Emergency Service in Wi-Fi Networks without Access Point Association

Manav Seth
School of Computing
University of Utah
Salt Lake City, Utah 84112
mseth@cs.utah.edu

Sneha Kumar Kasera
School of Computing
University of Utah
Salt Lake City, Utah 84112
kasera@cs.utah.edu

Robert P. Ricci
School of Computing
University of Utah
Salt Lake City, Utah 84112
ricci@cs.utah.edu

ABSTRACT

Emergency "911" service is a critical function provided in the PSTN, cellular and VOIP networks. Wi-Fi, despite its growing importance, has no such service. In this paper, we develop a 911-like service for Wi-Fi capable devices, enabling them to send emergency messages through any available hotspot or access point. Our service makes use of existing 802.11 management frames and does not require the client device to associate or authenticate with the access point; this makes it available even on protected networks to which the client would not normally have access, even encrypted ones. This design ensures maximum potential reach and usability, and helps to increase public safety.

Categories and Subject Descriptors

C.2.1 [**Computer-Communication Networks**]: Wireless communication

General Terms

Wireless Service

Keywords

Emergency Service, 802.11 Wi-Fi

1. INTRODUCTION

Emergency "911" service is a critical function provided in the PSTN, cellular and VOIP networks [20, 22, 19, 18, 27]. In the U.S., the first 911 system was installed in 1968. Since then, the E-911 service has undergone several improvements and have been deployed both for cellular and VOIP in addition to the fixed line phones. The E-911 automatically associates a physical address with the calling party's telephone number, and routes the call to the most appropriate Public Safety Answering Point (PSAP) for that address. PSAP is a call-center responsible for answering calls to an emergency telephone number for police, firefighting, and ambulance services. There are roughly 6100 primary and secondary PSAPs in the U.S. Currently, some of the emergency services commonly available are:

- Enhanced 911 Service [8]
- Cellular Enhanced 911 [7]
- VOIP Enhanced 911 [21, 17]
- Automatic Wireless Fire and Smoke Alarms [1, 9]

Furthermore, the FCC has advertised that it will update the current E-911 service and enable citizens to report crimes through text messages, and even allow users to send video streams from their mobile phones to emergency centers [11].

Unfortunately, Wi-Fi, despite its growing importance, has no such emergency service. Wi-Fi is currently used by over 700 million people and there are close to 750,000 Wireless Hotspots around the world [6]. In 2009, 800 million devices capable of accessing the Internet using Wi-Fi were sold. Furthermore, the International Telecommunication Union (ITU) estimated that mobile cellular subscriptions worldwide will reach approximately 5.3 billion by the end of 2010 [10]. Of these, nearly 1 billion will be equipped with high-speed mobile web access. Hence, since more and more people are choosing Wi-Fi as their main means of communicating, it is imperative that there is an emergency service made for Wi-Fi. One of the challenges in providing such a service for Wi-Fi networks arises from the fact that more and more Wi-Fi networks are now secure. This security requires Wi-Fi users (mobile devices) to be authenticated by Wi-Fi access points before any data, even emergency data, can be sent or received.

In this paper, we build an emergency service in Wi-Fi networks that does not require any access point association or authentication. Using our service, Wi-Fi enabled mobile devices will be able to use any nearby access point or hotspot, secure or not, to send an emergency message, without going through any authentication or the association phases of the IEEE 802.11a/b/g/n protocols. At the same time, malicious users will not be able to misuse this service to access the Internet since this service will only allow a user to send an emergency message to an appropriate destination, which will be decided by the service itself. Some of the highlights of our design of Wi-Fi emergency service are as follows:

- **Build a new service**: This research shall enable any device equipped with a Wireless Interface Card to send an emergency or a distress message at any time to a Public-Safety Answering Point (PSAP) using any

ACWR '11 December 18 - 21 2011, Amritapuri, Kollam, Kerala, India

available 802.11 Wireless Access Point or a commercial hotspot having Internet access. The user will not be required to authenticate or associate with the access point and hence makes it possible to use even a protected or encrypted network to which the client would not normally have access, only for the purpose of sending an emergency message.

- We minimize the time to send the emergency message especially, in the presence of high load in the Wi-Fi network. Our system chooses an access point for emergency message transmission based on the following factors - strength of the signal received (RSS) from the access points, the number of current associations at the access points, and the past history of failures of access points in transmitting the emergency message.

- We build simple reliability by requiring the access points to acknowledge, positively or negatively, the transmission of an emergency message from a mobile device to the PSAP.

- The mobile device wanting to send an emergency message is able to check if the access point indeed has Internet connectivity before attempting to send the message.

- Our service also supports sending text messages and attachments to the nearest PSAP.

- Our service is also capable of finding the approximate location of the user and report it to the PSAP along with details like the MAC address and type of device used by the sender.

