Designing a National Emergency Wireless System

by

Richard Anderson

BS Information Science, University of Pittsburgh, 2003

Submitted to the Graduate Faculty of

School of Information Science and Telecommunications in partial fulfillment

of the requirements for the degree of
Master of Science in Telecommunications

University of Pittsburgh

2005

UNIVERSITY OF PITTSBURGH

School of Telecommunications

This Thesis was presented

by

Richard Anderson

It was defended on

April 19, 2005

and approved by

Prashant Krishnamurthy, Associate Professor, Telecommunications Program

Richard Thompson, Director/ Professor, Telecommunications Program

Martin Weiss, Chairman, Department of Information Science and Telecommunications

Thesis Advisor : Richard Thompson

Abstract

Designing a National Emergency Wireless System

Richard Anderson, B.S.

University of Pittsburgh, 2005

This paper looks at combining modern telephone services together for emergency support services. The newer services provided by 2.5 and 3G technologies, such as broadcast text messaging, GPS tracking and the ability to send video and images, has expanded our capabilities for sending information to a large consumer base. By taking these services, and targeting them towards emergency response crews as well as civilians, a new emergency system can be designed. Utilizing leading edge wireless technologies will allow workers to communicate faster, distribute information effectively, and provide better support during an emergency. Civilians can be warned of an impending disaster and can be alerted as how to proceed in an emergency situation. These new services can be added to the current infrastructure and can work on many of the devices already in use on the current cellular network.

Table of Contents

Table of Figures

1.0 Introduction

The first section of this paper provides the background and history of the current emergency alert system. It is important to first understand the purpose of why the system was created and why it is needed today. As the nation changes through threats of terrorism and natural disasters, our technology changes to support us as well. There have been many advances in security and technology services, and there is a definite need for new services to help citizens in times of trouble. This section also defines the target users and the differences between them. The need for emergency services is different for civilian users and emergency response crews. By identifying the target users of the system we can better model our devices and services.

1.1 History

The design of a National Emergency system was first created in 1967 to "provide the President with the capability to provide immediate communications and information to the general public at the National, State, and Local Area levels."[4]. The EAS as it is known today, encompasses 3 basic mediums of transmission: AM and FM radio, TV, and Cable TV transmission. It is also transmitted through wireless cable mediums where the population of observers is greater than 10,000.

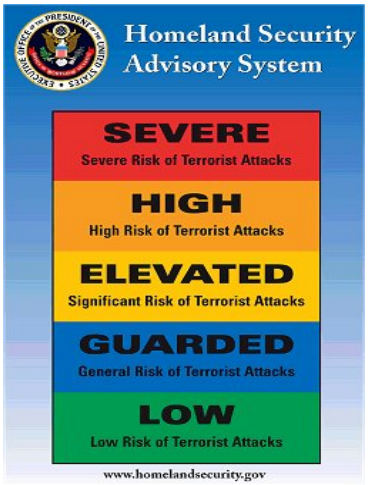
This thesis describes an emergency service for wireless technologies. In particular, it can be adaptable to 2G, 3G and newer Wi-Fi technologies. It will use the existing telecommunications infrastructure to both notify users of emergency situations, and direct them as necessary away from the area of harm. In addition to the emergency applications for which it can be used, the systems technology can be used for even more, wider applications.

An important concept to keep in mind is that the technologies currently exist to make this system work. Making the technologies interoperable with each other is the challenge. The author hopes to analyze the current systems in place and gives suggestions on how they can be brought together for a public safety service.

1.2 Changing times

The current state of the United States is much different than it was prior to September 11. Following the terrorist attacks on our own citizens, our government has overhauled its policies on security and warning mechanisms. With the creation of the Homeland Security department, a standard warning system was developed, which could be updated through television and news mediums in real time.

The visual warning system composed of only a few colors could be raised or lowered to inform the public of existing threats. Prior to this system was the Emergency Alert System (EAS), which sent out an 8-25 second dual-tone audio alert followed by the EAS message itself to the public via TV and radio media [4]. Although these systems were simple, they were not nearly informative enough and were too general in their warnings. The warnings are also sent out to users outside of the target zone, which is inefficient at the least.



1

Fig.1: Homeland Security Advisory System (www.homelandsecurity.gov)

Considering the widespread growth of wireless systems within the past 10 years we are looking at the “fastest growing technical device ever [7].”

The American market for cell phones, PDA’s, wireless hubs and other portable devices has greatly increased the spread of information. We have a medium with two advantages over any current emergency system. It can reach a much larger market of online users, and it has a specified range to target the critical users. Another aspect to consider is how ingrained the technology is today. Almost all individuals have cell phones, and many people now have multiple wireless devices. The tremendous growth of cell phone sales

over the past decade has helped distribute a communications medium to people in a way that has never been seen before.

The outcome of the attacks on 9/11 would have been very different if an emergency system such as this were in place. More people would have been warned and evacuation procedures could have been better coordinated. With the system proposed here, we can take the system a step further; we can relay correct evacuation instructions to people in the case of a widespread emergency. This will mitigate panic and will help to route congestion when traffic becomes an issue.

1.3 Target User Areas

In an emergency situation, the users are public safety officials and civilian users. Civilian users already have their own phones and data transferring capabilities between various phones and vendors. The challenge lies in designing devices for public safety officials. Much of the current emergency response equipment is outdated and can't support 3G technologies. There may be room to standardize graphic formats and modulation requirements for a new breed of wireless devices. This would allow interoperability between public safety officials (at least in terms of transferring information), and allow them to run on a separate network if needed.

In the situation where a base station has gone down, emergency workers could work in an impromptu mode until the network is restored. Their devices could work together as separate nodes to transfer information, and their equipment can form the backbone for a wireless Ethernet. This may also be useful if they can detect the signals from a trapped victim. With three emergency workers, one could essentially pinpoint a faint signal in rubble or covering through triangulation of the device signals. The ad-hoc system would use antennae diversity to increase the signal from a person trapped in an emergency situation. This could be used to save many lives in time sensitive cases where trapped victims need to be located quickly.

Making sure the right people get the right information is equally as important. Commercial services have commonly failed because of traffic during an emergency. In the case where responders need to communicate, the access to the network is denied due to the increase of traffic. People call their loved ones, news crews leave dedicated lines

open, and the swell of traffic prevents emergency responders from communicating and it causes more panic in the emergency zone.

Development of a good signaling scheme has been another area of research lately. In a Bell Labs paper on *Implementing Wireless Priority Service for CDMA Networks*, Michael D. Chambers and Douglas H. Riley have looked into building a frame which includes a wireless priority field to allow important calls to come through while less important calls are blocked. If a call comes in through the base station, the priority field may be set to allow the signal to pass on while other commercial users are dropped [6].

2.0 Current State of the Art

This section focuses on the state of the current systems in place. There are many aspects of these systems that will carry over to the proposed system. To understand the upgrades that will be necessary, a look at the current architecture will be needed. Understanding how the network is modeled now will help in understanding its limitations. The section then illustrates the previous systems for emergency response. The reader begins to see how the devices and GUI's play an important part in response to a disaster. This will lead into the next section about the discussion of the evolution of the system and how new applications will benefit the users.

2.1 Current Emergency Alert System

Developing a successful emergency system from scratch would be a daunting task for even an experienced security provider. Obviously, in order to be broadly applied to our cities and states, it would have to follow current regulation schemes. In particular, the Emergency Alert Service (EAS) would be the best format under which to structure the service.

The current EAS system began as a modification of the Emergency Broadcast System (EBS). In 1963, President Kennedy developed the EBS for broadcast stations to direct emergency information to the American people. Specifically, it was designed for the President to communicate with the people. Beginning in 1994, the EBS was replaced with the EAS, which updated the old system as a means to change with newer, more effective technologies. In 1997, the EAS began using digital signals to convey tests to broadcast stations. These signals can be decoded by televisions, radios, pagers and other devices (EAS Fact sheet).

