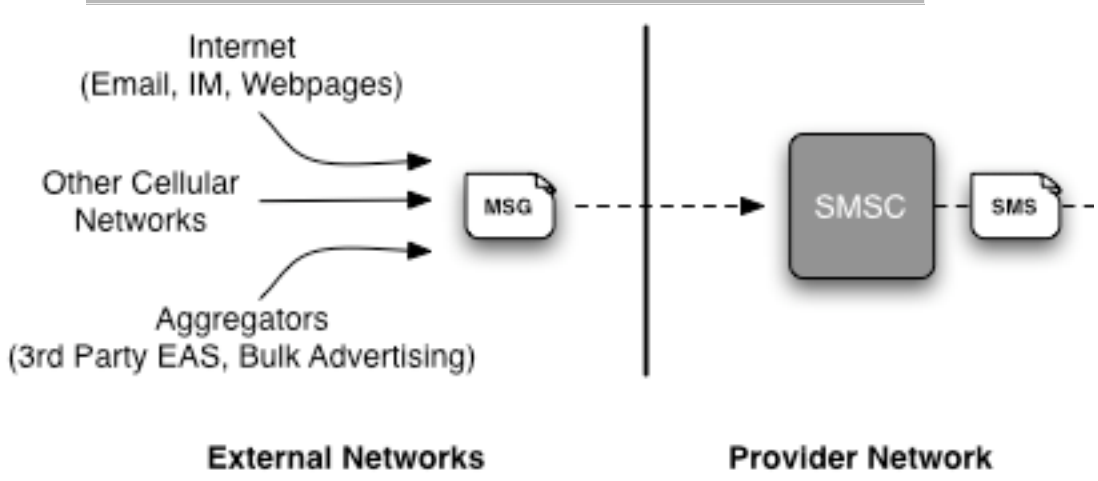


Figure 1: Text messages arrive in a provider's network from a wide variety of sources and are processed by the SMSC before being delivered to mobile devices.

In order to appreciate why the CMSAAC argued against the use of SMS for the distribution of emergency alerts, it is necessary to understand how cellular networks deliver text messages. In this section, we provide a technical overview of message delivery and a high-level description of how third-party vendors try to use these systems to deliver alert messages. We specifically examine GSM networks in these discussions as they represent the most widely deployed cellular technology in the world; however, it should be noted that message delivery for other technologies such as CDMA, IDEN and TDMA are very similar and are therefore subject to similar problems.

3.1 Cellular Network Architecture

3.1.1 Sending a Message

There are a number of ways in which text messages can be injected into a GSM or CDMA network. While most users are only familiar with sending a text message from their phone, known as *Mobile Originated SMS* (MO-SMS), service providers offer an expanding set of interfaces through which messages can be sent. From the Internet, for instance, it is possible to send text messages to mobile devices through a number of webpages, email and even instant messaging software. Third parties can also access the network using so-called SMS Aggregators. These servers, which can be connected directly to the phone network or communicate via the Internet, are typically used to send “bulk” or large quantities of text messages. Aggregators typically inject messages on behalf of other companies and charge their clients for the service. Finally, most providers have established relationships between each other to allow for messages sent from one network to be delivered in the other. Figure 1 shows these three high-level strategies.

After entering a provider’s network, messages are sent to the *Short Messaging Service Center* (SMSC). SMSCs perform operations similar to email handling servers in the Internet, and store and forward messages to their appropriate destinations. Because messages can be injected into the network from so many external sources, SMSCs typically perform aggressive spam filtering on all incoming messages. All messages passing this filtering are then converted and copied into the necessary SMS message format and encoding and then placed into a queue to be forwarded to their final destination.

3.1.2 Finding a Device

Delivering messages in a cellular network is a much greater challenge than in the traditional Internet. Chief in this difficulty is that users in a cellular network tend to be mobile, so it is not possible to assume that users will be located where we last found them. Moreover, the information about a user's specific location is typically limited. For instance, if a mobile device is not currently exchanging messages with a base station, the network may only know a client's location at a very coarse level (i.e., the mobile device may be known to be in a specific city, but no finer-grained location information would be known). Accordingly, the SMSC needs to first find the general location for a message's intended client before anything else can be done.

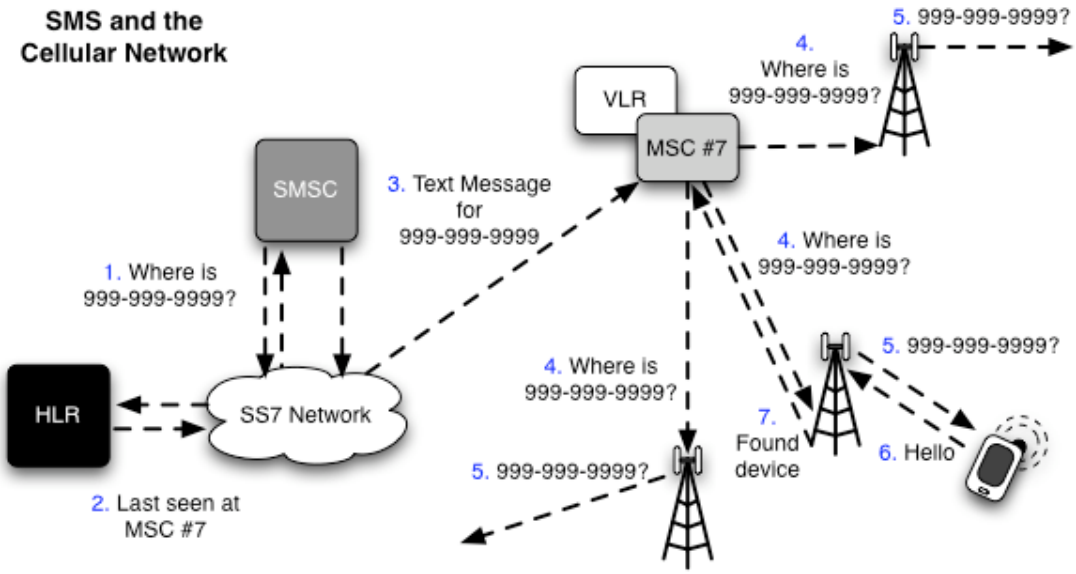


Figure 2: Before a message can be delivered, a mobile device must be located. Though the process illustrated here, the network determines the sector, one of three service areas on each base station tower, with which the target mobile device is operating.