We implement our emergency service on the Ubuntu Linux platform. We use laptops for mobile devices and desktops for access points. Our service requires us to inject modified management frames into the Wi-Fi network. Therefore, we require the wireless cards on the mobile devices to support the *monitor* mode[1]. We require the wireless card on the access points to support the *master* mode. Using our implementation, we run a variety of experiments under different settings. We find that our system can deliver an emergency message from a mobile device to a PSAP in 1.8 - 2.4 seconds, depending on the load on the selected access point. Thus, our experiments indicate that our emergency service can be used in real settings.

1.1 Why such a service?

An emergency service which could be used by the general public using any available wireless access point will have a lot of potential. Such a service will be useful when:

- Sending an emergency message at a crowded place, without the need of specialized emergency kiosks (e.g.: at Airports).

- Sending an emergency message when there are no cellular signals. (e.g.: Movie theatres, underground rooms)

- This service can indeed be one of the fastest ways to send an emergency message or a distress signal

- Can be used by handicapped people who are unable to communicate or call an emergency service.

Rest of the paper is organized as follows. Section 2 describes the basic architecture of the service, the relevant details IEEE 802.11 framing, the detailed working using wireless NIC cards, some limitations and current problems of the system. Section 3 contains our evaluation procedure and results achieved. Section 4 discusses some existing work for providing emergency services to user using wireless devices and in Section 5 we indicate some directions for future work. We then conclude in Section 6.

2. ARCHITECTURE OF THE SERVICE

Motivated by the E911 Service, our architecture consists of a end-user terminal or host system which communicates with a Public Safety Answering Point (PSAP). The PSAP takes responsibility for listening to or reading the emergency message, making a decision based on the type of emergency, location, etc. and sending it along to the appropriate emergency service, such as a Police station, Fire station, or Ambulance service.

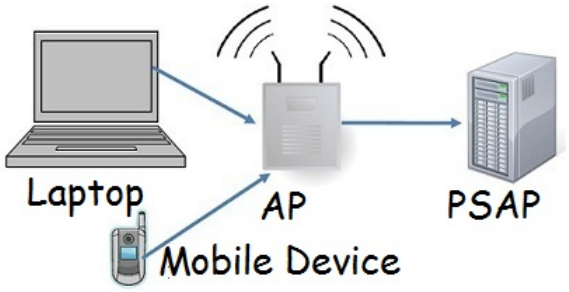

Figure 1: Basic Architecture of the Service

The user terminal can be any device having an 802.11 network interface card. The method by which the user activates the system may differ by the type of mobile device. On a laptop, this might mean pressing a pre-defined key sequence or running a particular command. On a smartphone, it might mean running a special app or pressing a "panic" button. Once activated, the user's device begins sending a message, which is relayed to a PSAP by an IEEE 802.11 compatible access point (AP) or router, as show in Figure 1. This relaying is done by using a novel mechanism that does not require the user device to associate with the AP, and which is described in the remainder of this section.

Software on the mobile device is responsible for activating the system, letting the user compose or select the emergency message, and transmitting it to an appropriate access point. A daemon running on the AP is responsible for receiving this message, finding the approximate location of the user, relaying the message to the PSAP, and verifying whether or not the message is successfully received by the PSAP.

2.1 IEEE 802.11 Framing

A primary design consideration for our system is that it should be *universally available*. Many APs are configured

[1]Monitor mode, or RFMON (Radio Frequency Monitor) mode, allows a computer with a wireless network interface card (NIC) to monitor all traffic received from the wireless network, as well as inject MAC frames in the wireless network.

to give access to a certain set of users by controlling which devices are allowed to associate, requiring a password, or encrypting the network traffic. In order to maximize the coverage of our system and its benefit to public safety, APs must be able to offer this service even to people who would not normally be able to use the AP. Our design should also make minimal changes to the 802.11 protocol, so that it is easy to add to existing AP designs (in many cases without hardware modifications.)

To achieve these goals, the communication between the user's mobile device and the access point makes use of 802.11 management frames. These frames can be sent even by client devices that are not associated with the AP, and they are always unencrypted. We make use of parts of these frames that are unused in the current 802.11 specifications. We give some background on the basics of 802.11 framing, and discuss how our design makes use of its features for emergency message transmission.

In IEEE 802.11, there are three major frame types.

1. *Data Frames* are the most common 802.11 frames, transferring data packets from station to station. Several different data frame types can occur, depending on the network.

2. *Control Frames* are used in conjunction with data frames to deliver data reliably from station to station.

3. *Management Frames* perform supervisory functions; they are used to join and leave wireless networks and move associations from access point to access point.

Data frames and control frames are only used after authentication and association with an AP. Therefore, we make use of management frames: this allows APs to offer emergency service to any user, without having to allow those users to authenticate and associate.

To explain our modifications to 802.11, we begin with the standard 802.11 frame format.