The EAS has a few basic parameters that would map onto the cellular model quite well. Automatic operation is used to allow stations to send and receive emergency

information quickly and automatically (EAS Fact sheet 2). With the use of preprogrammed messages, a signal can be relayed to towers with specific information on where the messages are to be sent. For instance, if there was knowledge that an emergency situation was occurring in a certain cell, and the closest tower was unmanned, a signal could be sent from a neighboring cell to the MTU (Mobile Transmission Unit). In this case, our current network communication can be used rather effectively. The stations already communicate automatically during the handoff process and to update traffic information. Without much modification, we can use this monitoring information, previously used for increasing system performance, to take the human factor out of the operation.

Redundancy and less intrusion are two other parameters of the EAS that would be consistent with our model. Redundancy is not always available however. In some cases, there may only be one functional tower that may be taken out during an emergency. This would most likely be in a rural area, as opposed to the urban environment where towers can be seen in almost any given direction. All major telecommunications providers have emergency risk models for when sections of their network go down. They have built redundancy in order to route traffic under certain thresholds and with certain efficiencies. If the government were to regulate a system such as this, it will have to meet performance benchmarks.

The signal itself may need to be modified for less intrusion. Most of us are familiar with the old system tests. “This has been a test of the Emergency Alert System—this is only a test…” This works for cable, radio, and public services, but on private mobile systems it would be obtrusive and inefficient. Imagine if once a week you were to receive a call on your cell phone, or a text message concerning a “test” of the system. This would add more of a nuisance and would hardly justify its purpose as a service tool. Fortunately, with cell phones and mobile units, communication is done asynchronously on the network, and more important, pervasively. Where radio and TV are mainly one-way, mobile units are bi-directional. They are constantly sending out and receiving monitoring signals with their location relative to the nearest towers. We would never have to invade the users’ privacy with weekly and monthly messages. The tests can be sent out to each device, and by monitoring the number of devices that respond, we can

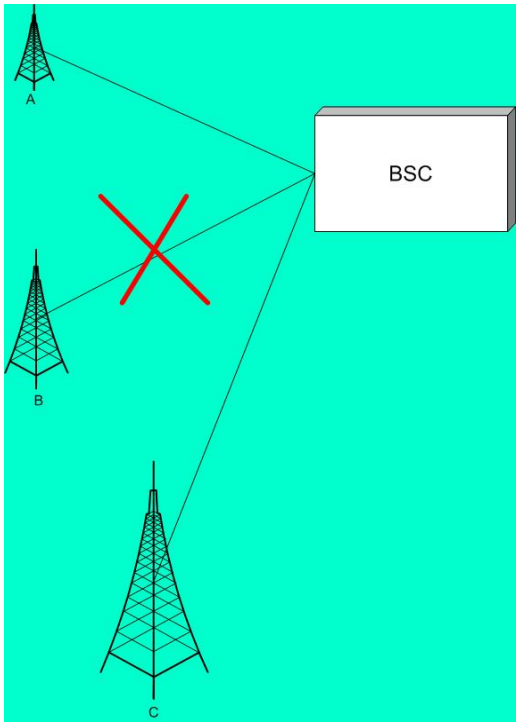
model the success of our system. This may lead to adding towers in certain places and boosting the transmission strength in certain areas.

The most important aspect of the EAS is that we will be reusing the existing infrastructure. This will mean lower costs and interoperability with the current system. Over time, the legacy components will be phased out as upgrades are needed.

2.2 Current Infrastructure and limitations

The EAS was not designed for wireless emergency use. The radio spectrum is very robust and can accommodate users well outside of the ideal power range. With a mobile, two-way communication system such as this one, power requirements and signaling standards will need to be modified.

Currently, cell towers are built to only execute adjacent handoffs organized by a Base Station Controller (BSC). Because cell towers communicate through the BSC, there may be issues communicating when a BSC is down or the tower itself goes down. In Figure 2, tower B has lost communication to the BSC. In this case, by using a shadow network design, the tower could uplink transmission to the other surrounding towers, and the information could then be passed on through the wired network via the BSC. When the BSC realizes it has lost communication, it would relay the information to the nearest stations to switch into a shadow communication mode to accept radio transmission from the tower if possible. In cases where the tower is permanently down, mobile base stations can be set up to relay a users call to the surrounding functioning towers.



2

Fig.2: In the case tower B is not connected to the network, how can communication be restored?

Current telephone systems use a variation of this idea with SS7. The importance of SS7 as it relates to this paper is that towers can communicate with other stations not directly adjacent to themselves. With the cellular network, the towers can communicate with each other, but the connection between the user and towers is not interconnected in this way. In the case of a disaster, the network may realize a tower is down, and the surrounding towers would recognize this as well. The surrounding functioning towers would recognize this based on the SS7 architecture, but communication in the affected area would still be down. Wireless ad-hoc networks can be setup to relay information to the surrounding, functional towers.

Known as “Shadow Networks”, these base stations surrounding an emergency region redirect their signals to accommodate users where the signal has gone down [2]. If too many towers go down, the traffic interference will create more problems for the affected area, so designing an infrastructure to support these networks is crucial. Ad-hoc networks are limited in scope because many of the current devices in the market do not support the technology and it has not been implemented extensively in commercial systems. When a section of the wireless network goes down, shadow networks can serve people located within the surrounding areas. In areas where the wired network is down, the base station can pick up the signal from users within the affected cell, and transmit the signal to surrounding towers on a separate uplink frequency. The surrounding towers can then send the traffic back over the wired network. This may be a way for us to manage traffic and prevent flooding. Directional antennae on functioning towers can be used to pick up the signal from the shadow area. This traffic can then be prioritized and sent over the network.

The ideal system would require metropolitan and urban areas to have shadow networks designed around them. Suburban and rural areas with smaller population densities are less critical during a disaster and would not need as complicated an infrastructure.

2.3 Current Projects

The technology is in place for a mobile EAS, but pulling the different areas together will be a challenge. The competition among vendors and declaring equipment standards are two issues currently slowing the deployment of Project MESA, the government's mobile emergency response system. The scope for Project MESA is to provide mobile services for emergency responders. It would be beneficial to increase the scope to include broadcast text messaging and GPS services to civilians. Making sure these services are effective to their users will be a constant work in progress. Devices and interfaces will have to constantly evolve as flaws are discovered.

As beta designs are developed, they should be rolled out during low-emergency situations where their involvement will not cause negative side effects. It is important to look at the form factors of the various devices and decide what types of emergency messages will be the most effective. I believe that this will be the most critical part of the design and at the same time the hardest to implement across all vendor platforms. Cell phones are known to have a much smaller interface than PDA's, which are much different than laptop devices.

Fig. 3 Emergency responders may have laptops or tablet PC's for use. Civilian users will receive text messages and GPS instructions. The various GUI's to be designed need to take these form factors into consideration..

3

We are also at a critical point with the technology where higher data rates are bringing newer applications to our devices. Many cellular devices now support multi-colored photo and video capabilities in addition to current text features. However, we must look at the current market and compare it with the market growth in order to determine which types of GUI's will be more effective. Colored displays may have some

uses in certain instances, but the system should employ a grayscale color scheme to provide the least amount of distraction to the user.

Another point to consider is the difference between emergency responder equipment and the average user equipment. Emergency workers may have standard devices capable of high quality graphics and images. These features should be used to the best of their extent during an emergency. The information transmitted to civilians would most likely be a text message warning, which would be broadcast as a normal text broadcast is done today.