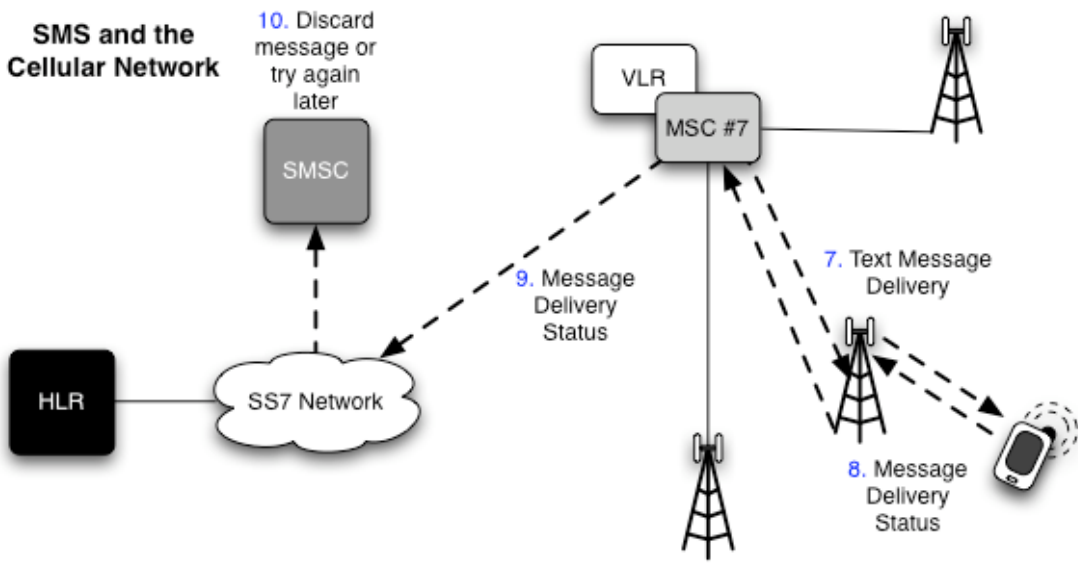


Figure 3: Once a phone is located, the network can deliver a text message. After the network attempts to deliver the text message, it tells the SMSC whether or not it was successful. On delivery, the text message is deleted from the SMSC. Otherwise, the message remains on the SMSC until a later attempt.

A server known as the *Home Location Register* (HLR) assists in this task. This database acts as the permanent repository for a user's account information (i.e., subscribed services, call forwarding information, etc). When a request to locate a user is received, the HLR determines whether or not that device is currently turned on. If a mobile device is currently powered off, the HLR instructs the SMSC to store the text message and attempt to deliver it at another time. Otherwise, the HLR tells the SMSC the address of the *Mobile Switching Center* (MSC) currently serving the desired device. Having received this location information, the SMSC then forwards the text message on to the appropriate MSC.

3.1.3 Wireless Delivery

As mentioned earlier, even the MSC may not know more information about a targeted device's location. In order to determine whether or not the current base station serving this device is known, the MSC queries the *Visitor Location Register*, which temporarily stores information about clients while they are being served by the MSC. In most cases, this information is not known, and so the MSC must begin the extensive and expensive process of locating the mobile device. The MSC completes this task by generating and forwarding paging requests to all of its associated base stations, which may number in the hundreds. This process is identical to locating a mobile device for delivery of a voice call.

Upon receiving a paging request from the MSC, a base station attempts to determine whether or not the targeted device is nearby. To achieve this, the base station attempts to use a series of *Control Channels* to establish a connection with the user. First, the base station broadcasts the paging request over the *Paging Channel* (PCH) and then waits for a response. If the device is nearby and hears this request, it responds to the base station via the *Random Access Channel* (RACH) to alert the network of its readiness to receive information. When this response is received, the network uses the *Access Grant Channel* (AGCH) to tell the device to listen to a specific *Standalone Dedicated Control Channel* (SDCCH) for further exchanges. Using this SDCCH, the network is able to authenticate the client, perform a number of maintenance routines and deliver the text message. By limiting the operations necessary to deliver a text message to the control channels used for call setup, such messages can be delivered when all call circuits, known as *Traffic Channels* are busy.

When the attempt to deliver the message between the targeted device and the base station is complete, the device either confirms the success or failure of delivery. This status information is carried back through the network to the SMSC. If the message was successfully delivered, the SMSC deletes the message. Otherwise, it stores the message until a later period, at which time the network re-attempts delivery. Figures 2 and 3 offer a high level overview of this entire process.

3.2 Third-Party Provider Solutions

In the past few years, a significant number of third-parties offering to deliver alert messages (and other information services) via text messaging have appeared. Citing the need for improved delivery targeted to a highly mobile population, many such services advertise text messaging as an instant, targeted disseminator capable of delivering of critical information to tens of thousands of mobile phones when it is most needed. These systems have been extensively deployed on college and university campuses throughout the United States.

The architecture of these systems is relatively simple. Whether activated through a web interface [7, 11, 32, 41, 42], directly from a phone [22], or as software running on a campus administrator's computer [31, 28], these services act as SMS aggregators and inject large numbers of text messages into the network. Colleges and universities subscribing to these services then collect mobile phone numbers from students, faculty and staff. In the event of an alert, all or a subset of the collected numbers can be targeted. While network providers may offer some limited information back to the third party, aggregators are largely unaware of conditions in the network or the geographic location of any specific individual.

4 Understanding the Mismatch

Having explored the technical details of alert message insertion and delivery in cellular networks, we now discuss why EAS over SMS in current systems is simply not feasible or recommended.

- **Cellular networks are not designed to delivery emergency-scale traffic loads:** Planning and deploying cellular networks is an expensive undertaking. From specially designed equipment to competition over scarce wireless spectrum, such systems must be carefully deployed so as to meet expected customer demand in an economically feasible manner. Like any other system, it is simply not possible for cellular networks to provide virtually unlimited capacities.

  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. Through the following equations, network planners can accurately approximate the impact of such tradeoffs:

$$P[blocking] = \frac{\frac{A^n}{n!}}{\sum_{l=0}^{l=n-1} \frac{Al}{l!}}$$

  where *n* is the maximum number of concurrent calls and *A* is the offered load in "Erlangs". For instance, assuming that 200 users in an area supporting up to 16 concurrent phone calls each make approximately one call per hour, each of which lasts an average of two minutes, a user making a phone call would get a busy signal on approximately 0.1% of their attempts. In a conservative emergency scenario, where each of the 200 users sends or receives six calls per hour (one every 10 minutes) and all of the previous conditions hold, the probability that a call will be met with a busy signal jumps to 44.2% percent.

  Expanding a network deployment to accommodate an unlikely burst is costly for a number of reasons. First, the number of simultaneous calls that can be supported is tied to the available spectrum. As the most recent spectrum auction demonstrated, the purchase of additional wireless capacity is often prohibitively expensive.[4] Moreover, because such infrastructure is not needed for normal operations, large parts of the network would remain underutilized. For instance, by adding enough spectrum to the above example to drop blocking to normal levels during an emergency (approximately 2.5 times the current configuration, the network would

experience a utilization rate of 18.5%, down from 41.7%, making a positive return on the provider's investment difficult. Requiring cellular providers to maintain such resources would be similar to requiring all grocery stores to constantly stock their shelves with quantities of inventory far beyond what they can reasonably expect to sell - in both cases, significant resources would go to waste under normal circumstances.

With billions of text messages transmitted around the world every month [24], it would still appear as if cellular networks could support nearly unlimited delivery. However, the reason that such volumes are possible is due to the distribution of messages. In particular, because the volume of messages to a specific area are generally regular and small compared to the world-wide total, such loads can be handled. Moreover, delay or lack of reliability for routine messages is typically not a major concern to subscribers. As the simple calculations above demonstrate, a violation of such normal conditions quickly results in delay, congestion and message loss. Traynor et al [38, 39] observed this phenomenon from the perspective of an attacker. This work demonstrated the ability to deny legitimate voice *and* text messaging services to Manhattan using the bandwidth available to a single cable modem. Regardless of whether the source is malicious or benign, sending large quantities of text messages to one geographic region is simply not supportable by current cellular infrastructure.

- **Cellular networks are not the Internet:** The Internet is built around the guiding philosophy of the "End to End" Principal. In very simple terms, this principal argues that functionality not required by all kinds of traffic should not be implemented in the core of the network. For instance, because not every application requires all packets to be delivered in order to correctly operate (e.g., streaming audio and video), reliable delivery is implemented in the end points of the network and not in core routers. Because the core of the network does not provide or manage any flow-specific services, the cost of forwarding packets in the Internet is solely dependent on the size of the packet.