Figure 2: Generic 802.11 MAC frame

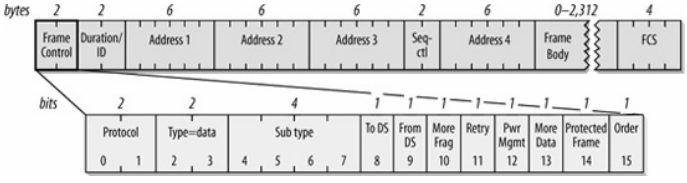

Figure 3: Frame control field

Figure 2 shows the generic 802.11 MAC frame. [2] Fields are transmitted from left to right. Each frame starts with a two-byte Frame Control subfield, as shown in Figure 3. The components of the Frame Control subfield relevant to our discussion are:

- *Type and subtype fields*: The `type` and `subtype` fields identify the type of frame used. For example, management frames have `type=00`. Probe requests, one particular type of management frame, have `subtype=0100`.

- *More fragments bit*: This bit functions much like the "more fragments" bit in IP

- *Protected Frame bit*: If the frame is protected by link layer security protocols, this bit is set to 1, and the frame changes slightly

- *Order bit*: Frames and fragments can be transmitted in order at the cost of additional processing by both the sending and receiving devices. When the "strict ordering" delivery is employed, this bit is set to 1.

The *Duration/ID field* follows the frame control field. Under some conditions (when its 15th bit is set to 0), it can be used to represent the NAV (Network Allocation Vector). This value represents the number of microseconds that the medium is expected to remain busy for the transmission currently in progress; as described later, we use it to increase the priority of emergency messages so that they will get through even on heavily-loaded APs.

Management frames are used for Association, Disassociation, Scanning, Authentication, etc. Whenever a wireless station wants to determine which access points are in range, it broadcasts a Probe request. All APs that receive this request respond with a Probe Response frame, containing capability information, supported data rates, etc. to the station. Hence, probe requests and probe response frames are used even when the wireless station is not associated or intending to associate with an access point. Additionally, the frame body for a probe request has very few mandatory elements and hence can be easily modified with very little change to the existing protocol. Hence, for purpose of this research, we use the probe requests and probe response management frames to transmit emergency messages.

Our design tweaks the Frame Control subfield for these two management frames. Specifically, an emergency message of this service always has its *Order bit* set as 1. This enables us to make the frames of this service distinguishable from the "normal" 802.11 traffic. This is because normal 802.11 management frames always set the *Order bit*, *More fragments bit* and *Protected Frame bit* to 0.

2.2 Emergency Message Frames

IEEE 802.11 Management frames are quite flexible. Most of the data contained in the frame body uses fixed-length fields called *fixed fields* and variable-length fields called *information elements*. To embed the emergency service into the protocol, we use this flexibility of the management frames. We use the frame body of the management frames to store the emergency message, and set the *Order Bit* to 1 to distinguish the emergency frames from other 802.11 traffic.

Sending an emergency message is divided into 3 parts:

1. Selection of an AP

2. Forming and sending of the emergency packet by the mobile device

3. Processing of the received emergency packet by the AP

[2]All diagrams in this section follow the IEEE conventions specified in the IEEE 802.11 protocol.

For the purpose of selecting an AP, a process running on the wireless station scans all the available wireless networks and prioritizes them based on the signal strength values and the number of connections the access point is serving. This is similar to standard AP scanning performed by client devices. Because sending a message to the AP does no good if the AP is not connected to the Internet (such as an ad-hoc wireless network, or one which has experienced a temporary loss of connectivity) we have also added the ability to check whether the chosen AP has Internet. For this purpose, the node sends a modified probe request packet with the *Protected Frame Bit* and *Order Bit* set to 1. When the AP receives this probe request from a mobile device with these 2 bits set, it determines:

1. This is a frame part of the emergency service, so it should be forwarded to the daemon managing this service.

2. The mobile device is requesting lookup of Internet connectivity.

The AP then responds with a modified probe response frame. If it has Internet connectivity (ie. is able to contact the PSAP), the same two bits are also set in the response. Otherwise, the *Protected Frame bit* is set to 0.

The process of selecting an AP is done at startup of the mobile device and after regular intervals. This is done to minimize the time taken to send an emergency message; the scanning process takes a non-trivial amount of time.

After the mobile device has selected an AP, it then can send an emergency message at the appropriate. To achieve this, the station sends a modified probe request frame to its selected AP. To prepare this frame, the *Order Bit* bit of the Frame Control field is set to 1. The emergency message is put in the frame body of the packet.

The priority of the emergency message is increased by using an approach similar to SpectraLink Voice Priority [12]. Spectralink, a manufacturer of handheld 802.11 VOIP phones, has devised a special set of 802.11 protocol extensions, called Spectralink Voice Priority (SVP), to assist in making the network more efficient for voice transport. To support SVP-type mechanisms in the emergency service, access points and nodes must transmit emergency frames with zero backoff. In the presence of contention for the wireless medium because of data traffic, the emergency frames with zero backoff will certainly have a priority boost because data frames are likely to have a positive backoff slot. Specifically, the duration field of the frame is set to 0 and since the emergency message is a directed probe request, setting the duration as 0 will enable the frame not to be kept waiting in the queue.

The service also takes care of fragmenting the frame body if its length is more than 2312 bytes (the maximum allowable size). In this case, the *More fragments bit* in the Frame Control is also set to 1, in accordance with the 802.11 protocol.