3.0 Proposal

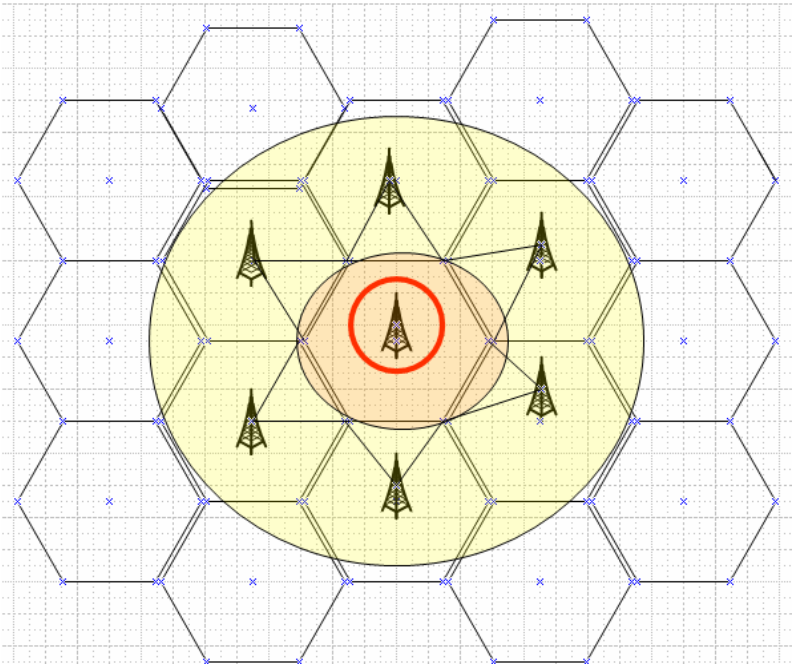
This section is devoted to explaining the proposed system. Beginning with the redesign of the current infrastructure, it also focuses on how to best distribute information in the system. From here, we describe some of the services available to the end users. The final product is described, and all of the components that will merge are explained in detail. From ad-hoc networks to system testing and security, the evolution of services and design are explained in full.

3.1 Re-designing the Architecture

The proposed emergency system should be very precise in how it distributes information. Every base station uses GPS coordinates to identify a particular area. All mobile units are tracked from a mobile switching center and this information is constantly updated as users move in and

out of a location. The means to track an area are there, so in the case of an emergency we can send a signal to a targeted region.

However, there is a major problem with this; the chain is only as strong as its weakest link. What happens if a base station goes down? This upsets traffic flow in the wireless network and has caused major problems in the past.



4

Fig. 4 The circled area is down has no communication.
Adjacent towers increase power toward focused region to maintain service.

In the event of an attack or an act of nature, a transmitting center may be destroyed or rendered inoperable. This would completely shut down the system for a large period of time. Through analysis, it is possible to monitor routing situations and emergency response systems to find ways of routing messages through downed links. Modern cell phones use multiple towers at the same time to relay information. Most telecommunication companies have some kind of disaster plan, and others specialize in this area. It will be important to incorporate these ideas with the emergency system so that the down time will not be noticeable to the users.

Once again, this is an opportunity to incorporate shadow networks into the infrastructure. This will help mitigate the problems of network traffic flooding when a key node goes down. Many companies may need to upgrade their infrastructure to communicate in this way. Building a shadow network into the current network may depend on the population density and size of the area.

Implementing priority packets for emergency responders will enable them to use the network while dropping other civilian users. This implies an IP architecture underlying our network. Currently, 2.5G systems provide data networks in addition to

their voice networks. The evolution to 3G will require higher data rates made possible by networks completely running IP traffic. This will be a good instance where the priority field is used in the IP header. Base stations are currently being upgraded to support these 3G services, and many are already running some IP for their data networks.

From here, surrounding base stations will broadcast emergency information to people within their sectored cells. The traffic on the network will not accept civilian uplink of voice or data transmission unless needed. This would happen if it were necessary to collect location data to survey the scene, where only civilians may be located. This extra information may be helpful to emergency responders, but would also increase the traffic on the network. Deciding whether this is an effective way of communicating information during an emergency will need to be tested extensively.

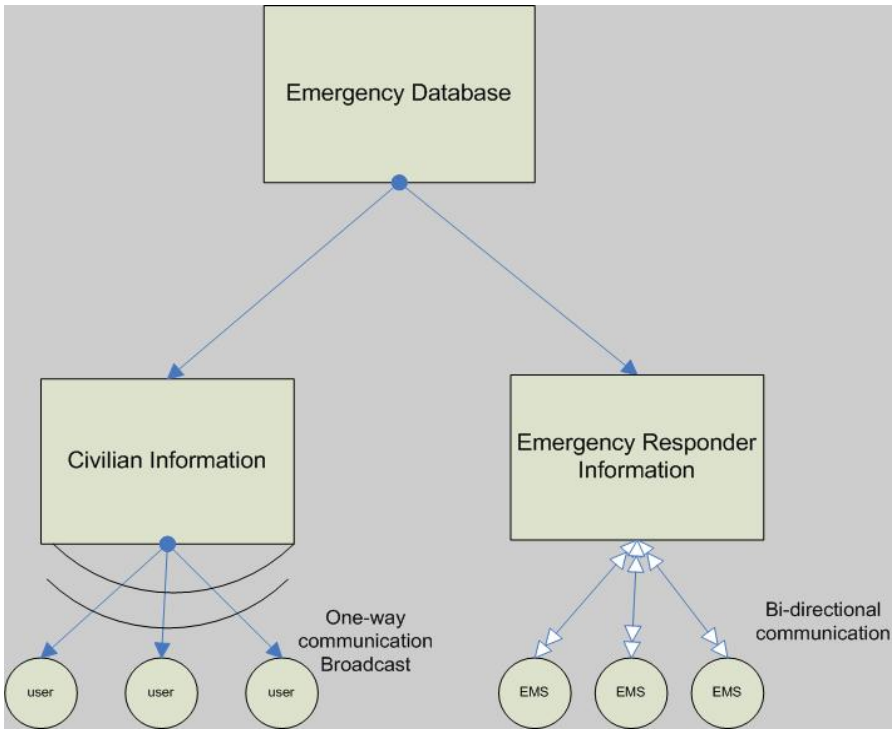


Fig. 5 Showing how information is passed to both target user areas.

5

From the figure above, one can see how traffic will be segmented. Civilian traffic will be a one-way broadcast message. We can then use an emergency flag in a CDMA frame to put the MU into an emergency mode. This emergency mode will have a unique code for all devices within this area. All civilian devices will occupy this portion of

bandwidth and drop from transmitting data. This will free up needed bandwidth for emergency responders who will need to utilize two-way communications.

Depending on the sectoring of a cell, broadcast details can be more refined in their scope. When an emergency occurs, a tower may only need to transmit certain information in one direction. In the figure below, the tower is transmitting to the area in red. In this case, the other sectors of the tower would transmit as normal. The sector providing coverage to this area would transmit in emergency mode, regulating traffic to those within the coverage area.

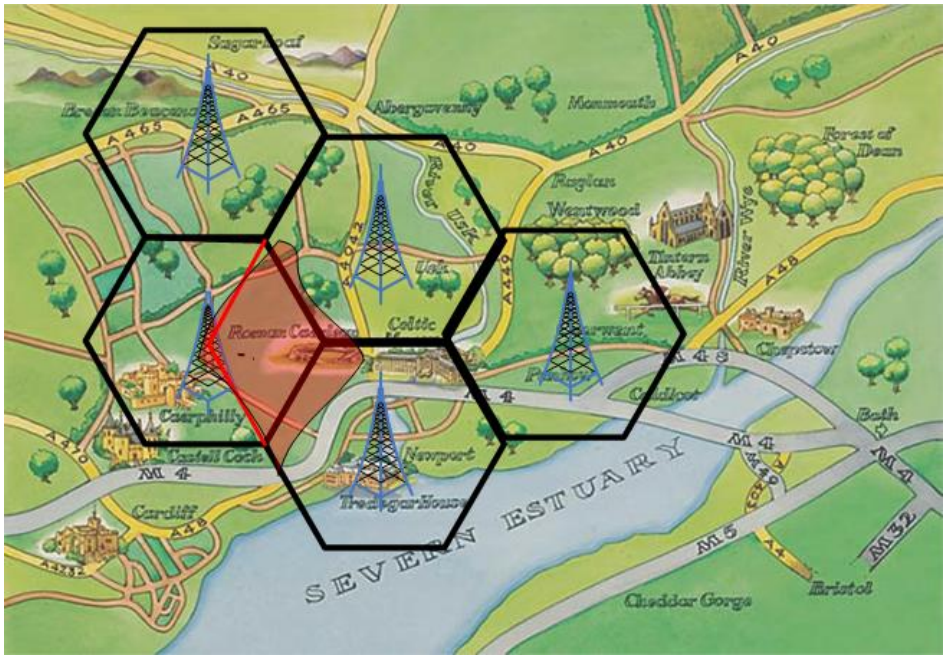


Fig.6 The area highlighted in red shows the sector of emergency coverage.