  The same can not be said for cellular networks. As Traynor demonstrated in his dissertation [37], cellular networks expend significant effort when establishing a connection. As demonstrated in Section 3, these operations include locating a targeted mobile device and performing significant negotiations before a single packet can be delivered. While the delivery rates of cellular data services have been steadily improving over the past decade, this setup and delivery of the first bit of information remains a significant bottleneck in the process. This means that while it is possible to download large files relatively quickly using such networks, beginning the download remains expensive.

Part of the difficulty in delivering emergency alerts to a large population via SMS is also due to the nature of communication in these systems. The vast majority of uses for text messaging today can be classified as “point to point”, or the transmission of a message from the network to a single user. While the original designers considered the need for broadcast, or “point to multi-point”, communications, such functionality was never fully developed in the standards process or implemented in provider networks. The difference between these means of communication is significant and can best be explained in another light - imagine an emergency occurring on a college campus and a professor being required to alert all students in an auditorium of the issue. Using the broadcast model, the professor could speak loudly once to all students and simultaneously alert them of the situation. Under the “point to point” model, the professor would have to walk around the auditorium and quietly tell each student of the issue. Clearly, as the number of students in the auditorium becomes large, the ability to alert them all in a timely manner using the “point to point” approach is extremely limited.

- **Targeting users in a specific location is extremely difficult:** One of the criticisms of more traditional EAS infrastructure is the lack of location-specific information. Television and radio broadcasts often cover many hundreds of square miles and therefore can only provide observations on a similarly large scale. Because text messages can be delivered to users regardless of their location, many argue that such infrastructure can easily be used to target and inform users within a particular area. Such clams have been frequently repeated in the press:

  “It’s a no-brainer: Wireless text should be the basis for an emergency information system... Look how this could’ve worked as Hurricane Rita bore down on Houston. Millions were told via TV and radio to get out of town. So they did and wound up creating the world’s most gargantuan traffic jam, made worse as cars ran out of gas. Sure, those cars had radios that could receive news reports or announcements. But radio is a mass medium that delivers broad information. Most of those people also had cellphones that could’ve delivered timely, targeted text updates.” - Kevin Maney (USA Today), 2005 [25].

  There are a number of difficulties with these assertions. First, as mentioned in Section 3, cellular networks are not aware of a user’s specific location except for when that user is actively communicating with the network. Accordingly, the network is often unaware of exactly which users are near particular base stations. While network operators would certainly have observed significantly increased call traffic from the base stations surrounding the highways in question, there is no way for them to instantaneously know which users are present. This, in combination with the point to point nature of SMS, would have made informing all those

individuals in a timely fashion impossible. Secondly, providing up-to-date traffic information via SMS for those already stuck on the highway would arguably have been of little real use. Highways, like cellular networks, are designed around the expected capacity generated by everyday use and not for emergencies. Instead, users that would be most likely to attempt to use the already congested highways would have best been served by such alerts. Predicting which users this would include, however, is simply not knowable.

A number of services offer improved location accuracy by installing special software on user phones [34]. By regularly transmitting GPS or network assisted geographic coordinates to the third party provider, messages can be better targeted to individuals in affected areas. However, this approach also fails because of many of the previously discussed reasons. First, while this approach does narrow down the size of the area to which such messages are sent, the amount of traffic sent to this area will still far exceed network capacity. Additionally, the transmission of location information itself adds significant traffic to the network. People attempting to communicate in this area will likely experience significant delays, potentially critically slowing down the response of emergency officials. Secondly, because devices are required to send regular location updates to the third party, an increased drain on device batteries will also be experienced, again leaving users unable to communicate. Such a constant demand for location information is the opposite of how current 9-1-1 services operate. Thus, given the characteristics of the current infrastructure, such an approach will not assist in the efficient delivery of emergency messages.

Even in more predictable settings such as college and university campuses, specifically targeting such alerts would be extremely difficult. The majority of third party providers of EAS over SMS implement their services by collecting a list of student, faculty and staff phone numbers for a particular institution. In the event of an emergency, messages targeting these users can be injected into cellular networks. However, knowing the number associated with a specific user is not a guarantee of their location. Students traveling across the country will receive the same alerts as those on campus. Moreover, such alerts will fail to reach visitors and neighboring citizens, even though the information contained within these messages may be pertinent to everyone in the area. Such services therefore fail to achieve the fundamental property required of EAS infrastructure - that all individuals with a device capable of receiving alerts can do so.

- **There is no way to authenticate the source of messages, making fraudulent alerts easy to send:** Being able to disseminate alert messages in a timely manner is not the only essential component when evaluating EAS requirements. Users must be able to trust the authenticity of every emergency message they receive. Failure to ensure that the source of a

message can be correctly identified allows malicious parties opportunities to add confusion to an emergency event.
Text messaging does not provide any means of authentication. Accordingly, it is possible for any individual with an Internet connection to inject messages with arbitrary contents to anyone with a cellular phone. As Figure 4 demonstrates, such messages are indistinguishable from legitimate messages.

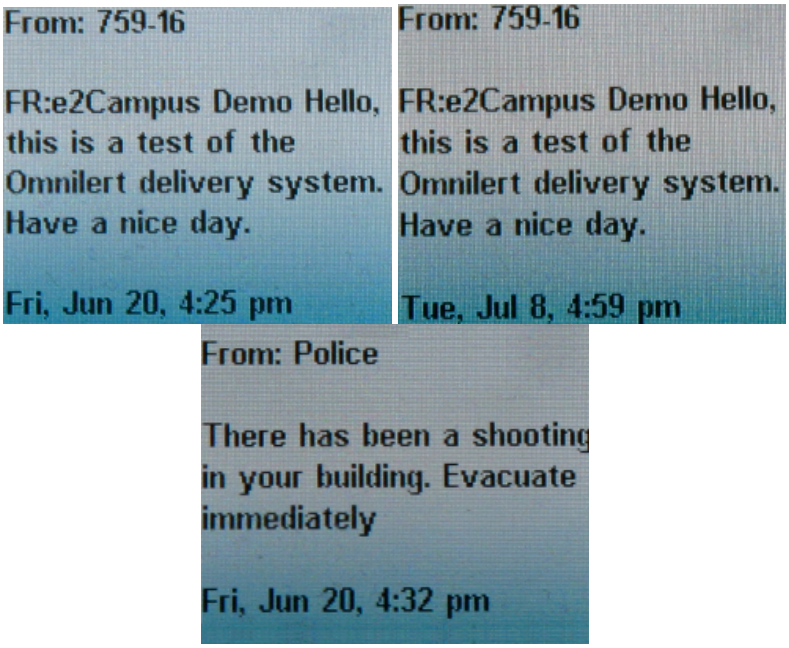


Figure 4: The picture on the top left was a test message sent using the e2campus website. The top right picture contains the exact same message and claims to be from the same source, but was sent from a service provider's web interface. The bottom picture is a forged emergency message warning the user of an on-campus shooting and claims to be sent by the Police.

The implications of this limitation are significant. 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 such false alerts have already been observed, including false warnings about earthquakes [23], tsunamis [3], school shootings [16], false Amber Alerts [30] and other dangers [5].

- **SMS is not a real-time service:** Phone calls are an example of a real-time service. From the moment a call is placed, users expect to be able to hold a conversation without large periods of delay between responses. This immediacy of communications is in stark contrasts to asynchronous services such as email, where users have learned to expect at least minor delays between messages.