In order to find the location, the access point uses Skyhook's [5] Wi-Fi Positioning System (WPS). The Skyhook WPS relies on existing WLAN access points for finding the location of devices that have 802.11 wireless interfaces. In WPS, the mobile device collects information about all visible WLAN access points in its vicinity, sends this information to the Skyhook location database which replies with a position estimate based on the aggregated information. The position estimate can then be directly used by a mapping application like Google maps or can be combined with other sources of location information, such as those from GSM stations or GPS. Positioning systems by Mexens [4] and the Fraunhofer institute [2] have a similar mode of operation. The access point also appends the MAC address and type of device used by the user to the emergency message. Then, forwards this message to the PSAP.

In our prototype, the communication from the AP to the PSAP is done via email, using a fixed address. (A deployed implementation could use a different mechanism, such as one that explicitly knowledges receipt at the final destination.) After successfully sending the email, the AP acknowledges this to the mobile device by sending a modified probe response frame with the *Order Bit* set to 1. If it fails to send the email, the AP does not send an acknowledgement. A simple flowchart of this process can is shown in Figure 4. The wireless mobile device, if it does not receive an acknowledgment, sends the emergency message to all APs in range except the one already tried. In this way, the user can be sure that the emergency message will be served by at least one AP. In order for the PSAP to distinguish between multiple copies of the message that may reach it through different APs, it has to keep track of the mobile devices served. Hence, the message also contains the unique MAC address of the mobile device, so that PSAP can distinguish between unique requests.

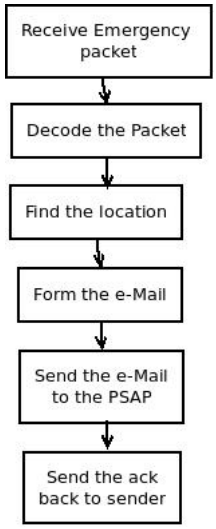

Figure 4: Role of the AP

To summarize, for the purpose of this service, the following frames are used:

- Probe request frame with *order bit* set: Used to to send the emergency message to the selected access point.
- Probe request frame with both the *order bit* and *More fragments bit* set: Used to to send long emergency messages to the selected access point.
- Probe request frame with both the *order bit* and *Protected Frame bit* set: Used to determine whether the chosen AP has Internet connectivity.
- Probe response frame with the *Order Bit* set: Sent by an AP as an acknowledgment of servicing the request

successfully. Also sent by the AP in response to the request of checking Internet connectivity if the AP does not have Internet access.

- Probe response frame with both the *Order Bit* and *Protected Frame bit* set: Sent by an AP in response to a request checking if the AP has Internet connectivity.

2.3 Implementation Details

Our prototype is implemented using a Ubuntu Linux laptop with an 802.11 wireless interface as the mobile device. Another Ubuntu Linux machine is configured to act a wireless access point (using `hostap` version 0.7.2).

To initiate the emergency message, we use a predefined key sequence (`ctrl + E`) on the wireless device. The process can also be started by entering the command at the terminal. The service can also be customized to the requirements of the user. For example, on a mobile phone, the emergency message could be sent by pressing a dedicated "panic" button.

The first step of this service is to **select an access point**. The two parameters used to quantify the value of an access points are received signal strength (RSS) and load on the AP. To determine the RSSI value (signal strength), our prototypes uses the `iwlist` command on Linux. To find the number of connections to an AP, the `tcpdump` tool is used to sniff the network of all the packets and then group the capture into groups based on the destination address.

As mentioned, the wireless station, after selecting the AP based on these two parameters, can also check whether the selected AP has Internet connectivity or not. In order to do so, it sends a modified probe request frame to the AP. The AP upon receiving this frame, initiates a different thread which does a *ping* to *www.google.com*[3] three times. If has Internet connectivity, the AP notifies the wireless station by sending the appropriate packet. A deployed implementation could more explicitly check for connectivity to the PSAP by contacting the PSAP directly with an application-level ping.

The following flowchart (Figure 5) illustrates the AP selection process.

To send any frame for this service, the wireless node injects 802.11 compatible packets, specifically the modified probe request packets. To achieve this, we put the wireless card in Monitor Mode and then inject packets using *pcap* library by manually forming the required packets and use raw sockets[4] to send them via the wireless card. In our prototype, the emergency message, is stored in a text file on the mobile device. The text file can be modified appropriately to accommodate the message the user wants to send to the PSAP. Further, the user has the option to attach a image with the emergency message. The emergency message, along with any attachments, forms the frame body of the packet which is injected. The entire process of sending the emergency packet can be illustrated using the following flowchart (Figure 6).

