September 19, 2018

WIRELESS EMERGENCY PROBE MESSAGE

David White

Kevin Klous

Magnus Mortensen

Jay Johnston

WIRELESS EMERGENCY PROBE MESSAGE

AUTHORS:
David White
Kevin Klous
Magnus Mortensen
Jay Johnston

ABSTRACT

The techniques described herein leverage The Institute of Electrical and Electronics Engineers (IEEE) 802.11ax probe request messages to encode an Emergency Beacon (Request for Help) within the initial non-Access-Point (AP) station's (client's) probe request packets which would notify the AP that a client is in distress and to notify Emergency Services (via text-to-911 and provide e911 location information). This new capability allows any 802.11ax AP to receive emergency beacons, regardless of how "closed" the networks are on that AP, thereby allowing any wireless client the ability to reach out for help and allowing the AP to relay that information onward towards emergency services.

DETAILED DESCRIPTION

Today, most wireless networks are "closed", whereby passersby are unable to use the network. This is logical, as corporations want to restrict access to their networks to their employees, which may only allow trusted devices and/or corporate devices onto their private network. Other corporations have dedicated networks for "guests" which are also often secured as companies have to pay for the Internet service and they want a way of policing access (although loosely with SSID pre-shared keys, which they may rotate).

So, even though IEEE 802.11 wireless is almost ubiquitous in a city, it is largely a series of overlapping walled gardens that are inaccessible to those within reach who have an emergency.

Assume a person (or even a thing) is having an emergency; today the main action is for them to yell "help". Anyone within earshot takes notice and acts. However, if no

one is around, their notification is unheard. It would be ideal if they could also leverage any of their devices to send out an SOS emergency beacon that could be picked up by any IEEE 802.11 wireless network (secured or not) and forwarded to the e911 provider for the area. Thereby extending emergency alerting to any wireless network. Although a lot of people have cellular devices, not all do, and not at all times. Therefore, this capability is a very valuable and necessary fundamental extension to wireless networks.

Currently, the IEEE 802.11ax specification provides for a way for an unauthenticated user to connect to a service set identifier (SSID) in order to establish an emergency voice call to a pre-configured emergency service. However, that approach has problems and uses a different method to accomplish its goal than the techniques described herein. Additionally, that approach does not provide a way to allow a text-type notification to emergency services. As a result, it puts the onus on the endpoint to be able to establish a call and to communicate via voice to a human operator. Thus, IEEE 802.11ax merely creates an audio-only communication pathway.

The techniques presented herein leverage IEEE 802.11ax probe request messages to encode an Emergency Beacon (Request for Help) within the initial non-AP station's (*i.e.*, client's) probe request packets which would notify the AP that a client is in distress and to notify Emergency Services (via text-to-911 and provide e911 location information).

Currently, the IEEE 802.11ax specification provides for a way for an unauthenticated user to connect to an SSID in order to establish an emergency call to a pre-configured emergency service, as described above. However, it does not provide a way to allow a text-type notification to emergency services, nor does the AP or controller participate in the emergency notification. Thus, IEEE 802.11ax merely creates an audio-only communication pathway.

According to the techniques described herein, we assume the endpoint is dumb, or that the individual (or Internet-of-Things (IoT) device) is incapable of verbal communication. In these cases, the ability to be able to "signal" a request for help is critical. An AP, upon receiving this signal will forward the message to its pre-configured local emergency contact center. Often this is a text-to-911 message to an e911 center to indicate a request for emergency assistance, and the location of that request. That

location is either relayed based on the GPS coordinates that the client sent in, or if they are missing, they are replaced with the coordinates estimated by the AP (leveraging location services), or they are the coordinates of the AP itself (indicating that the requestor is within a 100m radius of those coordinates).

802.11 Probe Request Frame Structure

The current frame structure of the Probe Request frame is depicted in Figure 1 below.