  Examples of the delay that can be experienced during times of high volume are most easily observed during New Years Eve celebrations. As hundreds of millions of users around the globe send celebratory greetings via SMS, service providers often become inundated with a flood of messages. Accordingly, the delivery of such messages has been noted to exceed more than six hours [12]. Even though providers often plan and temporarily deploy additional resources to minimize the number of blocked calls, the sheer volume of messages during such an event demonstrates the practical limitations of current systems.

  Why then has SMS been a successful means of communication during other national emergencies such as September 11th and Hurricanes Katrina and Rita? Numerous sources cite SMS as an invaluable service when both man-made and natural disasters strike [18, 26]. The difference between these events and other emergencies is the magnitude of messages sent. For instance, at the time of the attacks of September 11th, text messaging was still largely a fringe service in the United States. Had most users attempted to communicate via SMS, however, a report by the National Communications System estimates that current network capacities would need to be expanded by 100-fold [27] in order to support such a volume. The reliability of text messaging during Hurricane Katrina is due to similar reasons. Because only a very small number of people were communicating via text messaging, the towers undamaged by the storm were able to deliver such messages without any significant competition from other traffic. If SMS use during either of these events approached emergency levels, it would have experienced delays similar to those regularly observed on New Year's Eve.

- **Message delivery order is not always predictable:** Implicit in the misunderstanding of text messaging as a real-time service are misconceptions about the order in which messages will be delivered to targeted devices. Specifically, it is often assumed that messages will be delivered in the order in which they were injected by the sender.

  The order in which messages are delivered can be affected by a number of factors. For instance, Traynor et al [38] showed that the SMSCs of different providers implement a variety of service algorithms, including *First-In, First-Out* (FIFO) and *Last-In, First Out* (LIFO). Accordingly, it is possible for two providers to deliver the same stream of messages in opposite order. Even if

all carriers implemented the same delivery algorithm, congestion in the network can cause further disordering of packets. If an incoming text message is unable to be delivered due to a lack of resources on the air interface, the SMSC will store the message for a later attempt. However, if subsequent messages have been sent before this message fails and manage to gain the required resources, they will be delivered out of the sender's intended order. In an emergency such as a tornado, which may frequently change directions, such out of order delivery may actually send subscribers directly into the storm as opposed to away from it.

There are a number of emergency scenarios in which the above has occurred. During a wildfire evacuation at Pepperdine University in 2007, multi-part messages were transmitted to students and faculty to provide relocation instructions. However, some reported that the messages were not useful. One student later noted that "Each notification that was sent came through in six to eight text messages... And they were jumbled, not even coming in order" [4]. More serious conflicts in message delivery order were noted on the campus of the Georgia Institute of Technology [6]. After a chemical spill in 2007, a message alerting students and faculty to evacuate campus was transmitted. Later, instructions to ignore the evacuation notification were also sent. However, a number of students noted receiving the messages out of order [33], adding greater confusion to the situation. Similar problems have been reported at a number of other universities [9, 17].

5 Modeling Emergency Events in Real Environments

To truly understand the mismatch between the current cellular text messaging infrastructure and third party EAS, it is necessary to observe such systems during an emergency. Because such events are rare, we conduct a number of experiments to simulate such events. In so doing, we demonstrate that current systems simply cannot support the volume of text messaging traffic generated by third party EAS during an emergency.

5.1 Location Selection and Characterization

The events that unfolded at the Virginia Polytechnic Institute and State University ("Virginia Tech") on April 16, 2007 have become one of the primary motivations behind the calls to use SMS as the basis of an emergency system. Many argue that had such a system been in place during what became the deadliest campus shooting in US history, countless lives could have been saved. However, a thorough examination of such claims has not been conducted. In particular, it is not clear whether or not the messages transmitted by such a system

would have reached all students before the Norris Hall shootings. Accordingly, we have selected Virginia Tech as our location to characterize.

Located in the rolling hills of southwestern Virginia, this land grant university is home to over 31,000 students, faculty and staff [43]. For the purposes of this work, we assume that just under half (15,000) of these individuals subscribe to a GSM network. As is shown by the red triangles in Figure 5, the major GSM provider in this area provides service to the campus of Virginia Tech from four base stations. Given that each base station has three sectors (each covering a 60 degree range), we assume that the campus itself is covered by 8 of the 12 total sectors in the area.

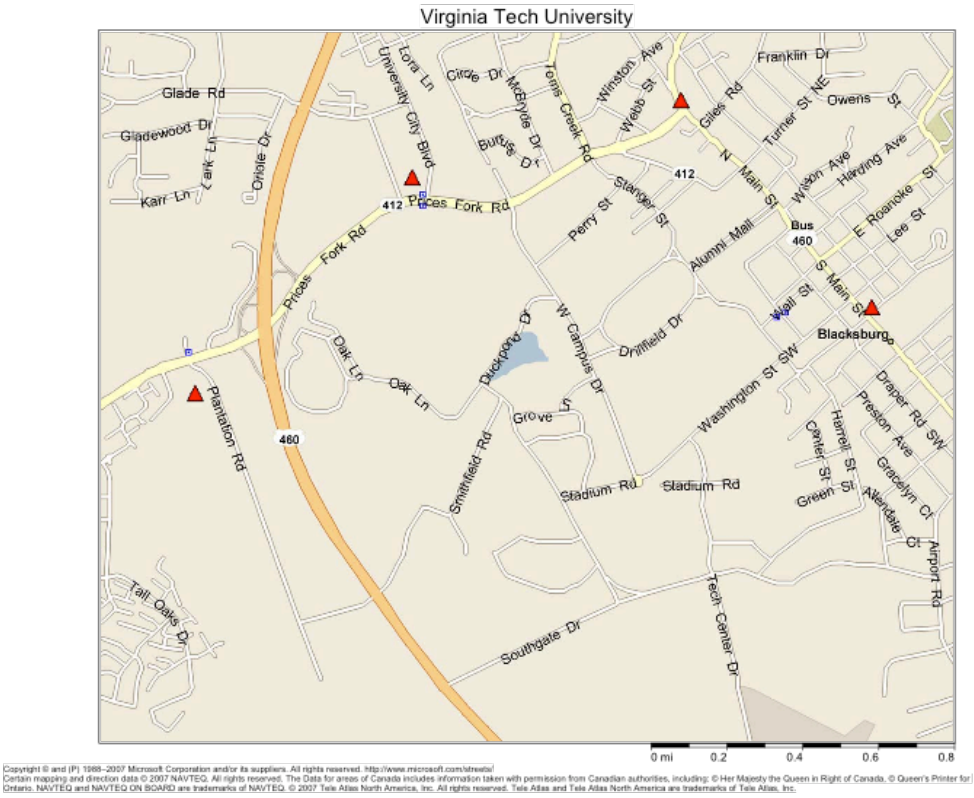


Figure 5: The placement of base stations (red triangles) for a major GSM provider near Virginia Tech. Given that each base station has three sectors, the campus itself receives service from approximately eight total sectors.

5.2 Mathematical Characterization of Emergencies

The first step in characterizing a cellular network during an emergency is determining capacity. In particular, we are interested in understanding the minimum time required to deliver emergency messages. If this time is less than the goal of 10 minutes set forth in by the current public EAS, then such a system may indeed be possible. However, if this goal cannot be met, current networks cannot be considered as good candidates for EAS message delivery.