6

It is also important to note that the current wireless system is not attached to the EAS in any way. A system upgrade would need to add functionality for broadcast voice and text messages. EAS messages will remain separate from GPS notifications, which may be used for a selective group of users. The purpose of the EAS is to alert civilians, while the emergency GPS and text notifications are in place to rescue and help in an emergency situation. Keeping these messages separate will help in evolving from current equipment to new equipment.

It is possible to use the current equipment to broadcast text messages to users. New equipment will only have to be added to support EAS messaging. Depending on the equipment in place, it may only need software added to distribute this message, as most radio towers are equipped to broadcast these messages as well.

3.2 Implementing the technology

One can also look at the MSC data in a quantitative way. It is known where traffic flows in a city and the major roadways, as well as the off-roads. This information is also available to us through GPS tracking. We can view the information graphically to see where traffic is flowing at what times, and where it can be routed. Essentially we make the MSC work as a mapping router and we route people down different paths. In the event a pathway goes down or is blocked, we can notify the users of a blockage and direct them to the best path. If we have multiple paths available to us, we would obviously not want to direct all traffic down one. We can choose randomly from our MSC data which roads to send people down during an emergency evacuation or disaster.

One disadvantage is that the destination of a user is never known. If a traveler appears to be headed towards the emergency area, they may not actually be going there. They could turn off the path or could be backtracking to a different area. In some cases directional information is therefore not needed and would be wrong. It should then be an offered service, but not a mandatory one. The user could have an option on their screen to request a navigation service if needed.

There is also a tendency for people to ignore or rebel against direction. This may lead some people to think it is possible to head towards a disaster region or to not evacuate the region because they don't fully understand the magnitude of the threat. By assigning emergency codes to different disaster types, local governments can send out proper warnings to their citizens. An example would be a tornado warning. Although they are considered by many to be a serious threat, regions in the southeast and Midwest have dozens of them a year. It should therefore be a choice of the local government to issue a warning based on the threat as perceived by the local citizens.

Location based systems are also met with resistance by privacy advocates. When information exists concerning a person's whereabouts, who has access to the information

and who can see the information is of great importance. This data is constantly processed by the base station controller, the home location register, and visitor location register of the service provider. In this case, the cell phone ID is transmitted to subscriber management systems to process billing data. At some point the device information is mapped to the person and their private data. This system should be maintained to keep the highest privacy standards for all users. In this way, only the service provider has access to the information, but it can be organized for the proper authorities to review.

This service is currently supported in GPS systems. The data is organized and distributed well enough so that an individual in a car can have voice directions given to him/her in real time. If one is driving down a road, he/she can be told to make a right at the next intersection if need be. To send individual signals to each person in a disaster area would flood the system and bring it down. But if the information was streamed to a base station and broadcast through directional antennae, the information could be given to mass groups of people at a given time. Since it is desirable to lead large groups of people to certain safe zones, a broadcast of this sort would be useful.

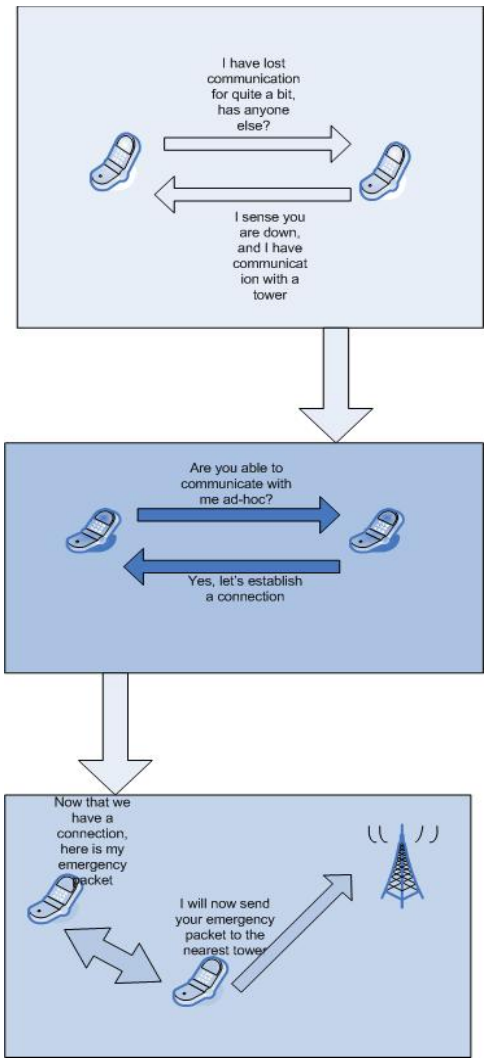
3.3 Evolution and Migration

The emergency network will have to be upgraded at some point, and evolving services and equipment from one generation to another is another problem presented. Recently, there have been many papers written about implementing high tech solutions for Homeland Security. Currently, there are two main second-generation (2G) services for public safety officials. Project 25 and TETRA (Terrestrial trunked radio) operate under the New Technology Standards Project and support data rates up to 1.544 Mb/s for 3G technologies [5]. Their services and features were built to serve “a broad spectrum of public safety and other governmental services, including law enforcement, emergency management and disaster services, life and property protection,..., the federal government, the Department of Defense, and federal law enforcement [5].” It addresses the problems related to distributing information to the authorities and emergency response crews during an emergency. What it does not address is how to provide support for civilians and the majority of victims during an emergency.

One of the drawbacks to the current services offered is the low data rate of the outdated technology. Although the Project 25 standards require higher data rates, in actual practice the rates are much lower Data rates only support up to 9.6 Kb/s with Project 25 and 28.8 Kb/s with TETRA [6]. This limits the use of text and visual information and presents a problem for other portable devices such as laptops and PDAs. In order to present higher data rates for wireless services, the Project 25/34 (P34) New Technology Standards Project was issued under a Statement of Requirements for public safety wireless data services [6].

These requirements issue proposals for interoperability between different telephone networks, the development of new communications infrastructures, and support for data rates varying from 1.544 Mb/s to 155 Mb/s. These data rates could support the graphical information needed to direct emergency response teams in the case of a disaster. They could also support visual information to the current line of cell phones and PDAs that have image support and higher resolution screens.

Another advantage of 3G systems is the support for Geographical position and automatic location data. This would be very useful in building a map of the disaster area, and locating victims trapped in the emergency zone. Right now, many companies support this type of service as an add-on, and GPS databases could be mapped on top of this information.



In the worst-case scenario, many base stations could be destroyed or rendered useless due to a natural disaster. An ad-hoc design may help to mitigate this problem by making each wireless device its own transceiver. In actuality, they already are working in ad-hoc, but the main tower controls the power consumption and range. Part of the evolution of devices would allow them to work in ad-hoc environments when needed.

It is then necessary to decide when to notify the phone company there is an emergency going on. Obviously one cannot send a signal from the cell tower. It is essential to find a way for a phone to know its location by a zone. From this data, it can recall its last known place. In an emergency where ad-hoc structure has developed, a signal can be passed notifying other devices of the emergency zone. This may be carried via an emergency frame in a VoIP packet, or a regular data signaling transfer.