On the machine set up as an AP, the `hostapd` daemon process sends the frames which belong to the emergency service (probe requests having the *Order Bit* set) to the emergency

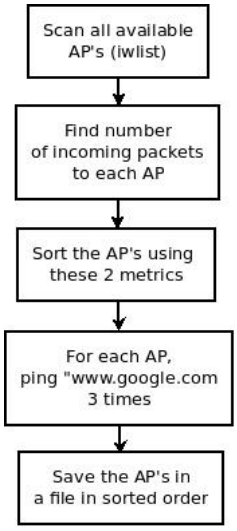

Figure 5: Selecting an AP

service daemon process running on the same machine. This is achieved using POSIX message passing API's. The daemon process then extracts the emergency message, find the location, relays the message to the PSAP and then sends an acknowledgment back to the host. The location, as mentioned, is found using the Skyhook WPS API. The response of the API is then formatted to this form:

Approximate Location:
latitude: 40.768348, longitude: -111.845170
Accuracy+/-171m 1
speed: 0.0km/h bearing: 0
Approximate Street Address:
12 Central Campus Dr
Salt Lake City, UT 84112

The PSAP on receiving this message takes the necessary steps of forwarding it to the appropriate destination like the Police, Fire department, Medical Hospital, etc.

The access point always creates a new thread to service an emergency request since this process should not interfere with its role as an access point and also it should be capable of servicing multiple emergency requests at the same time.

To summarize, the service is comprised of the following components:

- A program to select an Access point based on signal quality and strength
- A program which puts the wireless card in Monitor mode, calls the daemon process which makes sure the chosen AP has Internet connectivity.
- A program which puts the wireless card in Monitor mode, calls the daemon process which prepares the emergency message and sends to the AP.
- `hostapd` running on a Ubuntu Linux machine simulating an AP and forwarding emergency request packets to the daemon process.

[3] *www.google.com* because we use a GMail e-mail address as PSAP

[4] Raw sockets allow direct sending and receiving of network packets, bypassing all encapsulation in the networking stack of the operating system.

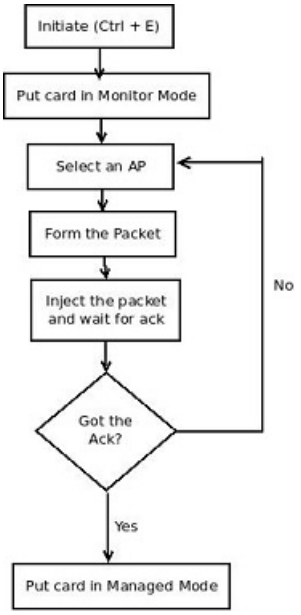

Figure 6: Sending the message to an AP

- A daemon process running on both the mobile device and the AP which actually creates the message and receives the acknowledgments.

2.4 Current Limitations

Our prototype implementation has a few limitations. The current prototype is not compatible with the chipsets which do not support packet injection. Many older wireless NIC cards available on laptops and desktops do not have this capability. Also, the wireless chips present in smartphones also do not allow packet injection. As a result, our current implementation could not be tested on such devices. To enable such an emergency service in these devices, the vendor has to incorporate the changes in the wireless driver or the 802.11 subsystem running on the devices. Our design, however, is specifically intended to make this easy, since it requires very few modifications in the current implementation of the protocol. Also, sometimes the wireless adapter is unable to transmit in monitor mode and is restricted to a single wireless channel, though this is dependent on the wireless adapter's driver, its firmware, and its chipset's features.

Our prototype will not run on any OS which does not have necessary API's and extensions for wireless monitor mode, for example older versions of Windows (prior to Windows Vista). For such operating systems, it will be necessary to develop or modify the drivers of the wireless network interface to enable monitor mode or use an USB Wi-Fi adaptor which supports monitor mode.

Another limitation of the prototype is the inability to determine that whether the PSAP has actually received the emergency email from the access point. The access point currently acknowledges the sender as soon as it is successful in sending the email across to the PSAP. This can be a problem since the sender will now not send another emergency message even though the PSAP has not received the email. This can be resolved by using an alternate protocol to contact the PSAP which explicitly acknowledges receipt of the message.

2.5 Possible attacks on the service, and defenses

The service is susceptible to a rogue or fake access point attack. In an area where there is no available access point or hotspots, the attacker can place a malicious or rogue access point which adheres to the protocol set up by the emergency service, but doesn't relay the message to the PSAP. Such an access point will even cause problems when the rogue access point has the highest signal strength. All the nodes will try to send the rogue access point the emergency message and will also be acknowledged. But the access point will never send the message across to the PSAP. Detecting rogue or fake access points has been a long standing problem [15].

One way to tackle this problem is to allow the sender of the emergency packet to send it to all the available access points. This is similar to broadcasting the packet, but undirected and broadcasted probe requests cannot be prioritized and hence we use directed "modified" probe requests to all available access points. This, of course, assumes that at least one out of the available access points is not a fake or rogue access point. This assumption is reasonable to make, provided there are multiple access points available in the given area. Another way to detect a rogue AP is to use the new wireless security enhancement IEEE 802.11i RSNA (Robust Security Network Association) which uses traditional cryptographic methods to provide strong mutual authentication between wireless clients and the access points. But this method suffers from the fact that the management and verification of digital certificates across multiple platforms and domains is known to be cumbersome. Also, this requires changes to the 802.11i protocol, since for the purpose of the emergency service, there is no actual association of the wireless client with the access point.