Given that most sectors have a total of 8 SDCCHs and that it takes approximately four seconds to deliver a text message in a GSM network [38, 10, 27] and the information above, the capacity of the GSM network serving the campus of Virginia Tech is:

$$\begin{aligned} C &= 15,000 \text{ messages} \times \frac{1 \text{ campus}}{8 \text{ sectors}} \times \frac{1 \text{ sector}}{8 \text{ SDCCHs}} \times \frac{4 \text{ seconds}}{1 \text{ message}} \\ &\approx 938 \text{ seconds} \\ &\approx 15.6 \text{ minutes} \end{aligned}$$

Because the contents of emergency messages are likely to exceed the 160 character limit of a single text message, the number of messages is likely to increase by at least four times:

$$\begin{aligned} C &= 15,000 \text{ messages} \times \frac{4 \text{messages}}{\text{user}} \times \frac{1 \text{ campus}}{8 \text{ sectors}} \times \frac{1 \text{ sector}}{8 \text{ SDCCHs}} \times \frac{4 \text{ seconds}}{1 \text{ message}} \\ &\approx 3752 \text{ seconds} \\ &\approx 62.5 \text{ minutes} \end{aligned}$$

The above calculations represent a conservative minimum time for the delivery of all messages. For instance, because the SDCCHs are also used to establish voice calls and assist with device mobility, it is highly unlikely that all 8 SDCCHs will be available for delivering text messages. Accordingly, the time required to deliver all such messages will simply not be close to the goal of 10 minutes, and certainly not instantaneous as some claim.

5.3 Simulation Results

To better understand the impact of a flood of emergency text messages on normal traffic, we further characterize an emergency scenario using a GSM simulator. This tool [38, 39, 40] focuses on the wireless portion of the network and allows researchers to view the interaction of between a variety of resources. Accordingly, we can explore the details of an emergency without having to wait for such an event. In the following subsections, we offer views of normal operations, a surge of text messages and a full emergency situation.

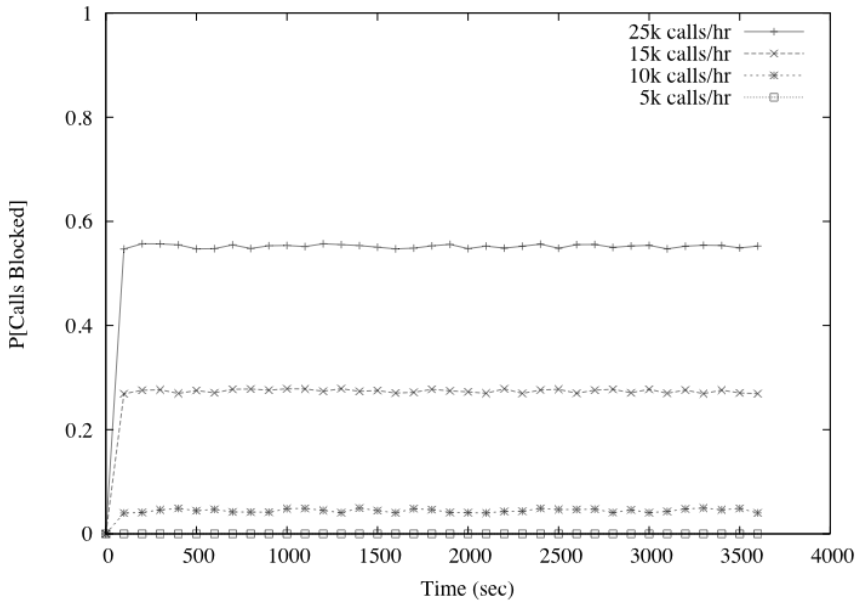


Figure 6: The probability that normal traffic patterns, at a variety of intensities, will experience blocking. Note that only under very busy conditions is blocking likely.

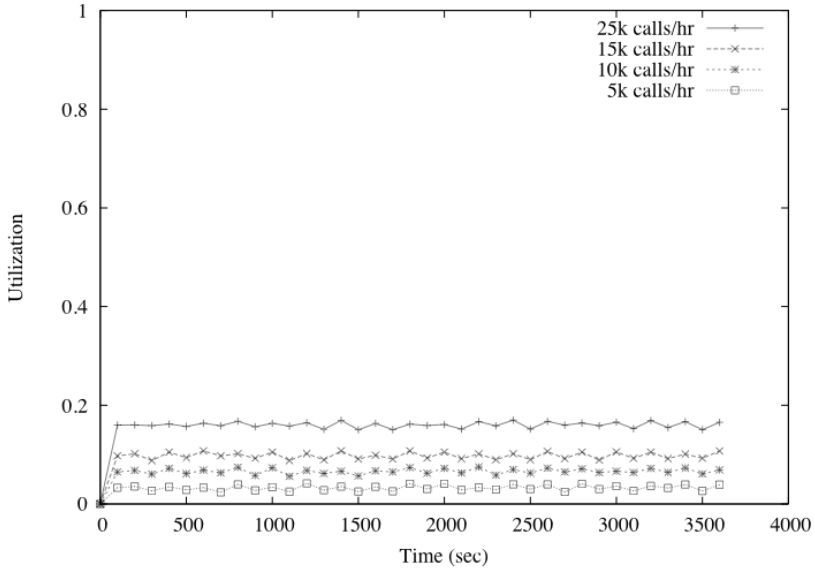


Figure 7: The average utilization experienced by control channels (SDCCHs) under normal conditions for a variety of traffic intensities.

5.3.1 Normal Traffic

Before exploring the characteristics of traffic during an emergency, it is necessary to understand normal conditions. Figures 6 illustrates the blocking rates for traffic channels under four different voice traffic loads given average phone call duration of two minutes. Most relevant to the current discussion is the nonexistence of call blocking. The absence of such blocking reinforces the robustness of the design of GSM as a voice communication system. Figure 7 further supports the blocking data by illustrating very low SDCCH utilization rates for offered loads of both 10 and 25K *calls*/*hour*.

Note that even during elevated periods of normal usage, the SDCCHs needed to deliver text messages remain lightly utilized. This observation during the design phase of the network motivated the use of SDCCHs for text message delivery.

5.3.2 SMS Surge

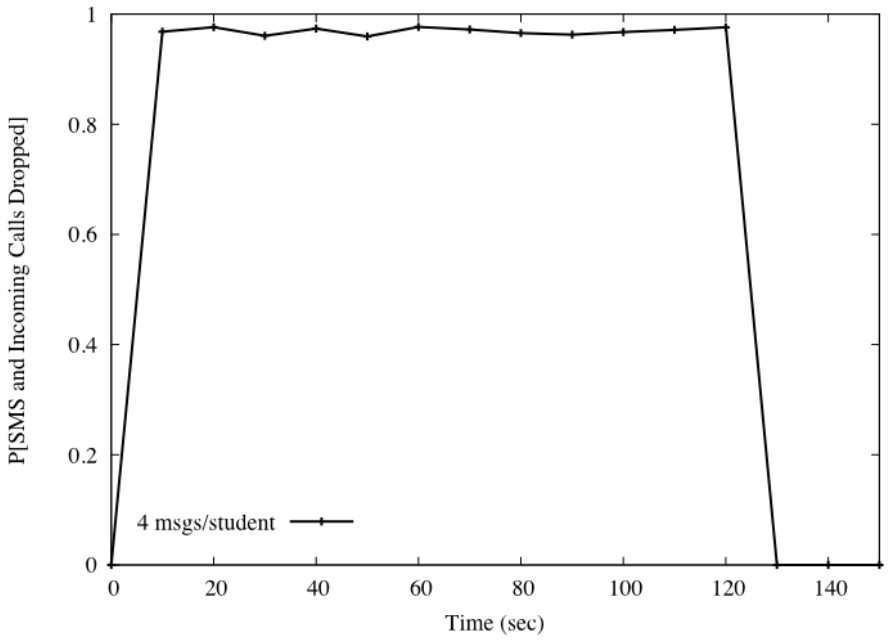


Figure 8: The influx of emergency text messages causes significant disruptions to network traffic, resulting in more than 98% of all new calls and text messages being undelivered.