When this signal is received, the phone may act as a beacon tool to alert emergency workers of its position. It may also communicate with other near-by nodes to alert them of its situation. The adjacent image shows the steps involved in transmitting the emergency information. A mobile unit times out in waiting from a base station response or receives a signal to go into emergency mode. It then sends out a signal to alert nearby devices. A nearby device responds to the signal to notify if it is capable of ad-hoc communication. They establish a dedicated link and relay information to the base station. This type of implementation would be useful in situations where other obstructions are blocking communications, such as a flood, collapsed building, or landslide.

New cellular devices should be built to store emergency information. Most of the location information is already stored on a device. Certain fields may need to be added for the device to properly manage its emergency information. For instance, in the case of emergency, a cell phone may go into ad-hoc mode, then communicate with another cell phone to relay emergency information to a nearby tower. This information could be gathered by emergency workers and used to locate victims during a disaster.

3.4 Mitigating Traffic Flooding

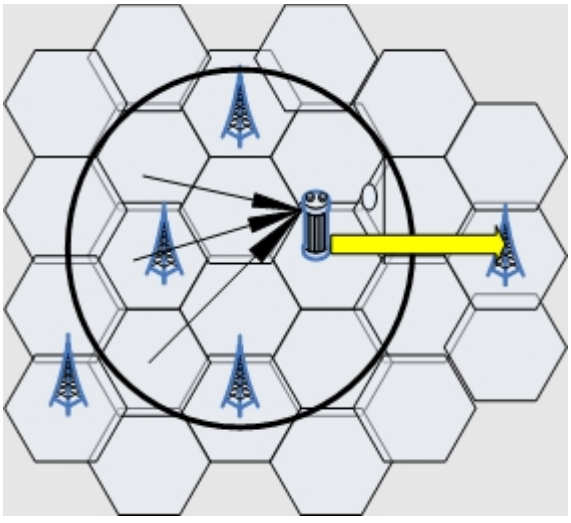
Probably the most important factor in the system design deals with making sure traffic flow is supported during a disaster. In every emergency situation, commercial services have failed due to traffic congestion. Thresholds need to be set on the capacity available in each sector. The best way to do this is by monitoring past data from emergencies in different metropolitan zones. It is possible to construct models to see how traffic spiked and we know what stations have gone down to cause this. We may look at a metropolitan area with a high population and figure there are 20 milli Erlang’s available for each user.

We may realize that during an emergency the traffic might spike an order of magnitude higher. We could then pad these areas so that extra antennas are added and during normal use each user may only use 10 mE of traffic.

Some tests may even require the device to respond to towers further away than necessary. This would be a good way of testing the system when a critical tower is down. If multiple towers are available, it is possible to configure the tests to randomly choose which towers transmit to which areas. We could then make system models to be used in similar situations. By running variations of disaster models, the network will have templates of which models perform best to the users in specific areas. Where the current EAS cannot be tested in this way to improve its performance, the cellular model can constantly evolve.

Shadow networks are one possibility to combat this issue. They are designed for backup purposes only. When portions of the network go down, outside towers connected to the wired network can help support the traffic load. The effectiveness of these networks has been shown to be a function of the number of active transmitters, the distance between the transmitters and receivers, the path loss exponent and the receiver sensitivity [2]. The limitations due to distance and equipment sensitivity can be lessened through the use of relay antennae placed in between the receivers and transmitters. By using extra radio equipment to service an area, we are able to send traffic to outside nodes in our infrastructure.

In the figure, the area within the circle denotes a disaster area where the towers have gone down. A relay has been brought in and placed to send signals to a tower outside of the normal range. Nodes within the disaster area can then be routed onto the wired network. This would alleviate traffic and the problem of traffic flooding during an emergency.



7

Fig.7 Showing how a relay transmitter can help reinforce emergency areas.

Bandwidth constraints and size limitations are certainly obstacles to overcome with this idea, but I do think this would be a good area for research. To my knowledge, there has not been anything done to specifically address this issue. Since this problem is encountered in every emergency situation, finding innovative ways to mitigate call blocking will be a good area for research.

3.5 EMS Design: Multi-User Communications

One proposed idea to mitigate this problem is with the use of ad-hoc networks. When a BS goes down, the mobile transmitters (MT) can establish a connection through other nearby MT's. It has been shown that a mobile unit can find a working station within an average of three hops [9]. Implementing a hybrid ad-hoc network would be a good design for disaster situations. As Fujiwara also described,

> "Primary roles are to collect damage assessment information and several kinds of emergency signals quickly and stably. The network has to maintain connections between nodes and BS in order to achieve the requirements."

In an emergency situation, many people may try to use their cellular devices and the flood of traffic may create too many blocks. However, as proposed by Fujiwara, Iida and Watanabe in their paper on an ad-hoc routing protocol for emergency communications, a robust routing protocol may be the answer to providing a working ad-hoc system. In emergency situations, "the network condition may change rapidly and extensively [9]" and so our communication system must change quickly to detect and transfer information.

Their proposed network scheme, "ECCA (Enhanced Communication Scheme Combining Centralized and Ad-hoc Networks) would allow for a hybrid of ad-hoc and centralized networking. I propose this as a means for public safety officials to communicate. For an ad-hoc network to work well there must be a great deal of interoperability in place between devices. Public safety officials with standardized government equipment could utilize this type of network the best. The drawback is that right now there is no good interoperability between public safety divisions. Local, state

and federal responders have no interoperability, which has been one of the major obstacles Homeland Security has been trying to overcome.

3.6 Testing

There must be a way to test the system to ensure it works properly. The devices should be tested for responsiveness and effectiveness. Sending out a constant signal may introduce heavy traffic to the system and constant messages would be invasive to the users, possibly even desensitizing them to the warnings. The messages must then be pervasive and only interact with the device itself. This can be accomplished with cellular systems and Wi-Fi systems where devices constantly transmit to the base station. The tower could send a message to the device and through an encrypted channel the device could respond, without ever notifying the user.

This now requires two signals in our system, one for an actual emergency, and one for monitoring the connection. If an emergency signal is sent, the device knows to transmit it to the user. If a monitoring signal is sent, the device will know to respond to the base station and not notify the user. In the case of a device not receiving a monitoring message, after so many cycles it may time out and the user could possibly be notified that they are not receiving a proper signal. It is possible to implement this through a data header field of some sort, rather than actually sending two separate signals. Bandwidth is very scarce, and as little as possible must be used in the signal.

Fortunately, some research has been done in this area. For channel access control, there are “two kinds of channels, a data channel and a control channel” [9]. The data channel is used to transmit data while the control channel sends status information between the BS and the nodes.

For broadcast frames, telephone companies already employ this technology to their users. Assuming they use a set field to designate a broadcast text message, interoperability between providers will be the only issue to overcome. Many providers have roaming agreements in place, and they can service users from other providers as well.

3.7 Channel Security

It is essential to determine a secure channel to broadcast this message and it must be in range of the various devices. We would need to send it through the 900MHz, 1900 MHz bands, as well as the 2.4 GHz band for Wi-Fi devices. The signal should be encrypted to prevent eavesdropping and to prevent false signals from being sent. One concern is that public safety officials do not have enough bandwidth available to them. If they use an ad-hoc hybrid network, they essentially create a small cell within their working area. Taking this into consideration, we can allow them currently used spectrum for use within these isolated networks.

The importance of security must be understood early on since we are entering a market with access to the Internet. There must be some approach to flaw testing in order to eliminate the flaws, prevent attacks to the system, and encrypt the system. At some point we must look again to the physical layer to ensure the towers are connected securely. Their current backbones will most likely suffice, and the operating company will most likely have strict measures in place to prevent outside tapping. Between the transmitters and receivers, some encryption will have to be deployed. It is important to find a method that can be processed quickly for cellular applications and will not consume large amounts of power. The current digital encryption used by vendors may be enough, but this signal should have some separation for added security.