Another problem which this service can encounter is a denial-of-service attack. If there are very few access points in an area, the attacker can continuously send emergency packets to the access points and this can deny service to other users. One solution to this problem is that the access point will keep track of the requests from a particular MAC address and will not service another request from the same MAC address until a timeout has passed since the last successful request. This way, the attacker will not be able to cause a denial of service attack of this kind. However, this solution is vulnerable to an attacker who is able to change his MAC address every time before sending the emergency packet.

The system is also susceptible to "prank calls". An attacker can send fake emergency messages and can cause trouble at the PSAP. This problem is analogous to the prank call problem in traditional 911 services. With cellular or PSTN 911 services, the PSAP knows the identity of the attacker since it can determine this based on the cellular or fixed phone line number. With our service, the MAC address similarly provides a unique identifier. While it is possible to spoof source MAC addresses in the 802.11 protocol, it is also possible to spoof caller ID in the PTSN [25]; this ability to spoof the source has not made 911 service unusable on the PTSN, so we expect that the effects will also be tolerable in our system. Because the location information is provided by the AP and not the client, the client is unable to send a fake location.

3. EVALUATION OF THE SERVICE

We evaluate and test our emergency service for correctness and performance. We test correctness by examining the e-mail the PSAP receives. This email should have the correct information about the sender and its approximate location. For evaluating performance, we run several experiments that measure the time taken until the PSAP receives the emergency e-mail from the selected access point under different loads on the access points. We also evaluate how access point prioritization and use of acknowledgment helps in dealing with heavily loaded access points.

We use three laptops as mobile devices and two PCs running Ubuntu Linux 9.04 as access points using the *hostap* program. The three laptops have wireless cards from different manufacturers, namely Intel 5100, Atheros AR5413 and Intel 3945. All the laptops run Ubuntu Linux 9.04. The APs have the Atheros AR5413 chipset. One of the two access points is WPA2 protected with a random password.

We write the daemon processes, as we explain in Section 2, in C. We write the scripts, also explained in Section 2, in Python and using Linux shell commands.

To send an emergency message, we use a specific key sequence `ctrl + E` on one of the mobile devices. We then measure the time duration since pressing the `ctrl + E` key sequence until the emergency e-mail is received by the PSAP. We summarize the time duration measurement under different scenarios in Table 1.

We also verify that out service always selected the access point with the highest signal strength to send the emergency message.

We also perform experiments to show the benefits of increasing the priority of the emergency messages. To implement this, a laptop is continuously sending traffic (802.11 probe requests) to a chosen access point. The other laptop acts as the sender of the emergency requests. Results obtained are shown in Figure 7. The graph depicts the time it takes to receive "x" emergency messages.

Clearly, an increase in the priority of the emergency messages reduces the time required for the message to be serviced.

After running these experiments, we conclude that the acknowledgment of mobile devices' emergency messages by the access point and the prioritizing of emergency packets on the wireless network improve the overall efficiency and speed of the service for practical wireless setups.

We also conduct experiments to measure the time an emergency message takes to be received by the wireless access point after being sent by the mobile device. We use the `gettimeofday` API call to measure the time difference. The times at both the sender and the receiver are synchronised. The results are tabulated in Table 3. The results again show that increasing the priority of the emergency message does help in reducing the time it takes in receiving the message at the access point, and ultimately will reduce the overall time to be received by the PSAP.

We also conduct experiments comparing our emergency service with the Short Message Service (SMS) provided by the mobile operators. Specifically, we use the Google Voice [3] to send SMSs to an AT&T mobile phone. The Google voice uses the Internet to send the short message across to the destination phone number. In our results, the average time an SMS took (we sent a total of 15 SMSs) to be delivered is around 9.8 sec. Our implementation, as seen by the results in Table 1, took 4.3 sec on an average for the case when we, before sending the message, scan the network for selecting the access point and also the network is heavily loaded with traffic.

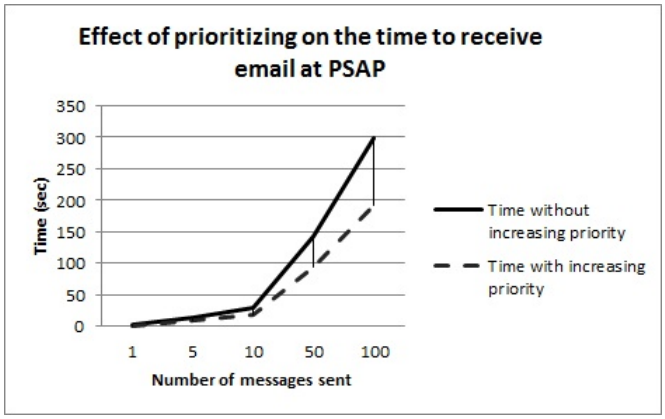

Figure 7: Effect of prioritizing emergency messages on Time to receive e-mail at PSAP

4. RELATED WORK

There have been many research and development works in the past which aim at providing emergency services to users. The first 911 system was installed in Haleyville, Alabama in February 1968 as a way to quickly connect a subscriber to the local police station. This system did not identify the caller but did provide a means to access emergency services that had not previously been available. This system was quickly adapted and improved by other telephone companies resulting in the E911 system which provides both caller location and identification. A pioneering system was in place in Chicago by the mid-1970s, providing both police and fire departments access to the source location of emergency calls. Enhanced 911 is currently deployed in most metropolitan areas in the United States and Canada. In addition, Cellular Enhanced 911 and VOIP enhanced 911 have also been developed to provide the service to the cellular and VOIP users.