We simulate the influx of emergency messages by assuming that the SMSC processes approximately 500 such messages per second. This approximates the rate at which such messages would be processed after having been injected through an aggregator (regardless of how quickly they were injected). Additionally, each emergency update is comprised of four text messages (640 characters), for a total of 60,000 messages. Note that this load does not include any voice or regular SMS traffic; however, similarly high blocking rates would disrupt both voice and SMS as they require the use of SDCCHs for connection establishment.

Figure 8 demonstrates that this burst causes problems for both the delivery of emergency messages and voice communications. In particular, during the burst, approximately 96.8% of all emergency messages are dropped by the network due to congestion on the SDCCHs. Given that the SMSC will not attempt to retransmit these messages again for at least 10 minutes, over half of the student body will not receive emergency information. Most critically, because the SDCCHs would be almost entirely congested, fewer people would be able to effectively communicate during such a period.

5.3.3 Emergency Scenario

Users having received notification of an emergency are unlikely to maintain normal usage patterns. In particular, users are likely to attempt to contact their friends and family soon after learning about such conditions. Whether by text message or phone call, however, such instinctual communication leads to significant congestion in cellular networks. This phenomenon led to an increase in the number of attempted calls to the Washington D.C. area by over 1000% percent on September 11th [27]. Accordingly, a similar spike in reactionary usage must be considered when designing text messaging-based EAS.

For this set of experiments, we assume that each sector receives approximately 1.5 incoming text messages per second and 1250 phone calls per hour. These values are equivalent to more than 43,000 text messages and 10,000 phone calls per hour. After approximately ten minutes, both text messaging and phone calls generated by users quickly spike to four times these levels. This traffic is in addition to the emergency text messages sent by the third party EAS. Figure 9 shows the impact of such traffic on voice and text messaging.

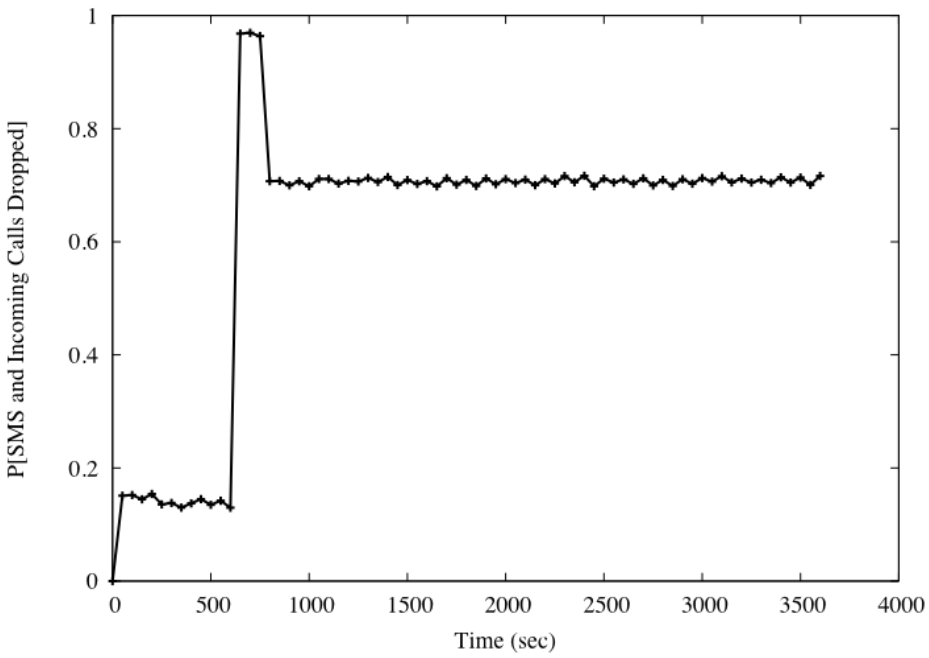


Figure 9: During an emergency scenario, it is likely that alert text messages able to reach their targets will cause significant spikes in usage. Such spikes make the delivery of voice calls and other information via text messaging nearly impossible.

Note that after the initial surge of emergency messages, nearly all messages *and* phone call requests cannot be delivered. In particular over 70% of all messages and phone calls are blocked. This value does not consider the impact of retransmission attempts by the SMSC for the text messages that were dropped during the initial surge. This result is also conservative in that it does not assume a continued increase of calls and text messages. Given that the emergency information critical to keeping the general public informed could change during this time, current cellular networks simply cannot support text messaging based EAS.

6 Best Practices and Moving Forward

From the discussions, mathematical characterizations and simulations in the previous sections, the mismatch between the current cellular infrastructure and EAS is clear. Accordingly, such systems can not currently form the basis of a reliable alert system in the timescales required by the WARN Act, regardless of promises made by third party systems. However, the ubiquity of cellular phones gives them a potential role in the delivery of critical information during an emergency. This role would be complementary to the other platforms of the Emergency Broadcasting System (television, radio, etc.).

Groups such as *Commercial Mobile Service Alert Advisory Committee* (CMSAAC) have addressed this problem. In particular, the CMSAAC determined that the messaging technology originally designed for mass notification, cell broadcast, is the most appropriate means of solving this problem. Unlike the point to point operation of current networks, cell broadcast would allow the rapid dissemination of emergency information through point to multipoint communications. Such a system could quickly reach all cellular users in an area and would not require knowledge of each particular user's location, similar to broadcast radio or TV. Such a solution may also improve the reliability of information delivered to the general population over third party systems. In particular, because cellular providers would conduct the dissemination of emergency information, it would be possible to add cryptographic authentication mechanisms to messages, allowing any user receiving a message to determine the source of such alerts.

Deploying networks with cellular broadcast capabilities will take time. Currently, standards organizations are working to agree upon common protocols to meet the technological challenges of mass notification and the time constraints of the WARN Act. As these standards are realized, the large scale deployment of such systems can begin in earnest. Until such systems are realized, however, legislators and the general public should not rely upon text messaging or third party EAS providers for delivering emergency information.

7 Related Studies

This work is not the first to note that text messaging systems have significant geographic volume limitations. In this section, we briefly discuss a number of previous studies highlighting related scenarios in which similar problems are identified.

Following the events of September 11th, 2001, curiosity about the ability to use text messaging as the basis of a reliable communications system during times of crisis arose. Charged with the coordination of the telecommunications infrastructure for purposes of national security, the National Communications System (NCS)[5] conducted an initial study of investigating the use of text messaging during an emergency. This study produced a number of important findings. Chief among them was the observation that if text messaging were to become the dominant means of communication during a crisis, current systems would require “100 times more capacity to meet this load” [27]. This study considered only the traffic generated by users and did not include the impact of traffic generated by EAS over SMS.