Public safety officials should have stronger encryption and security than commercial users. Assuming both user groups will be broadcasting their signals, they are both susceptible to the same threats. The information collected by dispatchers may be needed for analysis and could also contain sensitive information.

Again, the issue of interoperability becomes a major problem with security as well. There are various levels of security for communications, networking and physical levels of the safety networks being developed. Vendors and private manufacturers use their own security mechanisms as well. Deciding on one single security system for public safety officials will have to be done as a first step to interoperability.

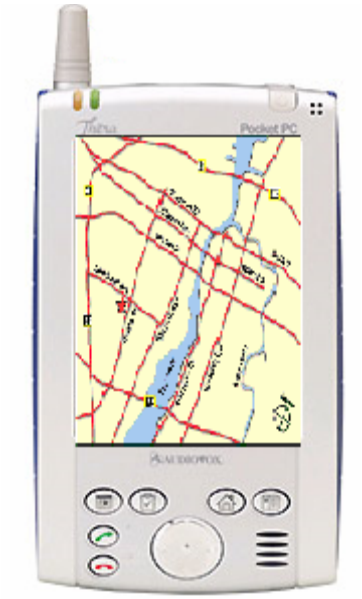
The emergency broadcast text messages should be encrypted to maintain the integrity of the message being sent. It is crucial that there is no interference with the data

being sent to civilians. The messaging should employ a very secure encryption scheme to prevent outside hacking or scrambling of the data.

4.0 Devices and GUI's

Wireless devices are generally built for portability and require smaller form factors in their design. Many PDA's and cell phones are built with variable screen sizes, however notebook PCs and Tablet PCs are built with larger screen sizes and higher resolutions. An obvious problem is how to distribute graphics among these various formats. The graphics need to be of a low quality format to minimize loading time. This will also have another advantage in that pictures will have to be simple and informative. In an emergency, instructions need to be clear to read and understand. They should also contain minimal details so that the user knows where to focus.

In the first example, a Toshiba 2032 model business phone shows a good map design:



8

Fig.8: Note the low level of detail, red colors for roads, and the use of light coloring in the background. Users can clearly see roads and a destination if available.

The screen size is slightly larger for this type of cell phone, but many GPS units have the same screen sizes. Right now, there are pocket GPS devices such as the Pharos Pocket PC Navigator designed for pocket PCs. These currently designed systems could be used for an emergency imaging service. To use these add-ons, one has to purchase an attachment for his/her device. For our case, each tower would only receive images within its area and could distribute them to phones within that cell.

The larger screen sizes available for laptop and Tablet PCs give more flexibility with image size and detail. Another example is presented to illustrate what a fully detailed map may look like on a tablet PC. In my opinion the use of this type of map demonstrates bad design. The image is displaying too much detail. Although the route is highlighted in red, there is more visual information than is necessary. It can be useful in visualizing the larger area, but there is also an abundance of extra information that would not be needed by emergency response or civilians.

9

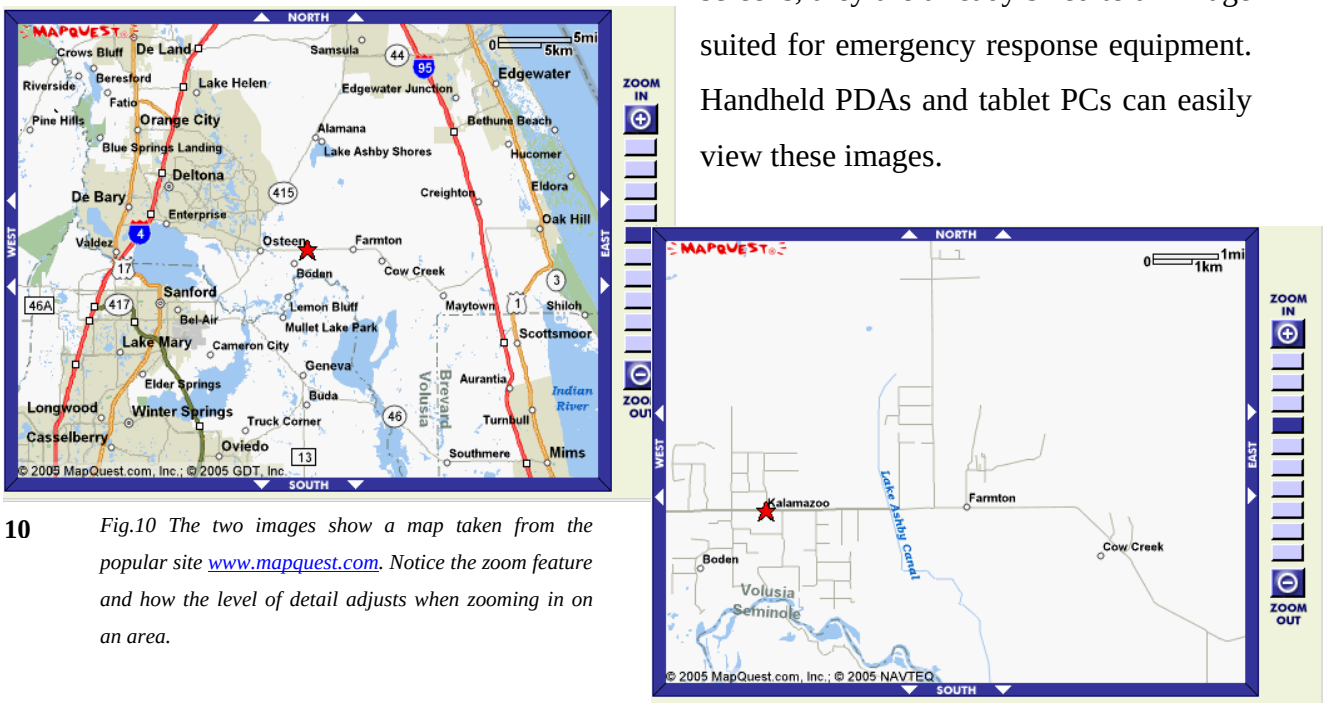
Fig 9: Note the higher level of detail, which can be difficult to read. The use of distinct color contrast will be essential.

A good design should be intuitive for the person viewing it. Emergency responders should have easy access to information quickly, so a "less-is-best" approach should be taken in designing the GUI. The visual aids and maps given to individuals should show only minimal detail for the purpose of their task. The proposed design would be similar to how modern map programs zoom into their targets. By zooming in on a map, one views at a more detailed picture, but the area presented is smaller. Instead of changing the area, I would design the maps to increase or decrease the level of detail. In this way, responders could view main roadways clearly distinguished from back roads and local streets.

The maps would be maintained through geo-spatial databases already maintained by various companies and GPS providers, as well as the US government. I am not discussing the security of the images in this paper. I will only suggest the maps being used for current GPS devices be sent to cell towers with spatial data to determine which

cell to send the image. Another source of maps that may prove useful can come from other common sources.

The image below is from the popular Internet website *mapquest.com* and there is a very useful tool located within this frame. The zoom features can be helpful for many reasons. People have a hard time distinguishing areas on a map. The zoom feature allows them to focus in and out on an area in order get a better mental picture of the area. The benefits of choosing popular web pages are familiarity with design for the user as well as the actual design itself. Because these maps and images are developed for computer screens, they are already sized to an image suited for emergency response equipment. Handheld PDAs and tablet PCs can easily view these images.