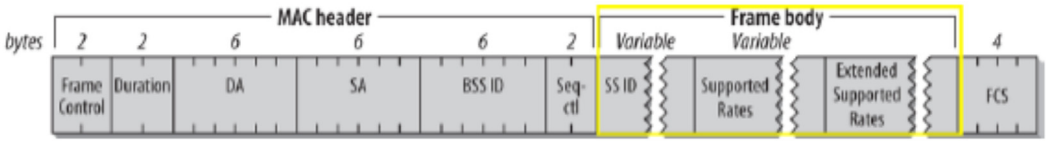

Figure 1

The frame body portion of the request frame contains various types of information depending on the needs and capabilities of the station (STA). Table 1 below illustrates the Probe Request frame body (IEEE 802.11-2016), with the Proposed Extensions according to the techniques described herein to the Probe Request frame body shown in bold/italics.

Order	Information	Notes
19	Extended Request	The Extended Request element is optionally present if dot11RadioMeasurementActivated is true.
20	***Emergency Beacon***	***The element is optionally present. This field is used to describe that the station (STA) is under distress. Data values include the GPS coordinate values of the STA (if available). If not possible, the STA may estimate the STA coordinates based on location services or use its own coordinates as a fallback mechanism. Additionally, type of help needed (Police, Fire, Ambulance) may be optionally indicated in the request***.
Last	Vendor Specific	One or more vendor-specific elements are optionally present. These elements follow all other elements

Table 1

Figure 2 below illustrates a Probe Request Emergency Beacon Flow Diagram according to the techniques described herein.

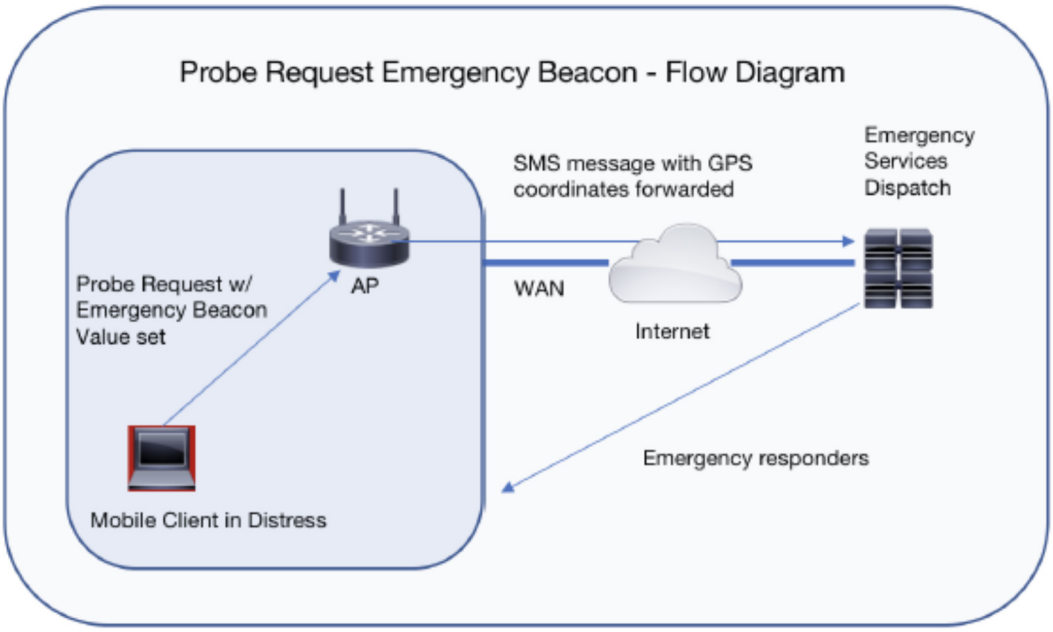

Figure 2

Upon receiving a text-to-911 message, the local Emergency Response Center would process it as any other text message they receive requesting assistance. The only difference is that the text message would indicate that it is a forwarded request based on a real distress call, but bi-directional communication is not possible.

Example Use Case

A user is out for a run and wearing a fitness tracker. Suddenly, the user has chest pains and falls to the ground. The user is wearing a wearable device, which is capable of IEEE 802.11 communication, but does not have cell phone connectivity. The user presses and holds a button on the wearable device, which actives the Emergency beacon. The wearable device searches for any wireless network and sends out the Emergency Beacon. The AP/Controller receiving the beacon then transmits a message to the SMS service which sends out the text-to-911 message. Included in the text-to-911 message are the GPS coordinates of the user in distress and a request for an Ambulance. The 911 center dispatches emergency services to the runner in distress.