A 2006 study by the European Telecommunications Standard Institute (ETSI) identified the increasing prevalence of spam as a significant threat to the operation of networks during an emergency. Although cellular providers perform extensive and aggressive filtering, spam and malicious messages can be injected into a network through a huge variety of sources including, web interfaces, open aggregators, infected mobile phones, competing cellular networks with less stringent filtering policies and bulk advertisers. Recognizing this, this report noted that the lack of authentication could allow an adversary to “create malicious emergency messages and cause a panic reaction for many mobile subscribers” [13]. Accordingly, the report reiterates that text messaging is not an appropriate technology to reliably reach large numbers of users in a limited time period.

The specific impacts on the reliability and security of such networks under torrents of text messages have also been explored. Traynor el al. [38] noted that an attacker could exploit connections between the Internet and cellular networks to cause significant outages. With the bandwidth available to a cable modem, an attacker could send a small but targeted stream of text messages to a specific geographic region and prevent legitimate voice and text messages from being delivered. While subsequent research was able to better characterize and provide mitigations against such attacks [39], it was ultimately discovered that a more basic problem was responsible. Instead of simply being a matter of using a low-bandwidth channel to deliver data, the real cause of such attacks was a result of fundamental tension between cellular networks and the Internet. Specifically, because cellular networks cannot amortize the significant cost of connection establishment when delivering data, they are fundamentally vulnerable to such attacks [40]. Accordingly, as long as text messages are delivered in the point to

point fashion as is done now, the expense of establishing connections with each and every phone in an area will remain prohibitively expensive.

8 Conclusion

Cellular networks have fundamentally changed the way in which our society communicates. Instead of calling a static location such as a home or office, we now call individuals and can reach them at nearly any time. Such “always on” connectivity may one day create new opportunities for the dissemination of critical information during an emergency. However, as demonstrated in this study, modern cellular networks are simply not capable of providing such a service, whether through voice calls or text messages. Through a series of experiments, we have shown that even under optimal conditions, these networks cannot meet the 10 minute alert goal set forth by the public EAS charter. Moreover, we have demonstrated that the extra text messaging traffic generated by third party EAS will cause congestion in the network and may potentially block the delivery of critical information, such as calls between emergency responders or the public to 9-1-1 services. Accordingly, it is critical that legislators, technologists and the general public understand the current limitations of these systems.

Efforts undertaken by the CMSAAC will allow cellular networks to take an active role during emergencies. Through the creation of new standards such as Cell Broadcast, many of the problems created by the current “point to point” architecture can be avoided. In particular, by allowing each base station to act as a virtual megaphone, cellular networks will be able to rapidly distribute up to the moment emergency messages to all phones. While nearly all major cellular providers are actively working to design, test and deploy such systems, it will take time before this piece of our critical infrastructure can perform such tasks.

9 Credentials and Acknowledgements

Dr. Patrick Traynor is an Assistant Professor in the School of Computer Science at the Georgia Institute of Technology, and a member of the Georgia Tech Information Security Center (GTISC). He received his Ph.D. and M.S. from Pennsylvania State University in 2008 and 2004 respectively, and in 2007 was awarded the Pennsylvania State University Alumni Association Dissertation Award. Dr. Traynor’s research focuses primarily on security for cellular networks and the impact of connecting these systems with the larger Internet. His work on this subject has been presented in top security and mobile networking conferences and journals and has also been covered by The New York Times.

Dr. Traynor wishes to thank the wireless industry association 3G Americas (www.3gamericas.org) for its support in funding research on this critical issue. Discussion or questions regarding Dr. Traynor’s conclusions can be submitted to traynor@cc.gatech.edu.

Appendix

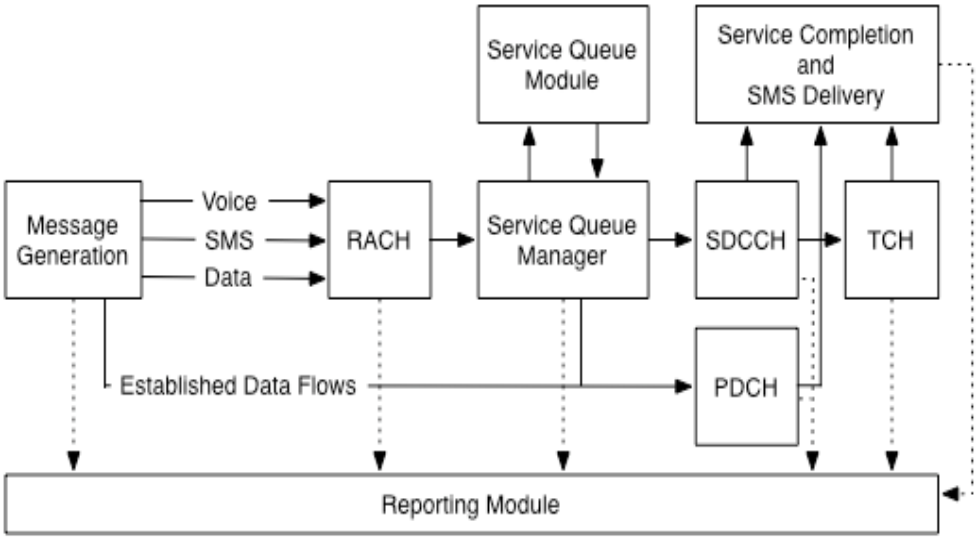


Figure 10: Simulator Architecture

Simulator Design

In total, the project contains nearly 10,000 lines of code (an addition of approximately 2,000 lines) and supporting scripts. A high-level overview of the components is shown in Figure 10, where solid and broken lines indicate message and reporting flows, respectively. Traffic is created according to a Poisson random distribution through a Mersenne Twister Pseudo Random Number Generator [21], saved to a file and then loaded at runtime. The path taken by individual requests depends on the flow type. We focus on the data path as the behavior of SMS and voice messages were explained in the previous iteration of the simulator.

If the network has not currently dedicated resources to a flow on the arrival of a packet, it is passed to the RACH module. This random access channel is implemented in strict accordance with 3GPP TS 04.18 [2] and is tunable via max_retrans and tx_integer values. Messages completing processing in the RACH are then delivered to the Service Queue Manager module, which is capable of implementing a number of queuing disciplines on traffic. For these experiments, we use simple FIFO queues as they best replicate network behavior. Messages are then sent to the SDCCH module, which processes messages if available. If no room is available, the message is dropped and the event is recorded by the Reporting Module. Should the message be a phone call, it is then forwarded on to a TCH, if available.

The accuracy of simulation was measured in two ways. The components used by voice and SMS were previously verified using a comparison of baseline simulation against calculated blocking and utilization rates. With 95% confidence, values fell within ±0.006 (on a scale of 0.0 to 1.0) of the mean. The simple nature of the PDCH module allowed verification of correctness through baseline simulations and observation.

References

[1] 3rd Generation Partnership Project. Alphabets and language-specific information. Technical Report 3GPP TS 03.38 v7.2.0.

[2] 3rd Generation Partnership Project. Physical layer on the radio path; General description. Technical Report 3GPP TS 04.18 v8.26.0.

[3] Agence France-Presse. Hoax text message spreads tsunami terror in Indonesia. http://www.breitbart.com/article.php?id=070606101917.31jf2eyb&show_arti% cle=1, 2007.

[4] S. Blons. Emergency team aids efforts. http://graphic.pepperdine.edu/special/2007-10-24-emergencyteam.htm, 2007.

[5] Cellular-News. Malaysian Operators Dismiss Hoax SMS. http://www.cellular-news.com/story/31247.php, 2008.