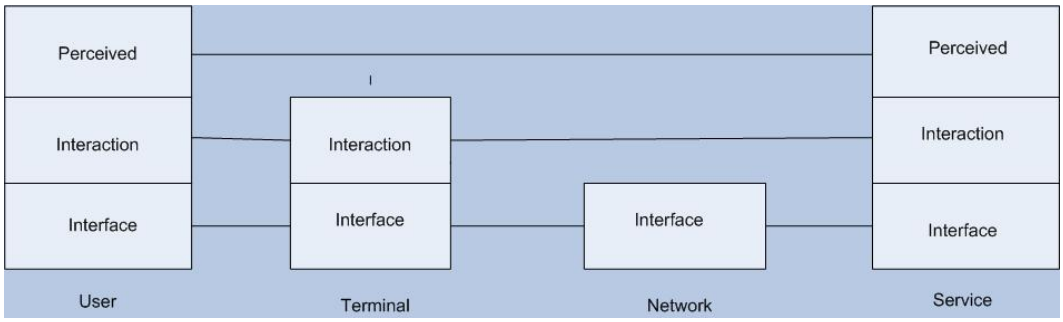


10 *Fig.10 The two images show a map taken from the popular site www.mapquest.com. Notice the zoom feature and how the level of detail adjusts when zooming in on an area.*

These images obviously need to be well sized and indexed to maintain a low bit rate for quicker viewing and to maintain the integrity of the map system. In order to be successful, one can take a look at some of the cognitive studies on user perception of interface systems.

4.1 Interface Design

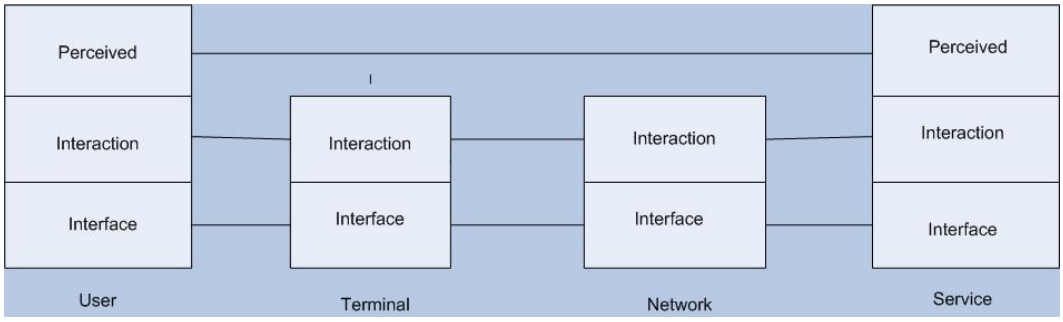
It is important to realize the abstract layers on how the users will interact with the system. The figures below are designed after network cognitive graphs done by Richard Thompson in his book "Telephone Switching Systems." They show how the user perceives the system and at what point they interact with the network or service. The layered processes shown in Fig.11 show how the varying levels will connect for civilian users. The users will interact with the terminal (phone), which interacts with the network. The users cannot interact directly with the network because the communication is one way between the terminal and network. This is slightly different from emergency response workers who can interact with the network in order to upload and transfer data. This communication interface is depicted in Fig. 12 below.



11

Fig 11(above): Civilian interface perspective. Civilians can view the network but can't interact directly with the network.

Fig.12(below): The interface for emergency workers allows them to communicate wit the network directly and update services for other workers.



12

5.0 Request for Proposal

The emergency services provided by this type of system need to be specified and exact in scope. Collectively, there are many uses for this service, but which ones fit best with current technologies and work will have to be decided over time. The FCC recently called for letters in an RFP for the EAS. An emergency system that could utilize the many new features of 3G would be an immense upgrade to the current system. Clearly defining how to design, build and test this system, along with an estimated cost for upgrading it will be essential for a proposal.

With the recent focus on Homeland security and the added funding for national security projects, the government would be the primary investor for this type of project, and the only supporter who is large enough to build it effectively. There are currently projects such as SAFECOM and Project Mesa that are dedicated to enhancing service for emergency responders. They both face the problems of interoperability between federal, state and local responder systems. If they can find a way of unifying these different levels, then building an emergency information network for these workers will be the next task.

Instead of requesting an overhaul of the current infrastructure, a request should be made adding broadcast text messaging to the current EAS services. This would be an option for cell users to enable, but free of charge. Based on varying levels of danger, a cell user may be notified of a forthcoming disaster. In the case of an extreme disaster, they would be notified regardless of whether they enabled their warning feature on their device. By dividing emergencies into different levels, a user can choose what level they would like to be alerted in the case of a disaster. In the case of the highest level of emergency, the user is notified automatically.

Level 3 Emergency: Major natural disaster, terrorist attack. – Mobile user notified directly
Level 2 Emergency : Flash flooding, mudslide, Category 3 Hurricane- User may be notified if feature is currently enabled on device
Level 1 Emergency : Small disasters; violent storms, local warnings. – Users notified if feature is currently enabled on device.

13

Fig.13 A sample design of how emergency situations will be divided. These levels separate emergencies into categories which a user can set their device to.

REQUEST FOR PROPOSAL OUTLINE

GENERAL INFORMATION

- Upgrade current emergency services to 3G to support civilians and emergency workers
- Implementation due to begin by 2007

PROJECT BACKGROUND

- Current emergency services are insufficient
- Knowledge of current emergency systems needed
- Knowledge of current telecom infrastructure needed
- Utilization of broadcast TXT messaging and GPS services

PROBLEM DESCRIPTION

- How do we provide location based services to civilians and emergency workers
- We would like to see priority services implemented to allow responders to communicate over the network
- We would like broadcast messages to be sent to civilians
- 3G services and a scalable emergency network
- Eliminate network downtime during disasters

DELIVERABLES

- An enhanced wireless emergency system
- Procedures on how to send efficient messaging
- Specialized equipment for emergency personnel
- Standardized equipment in commercial environments
- Nationwide compatibility

SELECTION PROCESS

- Reviewed by both government and industry sources
- Evaluated on proven effectiveness
- Tested through commercial use
- Peer review of all data will be needed

INFORMATION REQUIRED OF RESPONDENTS

- Policy and engineer work required
- Work to be done through government and vendor workers
- Will be able to deliver a secure broadcast text messaging system to all devices regardless of vendor.
- Will be able to deliver priority services to emergency workers
- Will be able to deliver a more robust network architecture

5.1 Development Costs and Planning

There is no easy way to predict the costs of building a system of this size. Deciding on how to roll out the upgrade will help in understanding the cost range of such a task. In the United States, the majority of the cellular system is CDMA with portions running GSM, notably from AT&T Cingular and T-Mobile. The cost of evolving from 2G systems directly to 3G is quite cheap for CDMA in comparison to upgrading to a 2.5 or 2.75 G network. However, for GSM it is cheaper to upgrade to a 2.5G system rather than directly to 3G. Because the nationwide GSM network is not as large as the CDMA network, this should not incur a large cost for upgrading services. We are considering the need for 3G based on the idea of sending rich graphic to emergency response workers, not for the civilian population. This means CDMA devices should be used for emergency response workers, since it will be cheaper to upgrade current 2G CDMA systems.

We will not need to upgrade the GSM networks running 2G to 3G because they can already support text messaging. For civilians using phones and devices, they will still receive warnings. Because it will be cost effective to upgrade to 2.5 or 2.75G services, we can still support data traffic, but not as graphic intense as with 3G.

Among the different CDMA standards, cdma2000 1xEV will most likely be the standard of choice for upgrading to systems that will be cost effective as well as robust for data handling during times of emergency. From a Qualcomm analysis of the varying CDMA standards, "cdma2000 1xEV offers the greatest competitive advantage because it is optimized for data throughput". The figure below shows a comparison of costs between the varying technologies, comparing the costs of sending data. This information was taken from the white paper "*The Economics of Wireless Mobile Data*" distributed by Qualcomm.

delays in technological development and deployment.