In cellular networks, most GSM mobile phones can dial emergency calls even when the phone keyboard is locked, the phone is without a SIM card, or an emergency number is entered instead of the PIN of the SIM card. Our service can be thought as analogous to this service. In our emergency scheme also, a mobile device can send an emergency message across to a PSAP using an available access point even if it is not associated with that AP.

Other systems such as cellular ad-hoc relay for emergencies (CARE) [16] have been proposed that relay an emergency call arising from a user outside the cellular coverage area via another user within the range of the network. There have been existing works that explore the enhancement of the design of 802.11 networks to support data communications in disaster environments, especially for medical uses [13]. In [20], the authors try to develop a wireless infrastructure for emergency purposes in medical care using low-power sensors. A related work [24] uses cognitive radio sensors and dynamic channel assignment to come up with a mobile ad-hoc network for emergency purposes. In [14],

S.No.	Scenario	Time taken	Remarks
1	Sending the message to a preselected AP	1.2 s	AP is not under heavy load
2	Sending the message to a preselected AP	1.8 s	AP is under heavy load, increasing priority of the emergency message
3	Sending the message to a preselected AP	2.4 s	AP is under heavy load, not increasing priority of the emergency message
4	Selecting an AP and then sending the message to an AP	3.8 s	Scanning of AP's take time
5	Selecting an AP and then sending the message to an AP	4.3 s	AP is under heavy load, increasing priority of the emergency message
6	Selecting an AP and then sending the message to an AP	5.1 s	AP is under heavy load, not increasing priority of the emergency message
7	Sending the message to a preselected AP	1.9 s	AP is not under heavy load, testing the AP for internet connectivity ("ping" message)

Table 1: Performance Testing of various cases

S.No.	Scenario	Difference in Timestamps
1	Sending the message to a preselected AP (without n/w traffic)	67.910(ms)
2	Sending the message to a preselected AP (with n/w traffic,) (increasing the priority)	452.613(ms)
3	Sending the message to a preselected AP (with n/w traffic,) (not increasing the priority)	998.184(ms)

Table 2: Time taken to send an emergency message to AP

the authors presents a vehicle-to-vehicle cooperative communication protocol which aims at enhancing traffic safety on busy highways. Another existing work [23] has aimed at developing a portable device that allows telediagnosis and teleconsultation of mobile healthcare providers by expert physicians. The vital bio signals and images are transmitted from the emergency site to the consultation site using the GSM mobile telephony network. Another sensor network based emergency service [26] provides a distributed navigation algorithm for emergency situations.

There exist products such as wireless smoke alarms [1] that operate on RF and require a seperate receiver. Furthermore, there also exist products including Wi-Fi smoke detectors and fire alarms [9] which are wire-free solutions for the traditional smoke and fire alarms. However, these devices must first be associated with an access point for their operation. Our emergency service does not have any such requirement.

All existing systems either require new hardware support like sensor networks or are not utilizing the power and availability of the 802.11 Wi-Fi protocol. Our emergency service, that we build for Wi-Fi networks, does not require any additional hardware support or extensive set up, and would be ubiquitously deployable and easy to use.

5. FUTURE WORK

An emergency service must be robust against common security threats. As we point out in Section 2.6, our emergency service is vulnerable to a denial-of-service attack in which an attacker can keep on sending emergency packets to an access point while also changing the source MAC address. Genuine users cannot obtain the emergency service while this attack is going on. One of our important future goals is to address this security threat. Furthermore, we plan to deal with the problem of rogue or fake access points disrupting the service. We will work towards a solution to this problem along the line of the research done by Jana et al. [15].

Another feature we plan to add to our emergency service is to have a provision for the PSAP to communicate with the sender of the emergency message. This can be done if the AP allows the PSAP to connect to the sender by allowing limited data connectivity for a short duration. The sender is allowed to communicate only with the PSAP and no other network nodes. However, this solution must also address the authentication of the sender and the PSAP. It must also prevent misuse of such a service.

We also plan to develop the same emergency service using the USRP2 which will be capable of sending and receiving IEEE 802.11b/g/n packets. Currently, a full bandwidth receiver for 802.11g is not available. We are working on developing one. Next, we plan to implement the access point functionality on the USRP2 so that a USRP2 can act as a full-fledged access point capable of serving multiple users at the same time. This full-fledged implementation will be helpful in collecting various measurements and benchmarks for the emergency service in Wi-Fi networks under different

traffic and access point usage scenarios.