[6] T. Christensen. Ga. Tech Building Cleared After Blast. http://www.11alive.com/news/article_news.aspx?storyid=106112, 2007.

[7] CollegeSafetyNet. Campus Alert, Campus Security, Emergency Warning, college safety Crisis notification, Reverse 911, Mass emergency notification, Emergency Alert System, Cell phone alerts, Email alerts, Text Message Alerts, Student warning system, Student notification, campus notification, and Mass notification at CollegeSafetyNet.com. http://www.collegesafetynet.com/, 2008.

[8] Commercial Mobile Service Alert Advisory Committee. Public Safety & Homeland Security Bureau - Commercial Mobile Service Alert Advisory Committee (CMSAAC). http://www.fcc.gov/pshs/advisory/cmsaac/, 2007.

[9] Courant.com. University Emergency SMS service doesn't deliver. http://www.courant.com, November 13, 2007.

[10] B. K. Daly. WIRELESS ALERT & WARNING WORKSHOP, 2007.

[11] e2Campus. Mass Notification Systems for College, University & Higher Education Schools by e2Campus: Info On The Go! http://www.e2campus.com/, 2008.

[12] A.-M. Elliott. Texters to experience 6 hour delays on New Year's Eve. http://www.pocket-lint.co.uk/news/news.phtml/11895/12919/palm-new-years% -text-delay.phtml, 2007.

[13] European Telecommunications Standards Institute. Analysis of the Short Message Service (SMS) and Cell Broadcast Service (CBS) for Emergency Messaging applications; Emergency Messaging; SMS and CBS. Technical Report ETSI TR 102 444 V1.1.1.

[14]

Federal Communications Commission. In the Matter of Review of the Emergency Alert System, Docket Number 04-296. http://www.fcc.gov/eb/Orders/2004/FCC-04-189A1.html, 2004.

[15] Federal Communications Commission. FCC Auctions: Summary: Auction 73: 700 MHz Band. http://wireless.fcc.gov/auctions/default.htm?job=auction_summary&id=73, 2008.

[16] J. Gambrell. School shooting text rumours emptied elementary school by 10am. http://www.washingtonpost.com/wp-dyn/content/article/2007/12/29/AR20071% 22901050.html?sub=new, 2007.

[17] L. GANOSELLIS. UF to test texting alerts after LSU glitch. http://www.alligator.org/articles/2008/01/08/news/uf_administration/lsu% .txt, 2008.

[18] D. Geer. Wireless victories, September 11th, 2001. Wireless Business & Technology, 2005.

[19] Groupe Special Mobile. Services and Facilities to be provided in the GSM System. Technical Report GSM Doc 28/85, Revision 2, June 1985.

[20] GSM World. Brief History of GSM & the GSMA. http://www.gsmworld.com/about/history.shtml, 2007.

[21] J. Hedden. Math::Random::MT::Auto - Auto-seeded Mersenne Twister PRNGs. http://search.cpan.org/~jdhedden/Math-Random-MT-Auto-5.01/lib/Math/Rand% om/MT/Auto.pm. Version 5.01.

[22] Inspiron Logistics. Inspiron Logistics Corporation WENS - Wireless Emergency Notification System for Emergency Mobile Alerts. http://www.inspironlogistics.com/, 2008.

[23] Jakarta Post. INDONESIA: Police question six more over SMS hoax. http://www.asiamedia.ucla.edu/article-southeastasia.asp?parentid=50410, 2006.

[24] K. Maney. Surge in text messaging makes cell operators :-). http://www.usatoday.com/money/2005-07-27-text-messaging_x.htm, July 27 2005.

[25] K. Maney. Wireless text is logical basis for an emergency info system. http://www.usatoday.com/money/industries/technology/maney/2005-10-04-wi% reless-text_x.htm, 2005.

[26] J. McAdams. SMS does SOS. http://www.fcw.com/print/12_11/news/92790-1.html, 2006.

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

[28] National Notification Network (3n). 3n InstaCom Campus Alert - Mass Notification for Colleges and Universities. http://www.3nonline.com/campus-alert, 2008.

[29] National Weather Service. What is EAS? http://www.weather.gov/os/NWS_EAS.shtml, 2008.

[30] Oregon State Police. False Amber Alerts showing up on cell phones. http://www.katu.com/news/local/26073444.html, 2008.

[31] Reverse 911. Reverse 911 - The only COMPLETE notification system for public safety. http://www.reverse911.com/index.php, 2008.

[32] Roam Secure. Roam Secure. http://www.roamsecure.net/, 2008.

[33] shelbinator.com. Evacuate! Or Not. http://shelbinator.com/2007/11/08/evacuate-or-not/, 2007.

[34] SquareLoop. SquareLoop - Home. http://www.squareloop.com/, 2008.

[35] The 109th Congress of the United States of America. An Act to Amend the Homeland Security Act of 2002 to direct the Secretary of Homeland Security to develop and implement the READICall emergency alert system. http://thomas.loc.gov/cgi-bin/query/z?c109:H.R.2101:, 2005.

[36] The 109th Senate of the United States of America. Warning, Alert, and Response Network Act. http://thomas.loc.gov/cgi-bin/query/z?c109:H.R.1753:, 2005.

[37] P. Traynor. *Characterizing the Impact of Rigidity on the Security of Cellular Telecommunications Networks*. PhD thesis, The Pennsylvania State University, 2008.

[38] P. Traynor, W. Enck, P. McDaniel, and T. La Porta. Exploiting Open Functionality in SMS-Capable Cellular Networks. *Journal of Computer Security (JCS)*, 2008.

[39] P. Traynor, W. Enck, P. McDaniel, and T. La Porta. Mitigating Attacks on Open Functionality in SMS-Capable Cellular Networks. In *IEEE/ACM Transactions on Networking (TON)*, To appear 2009.

[40] P. Traynor, P. McDaniel, and T. La Porta. On Attack Causality in Internet-Connected Cellular Networks. In *Proceedings of the USENIX Security Symposium*, 2007.

[41] TXTLaunchPad. TXTLaunchPad provides Bulk SMS text message alerts to businesses, schools, and advertisers. http://www.txtlaunchpad.com/, 2007.

[42] Voice Shot. automated emergency alert notification call - VoiceShot. http://www.voiceshot.com/public/urgentalert.asp?ref=uaemergencyalert, 2008.

[43] Wikipedia. Virginia Polytechnic Institute and State University. http://en.wikipedia.org/wiki/Virginia_Tech, 2008.

Glossary

- **AGCH** - Access Grant Channel
- **CCH** - Control Channel
- **CMSAAC** - Commercial Mobile Service Alert Advisory Committee
- **EAS** - Emergency Alert System
- **HLR** - Home Location Register
- **MO-SMS** - Mobile Originated SMS
- **MSC** - Mobile Switching Center
- **MT-SMS** - Mobile Terminated SMS
- **PCH** - Paging Channel
- **RACH** - Random Access Channel
- **SDCCH** - Standalone Dedicated Control Channel
- **SMS** - Short Messaging Service
- **SMSC** - Short Messaging Service Center
- **TCH** - Traffic Channel
- **VLR** - Visitor Location Register

---

1 A more precise definition of these channels and their characteristics are given in Section 3.1
2 FEMA is now an agency within the Department of Homeland Security (DHS)
3 The *Special Area Message Encoding* (SAME) protocol.
4 The FCC reports that over $19.1 billion dollars were raised in the 700 MHz auction [15].
5 Now a part of the Department of Homeland Security.