Table 7. Comparative Costs of Providing Data

	GPRS	WCDMA	1X	1xEV
Access Revenue/User/Month[1]	$40.00	$40.00	$40.00	$40.00
Cost/Mbyte @ Capacity[2]	$0.415	$0.069	$0.059	$0.022
Mbytes/Month/User	268	268	268	268
Network Cost/User/Month	$111.22	$18.49	$15.81	$5.90
Sales & Mktng and G&A/User/Month[3]	$16	$16	$16	$16
Earnings Before Interest & Taxes	–$87.22	$5.51	$8.19	$18.10
EBIT Margin	*–218%*	*14%*	*20%*	*45%*

[1] Source: Morgan Stanley Dean Witter; The Mobile Internet Report; 10/00; p.52. Estimates affordability of wireless data to be $25–$50 per month

[2] Excludes amortization of spectrum costs.

[3] Source: Based on a compilation of analyst projections for Sprint, VoiceStream, AT&T Wireless and Nextel.

Fig. 14: Shows 1xEV has the lowest cost per megabyte capacity. This means more available bandwidth within a region, addressing the current problems facing an emergency wireless service.

5.2 Costs of Network Evolution

If it is decided to upgrade the network hardware to cdma2000 1xEV, then costs will most likely be in the tens of billions to upgrade the entire nation. The most effective upgrade would start with major metropolitan areas. Limiting these to the top 30 cities, and assuming costs in the tens of millions, then we could assume the costs to be in the hundreds of millions, rather than billions. These costs are not based on collective data. Finding reliable sources for financial information is not an easy task due to the competitive nature of the cellular industry. Cost analysis is usually done in order to force an agenda, rather than provide an unbiased analysis.

The overall costs could be paid off over time through normal network use. The federal government should fund the initial costs in order to provide a national standard that will not be compromised by local budgets. This should take into account the upgrading of equipment for each provider in every area. With multiple providers covering the same areas, they should all have access to the new hardware. Equipment should be placed before the switching centers themselves in order for multiple vendors to attach their equipment into the emergency hardware. The figure below shows that we can keep separate hardware for the emergency services. This will eliminate costs of adding hardware to each vendor. It will also be more cost effective when upgrades are done because only one point in the architecture will need to be replaced.

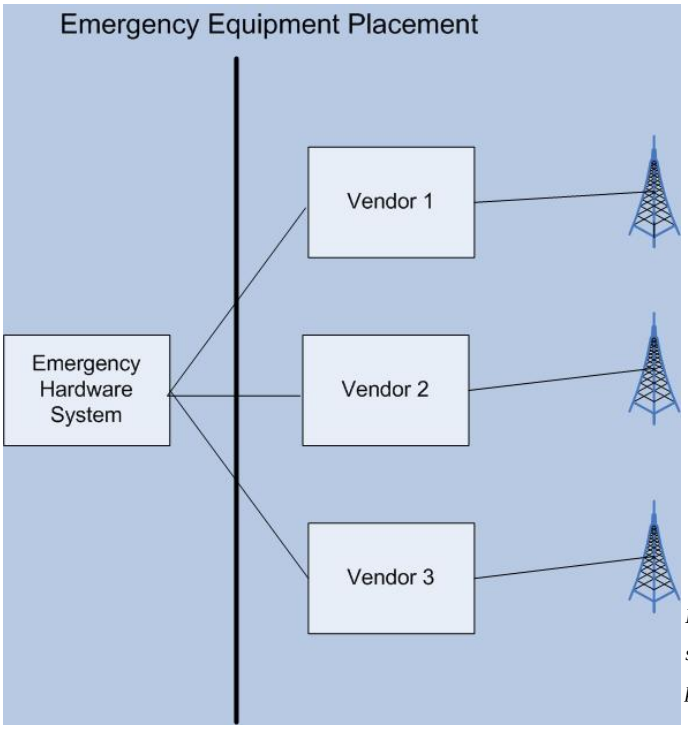


Fig.15: Showing a hardware system independent from provider equipment.

15

An upgrade of this system will require engineers to develop new hardware and equipment, test it, and deploy it. This would require teams comprised of roughly 70-100 workers in each area. Assuming an average worker cost of $160,000 (including direct and indirect costs) over the 30 top metropolitan areas, costs would be nearly $500 million. Each individual city would be approximately $20 million. Adding this cost to the estimated cost of hardware and system upgrades, one is looking at a price range in the billions of dollars. Upgrading costs will not be as expensive and will mainly be due to software upgrades, rather than hardware needs. Software upgrade teams will be much smaller and the costs for a team of 15-30 developers in the same $80,000 pay range (once again factoring in direct and indirect costs) would be a recurring yearly cost of $5 million. Over a ten-year period the cost of the entire system should close to $1 billion. Once again, these costs are estimates and the worker estimates are not based on data from service providers, which may fluctuate based on the size of the network and the area of coverage.

Analyzing the European market where wireless use is much more prevalent, upgrading costs can be much more for a large country, which may be the equivalent to the size of a region such as the Northeast. For a large region, an upgrade could cost close to $4.6 billion [1]. We can eliminate licensing costs if this is considered to be a government project. With this figure alone multiplied among the 6 main population regions of the U.S. (Northeast, Southeast, Midwest, Mideast, Northwest and Southest) estimated costs could be close to $30 billion to upgrade the entire nation.

6.0 Conclusion

There is potential for an effective national emergency system that provides services to effectively help people in times of disasters. Right now all of the services are available in some form. GPS mapping, image transferring and broadcast text messaging are some of the services that can be combined to provide information to people during a crisis. The problems that will be faced in combining these systems will include equipment upgrading and compatibility, traffic flooding, and the shortage of bandwidth. By using technologies

that utilize bandwidth more efficiently such as cdma2000 1xEV, we can help mitigate these problems. Separating the emergency systems from the vendor equipment will help to keep costs down and simplify upgrading of the network. Shadow networks and a combination of ad-hoc networks and wired networking will help to prevent traffic flooding when parts of the network go down.

This type of emergency network *can* be built and it should not be at a relatively high cost since most vendors are currently in the process of upgrading their networks for high data rate support. If the federal government sponsors this type of project, an implementation could be set within the next few years and coincide with the schedules of vendors such as Verizon and Sprint who are currently upgrading their own networks to EVDO and EVDV respectively.

Bibliography

[1] Olsen, L. Budry, "The Economic Perspective of the Mobile Networks in Europe," *www.sis.pitt.edu/~dtipper/PCS_mag.pdf*, 2004.

[2] F. De Turck, A.A. Lazar, "Modeling Wireless Shadow Networks," *MSSWiM'04 ACM,* pp.195-202, 2004.

[3] FCC Fact Sheet "The Emergency Alert System," *http://www.fcc.gov/eb/easfact.html*, pp.1-2, 2004.

[4] FCC, "Part 11–Emergency Alert System (EAS)," *http://www.fcc.gov/eb/eas/47part11.doc*, pp.1-3, 2003.

[5] K. Balachandran, K.C. Budka, T.L. Doumi, and J.H. Kang, "Third Generation Wireless Services for Homeland Security," *Bell Labs Technical Journal, Vol. 9*, No.2, pp. 5-21, 2004.

[6] M.D. Chambers and D.H. Riley, "Implementing Wireless Priority Service for CDMA Networks," *Bell Labs Technical Journal*, Vol. 9, No.2, pp.23-26, 2004.

[7] P. Krishnamurthy "Foundations of Wireless Communications-Lecture 1 Slides," p.33 2004.

[8] Qualcomm, "The Economics of Wireless Mobile Data," *http://www.qualcomm.com/main/whitepapers/WirelessMobileData.pdf*, pp.1-16, 2005

[9] T. Fujiwara, N. Iida, and T. Watanabe, "An Ad-Hoc Routing Protocol in Hybrid Wireless Networks for Emergency Communications," *Proc.24th ICDCSW*, 2004.

[10] Thompson, Richard, "Telephone Switching Systems," *Artech House Telecommunications Library*, Ch.15, 2000.

.