6. CONCLUSION

Our system enables any user to send an emergency or a distress message at any time without any cost to a Public-Safety Answering Point (PSAP) using any available 802.11 wireless access point or a commercial hotspot having Internet connectivity. The user is not be required to authenticate or associate with the access point. The service is designed such that the emergency message can be given a higher priority than the existing 802.11 packets in the network. Further, the service provides an approximate location of the user to the PSAP. Hence, the service is fully capable of being a full-fledged public emergency service and can be employed in highly populated places having wireless Internet access such as airports, shopping complexes, commercial buildings, etc. Our emergency service requires minimal changes to the existing access points and can be made to work using almost any available wireless NIC cards on PCs, laptops, and mobile phones.

7. ACKNOWLEDGEMENTS

This research was funded in part by National Science Foundation Grant #0520311.

8. REFERENCES

[1] Commercial wireless systems international llc. http://wirelessfirealarm.com/.

[2] Fraunhofer iis autonomous wlan positioning system.

[3] Google voice.

[4] Mexens llc navizon virtual gps service. http://www.navizon.com.

[5] Skyhook, inc. http://www.skyhookwireless.com.

[6] http://en.wikipedia.org/wiki/Wi-Fi.

[7] http://www.fcc.gov/cgb/consumerfacts/wireless911srvc.html.

[8] http://www.fcc.gov/pshs/services/911-services/enhanced911/Welcome.html.

[9] http://www.fireangel.co.uk/Fire-Safety-Products.aspx.

[10] http://www.itu.int/ITU-D/ict/material/FactsFigures2010.pdf.

[11] http://www.wired.com/epicenter/2010/11/fcc-911-texting/.

[12] Spectralink inc.: Şspectralink voice priorityŤ http://www.spectralink.com/files/literature/svp white paper.pdf.

[13] Arisoylu M, Mishra R, R. R. L. L. 802.11 wireless infrastructure to enhance medical response to disasters.

[14] Biswas, S., Tatchikou, R., and Dion, F. Vehicle-to-vehicle wireless communication protocols for enhancing highway traffic safety. *Communications Magazine, IEEE 44*, 1 (2006), 74 – 82.

[15] Jana, S., and Kasera, S. K. On fast and accurate detection of unauthorized wireless access points using clock skews.

[16] Janefalkar, A., Josiam, K., and Rajan, D. Cellular ad-hoc relay for emergencies (care). In *Vehicular Technology Conference, 2004. VTC2004-Fall. 2004 IEEE 60th* (2004), vol. 4, pp. 2873 – 2877 Vol. 4.

[17] Kim, J. Y., Song, W., and Schulzrinne, H. Kim et al. an enhanced voip emergency services prototype an enhanced voip emergency services prototype abstract.

[18] Lichter; Joseph James (Naperville, IL), M. M. J. Y. I. M. T. L. I. Enhanced emergency service for isdn based emergency services in a wireless telecommunications system, 07 2001.

[19] Lorincz, K., Malan, D., Fulford-Jones, T., Nawoj, A., Clavel, A., Shnayder, V., Mainland, G., Welsh, M., and Moulton, S. Sensor networks for emergency response: challenges and opportunities. *Pervasive Computing, IEEE 3*, 4 (2004), 16 – 23.

[20] Malan, D., Fulford-jones, T., Welsh, M., and Moulton, S. Codeblue: An ad hoc sensor network infrastructure for emergency medical care. In *In International Workshop on Wearable and Implantable Body Sensor Networks* (2004).

[21] Mintz-Habib, M.; Rawat, A. S., and H., Wu, X. A voip emergency services architecture and prototype. *Computer Communications and Networks, 2005. ICCCN 2005. Proceedings. 14th International Conference* (2005), 523–528.

[22] Oran; David R. (Acton, MA), G. S. S. J. C. System for discovering and maintaining geographic location information in a computer network to enable emergency services, 03 2007.

[23] Pavlopoulos, S., Kyriacou, E., Berler, A., Dembeyiotis, S., and Koutsouris, D. A novel emergency telemedicine system based on wireless communication technology-ambulance. *Information Technology in Biomedicine, IEEE Transactions on 2*, 4 (1998), 261 –267.

[24] Pawelczak, P., Venkatesha Prasad, R., Xia, L., and Niemegeers, I. Cognitive radio emergency networks - requirements and design. In *New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005. 2005 First IEEE International Symposium on* (2005), pp. 601 –606.

[25] Telespoof.com. Telespoof.com - Caller ID Spoofing Service. http://www.telespoof.com/.

[26] Tseng, Y.-C., Pan, M.-S., and Tsai, Y.-Y. Wireless sensor networks for emergency navigation. *Computer 39*, 7 (2006), 55 –62.

[27] Zellner; Samuel N. (Dunwoody, GA), E. M. J. R. G. M. J. R. T. A. G. Multimedia emergency services, 11 2009.