Atoca WG
Internet Draft
Intended Status: Informational
Expires: April 30, 2012

Gabor Bajko
Nokia
October 31, 2011

Emergency Alert Service support in IEEE 802.11 networks
draft-bajko-atoca-wlan-eas-01

Abstract

The IEEE 802.11 specification is evolving by defining new amendments to it, which are then rolled into the base spec. The 802.11u amendment, published in November 2010, contains support for Citizen to Authority type of Emergency Calls and Authority to Citizen type of Alerts.
This document attempts to explain what level of support for Authority to Citizen type of Emergency Alerts has been defined for IEEE 802.11 protocol.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on April 30, 2012.

Table of Content

1. Introduction

This document assumes the reader is familiar with the basics of the 802.11 protocol.
A STA first listens in a channel to see if there are any APs operating in that channel. If there are, then the STA will receive a beacon. This is the so-called passive scanning procedure. The STA may also choose to send a Probe Request in the channel and wait for a Probe Response. The Probe Request is sent to a broadcast address and contains conditions which an answering AP must satisfy. This is called active scanning.
A STA can only exchange data frames with an AP after the so-called association and authentication (if required) procedure. Management frames however, can be exchanged even before the association and authentication procedure, which the 802.11 specification calls pre-association frame exchange.

2. Conventions and Terminology

2.1 Conventions used in This Document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC-2119 [1].

2.2 Terminology

STA station, a device communicating with an 802.11 access point
GAS Generic Advertisement Service Protocol, defined in 802.11

3. Emergency Alert Service indication at a wifi AP

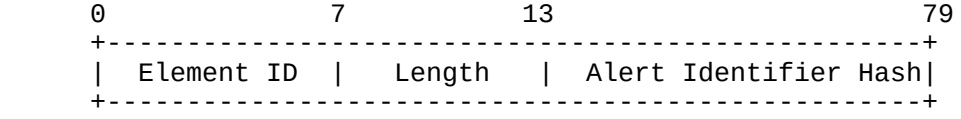
An AP compliant with the IEEE 802.11-2011 specification will have a MIB variable called dot11EASActivated which has the following definition:

```
dot11EASActivated OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-write
STATUS current
DESCRIPTION
"This is a control variable.
It is written by an external management entity or the SME. Changes
take effect as soon as practical in the implementation. This
attribute when true, indicates the STA is capable of supporting
emergency alert system. The capability is disabled otherwise. "
DEFVAL {false}
::= { dot11StationConfigEntry 128 }
```

When this MIB variable is set to TRUE, then the AP supports this feature. Else the AP does not support this feature.

When this MIB variable is set to true and there are emergency alert messages in the network, then the beacon will contain one Emergency Alert Information Element for each active alert message, in the beacon. These Emergency Alert Information Elements have to also be included in the Probe Response Frames, when a STA asks for it in a Probe Request Frame.

The Emergency Alert Identifier element provides a hash to identify instances of the active EAS messages that are currently available from the network. The hash allows the STA to assess whether an EAS message advertised by an AP has been previously received and therefore whether it is necessary to download from the network. The format of the Emergency Alert Identifier element is:



The Length is a 1-octet field whose value is equal to 8.
The Alert Identifier Hash (AIH) is an 8-octet field. It is a unique value used to indicate an instance of an EAS message. The value of this field is the hash produced by the HMAC-SHA1-64 hash algorithm operating on the EAS message.

AIH =HMAC-SHA1-64("ES_ALERT", Emergency_Alert_Message)

where AIH is then truncated to the first 64 bits of this function. The Emergency_Alert_Message is the EAS message itself.

NOTE: The same value of hash will be computed by each AP in an ESS and by each AP in different ESSs. Thus a STA, which can download emergency alert messages when in a pre-associated state, can unambiguously determine that it has already downloaded the message, avoiding unnecessary duplicates.

4. Retrieving an EAS message

The STA can find out whether there are any EAS messages in the network by looking for Emergency Alert Information Elements in the beacon or Probe Response messages.

When the STA finds out that there are EAS messages in the network, it can access those messages with the protocol defined in 802.11-2011.

The STA can check if it had previously downloaded that alert message by computing a hash of the message and comparing it with the hash

value present in the Emergency Alert Information Element of the beacon or probe response frame.

The STA does not have to be associated with an AP in order to access and download the EAS message, it can do that in the pre-associated state as well. The STA needs to send a GAS Request public action frame to the AP by setting the Element-ID of the request to the EAS value and including the hash of the EAS message into the Query Request field. Then, in the GAS Response frame, the AP will deliver the requested EAS message to the STA.
According to the 802.11 specifications, the EAS message in the GAS Response frame is expected to be formatted in accordance with OASIS EDXL.

A STA which is already associated and authenticated with an AP, can also use GAS ANQP protocol to download the URI of a local Emergency Alert Server. The STA can then retrieve the EAS message using a URI formed by concatenating the downloaded local Emergency Alert Server URI with the hexadecimal numerals of the Alert Identifier Hash converted to UTF-8 encoded characters and the ".xml" file extension. For example, if the Emergency Alert Server URI is http://eas.server.org and the Alert Identifier Hash is "0x1234567890abcdef", then the URI would be http://eas.server.org/1234567890abcdef.xml
The XML file is expected to be formatted in accordance with OASIS EDXL.

The mechanism by which the EAS message is retrieved from the formed URI is not specified in the 802.11 specification.

When an EAS Message has expired, an AP with dot11EASActivated set to TRUE shall remove the corresponding instance of an Emergency Alert Identifier element from its Beacon and Probe Response frames.

5. Protocol considerations

An Emergency Alert distribution protocol intended to work with WiFi Access Points will need to deliver the Alert message to the AP, which in turn will need to save it in a MIB variable. Currently there are no MIB variables defined in the 802.11 standard to store Alert messages.
Once the AP, which has EAS implemented and enabled, receives an Alert message, it needs to include an Emergency Alert Information Element into the beacon and probe responses, and remove it once the Alert message expires.
The AP would probably need to register itself to an Alert Distribution Server in order to receive the Alerts.

6. IANA considerations

None.

7. Security considerations

This document is provided for information to the IETF community. The protocol described here relies on the existence of a protocol which can distribute emergency alert messages to the wifi access points. As described here, the STAs can access an alert message in pre-associated state as well, when the STA did not authenticate the AP or the network behind the AP. Careful consideration should be taken on when such an alert message can be trusted and be displayed on the screen of a wifi device.

8. Normative References

9. Informative References

http://standards.ieee.org/getieee802/download/802.11-2007.pdf
http://standards.ieee.org/getieee802/download/802.11-2011.pdf (to be available in 2012)

10. Author’s Addresses

Gabor Bajko
gabor.bajko@nokia.com