IEEE P802.11
Wireless LANs

|  |
| --- |
| SFD Proposal |
| Date: 2019-08-13 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Hitoshi Morioka | SRC Software | Fukuoka, JAPAN |  | hmorioka@src-soft.com |
|  |  |  |  |  |

Abstract

This document describes a frame authentication SFD proposal based on 11-19/451r3.

# Introduction

As described in 11-19/451r3, the proposed frame authentication mechanism uses 2 types of frame, one is “eBCS Info frame” and the other is “eBCS Data frame”.

The eBCS Info frame derivers information that is required to authenticate eBCS Data frames.

The eBCS Data frame derivers data that contains the contents to be consumed by eBCS receivers.

The frame sequence is shown in Fig. 1.



Fig. 1: Frame sequence

The eBCS Info frames are transmitted in a fixed interval *TI*. Each eBCS Info frame has a sequence number that is incremented.

A series of TESLA keys are generated at the time of generating each eBCS Info frame. The TESLA key is identified by the eBCS Info frame sequence number and the index of the series of TESLA keys as *Ks,i*.

The eBCS Info frame should be Public Action frame.

The eBCS Data frame can be either Data frame or Public Action frame. The restrictions of the both frame types are almost same in the current standard. From the point of view of the implementation difficulty, this proposal uses Public Action frame for the eBCS Data frame.

The following SFD proposal implements this frame authentication mechanism based on Draft P802.11REVmd D2.0.

# SFD Proposal

**3. Definitions**

**3.2 Definitions specific to IEEE Std 802.11**

**Enhanced Broadcast Service (eBCS) receiver:** An STA that receives Enhanced Broadcast (eBCS) frames.

**Enhanced Broadcast Service (eBCS) transmitter:** An STA that transmits Enhanced Broadcast (eBCS) frames.

6. Layer management

6.3 MLME SAP interface

**6.3.<ANA1> eBCS Info transmission**

*Describe MLME SAP for eBCS Info frame transmission.*

6.3.<ANA2> eBCS Info reception

*Describe MLME SAP for eBCS Info frame reception.*

**6.3.<ANA3> eBCS Data transmission**

*Describe MLME SAP for eBCS Data frame transmission.*

6.3.<ANA4> eBCS Data reception

*Describe MLME SAP for eBCS Data frame reception.*

9. Frame formats

9.6 Action frame format details

9.6.7 Public Action details

9.6.7.1 Public Action frames

*Add eBCS Info and eBCS Data to Table 9-362.*

9.6.7.<ANA5> eBCS Info frame format

*Describe eBCS Info frame format that contains:*

* *eBCS Info sequence number*
* *eBCS transmitter’s certificate signed by CA*
* *Timestamp*
* *Authentication algorithm identifier*
* *eBCS Info transmittion interval*
* *Contents information*
	+ *Human readable title*
	+ *Higher layer protocol type*
	+ *Destination IP address and UDP port (if UDP/IP)*
* *TESLA key change interval (if TESLA is used)*
* *TESLA key disclosure delay (if TESLA is used)*
* *TESLA initial key of this sequence (if TESLA is used)*
* *TESLA disclosed key of the last sequence (if TESLA is used)*
* *Signature for this eBCS Info frame signed by the eBCS transmitter’s private key*
* *Contents data (if data is small enough and public key authentication is used)*

9.6.7.<ANA6> eBCS Data frame format

*Describe eBCS Data frame format that contains:*

* *eBCS Info sequence number*
* *Higher layer protocol information*
	+ *Higher layer protocol type*
	+ *Source/Destination IP address and UDP port (if UDP/IP)*
* *TESLA key index for the authenticator (if TESLA is used)*
* *TESLA key index for the disclosed key (if TESLA is used)*
* *TESLA key to be disclosed (if TESLA is used)*
* *Authenticator (for TESLA) or Signature (for public key)*
* *Contents data*

10. MAC sublayer functional description

10.6 Multirate support

10.6.5 Rate selection for Data and Management frame

10.6.5.<ANA7> Rate selection for eBCS frames

*Describe rate selction procedure for eBCS Info/Data frames that enables to select any available rate.*

11. MLME

11.<ANA8> Enhanced Broadcast Service (eBCS) procedures

11.<ANA8>.<ANA9> eBCS Info frame generation and usage

11.<ANA8>.<ANA9>.1 eBCS Info frame transmittion

*Describe eBCS Info frame transmission procedure.*

11.<ANA8>.<ANA9>.2 eBCS Info frame reception

*Descrive eBCS Info frame reciption procedure.*

11.<ANA8>.<ANA10> eBCS Data frame generation and usage

11.<ANA8>.<ANA10>.1 eBCS Data frame transmission

*Describe eBCS Data frame transmission procedure.*

11.<ANA8>.<ANA10>.2 eBCS Data frame reception

*Descrive eBCS Data frame reciption procedure.*

12. Security

12.<ANA11> Frame authentication for eBCS

12.<ANA11>.1 General

*Describe abstract of the eBCS frame authentication mechanism that contains:*

* *eBCS public key frame authentication that uses only public key algorithm*
* *eBCS TESLA-public key frame authentication that uses combination of TESLA and public key algorithm*

12.<ANA11>.2 eBCS public key frame authentication

*Describe eBCS public key authentication procedure.*

12.<ANA11>.3 eBCS TESLA-public key frame authentication

*Describe eBCS TESLA-public key frame authentication procedure.*

Annex B

B.4 PICS proforma-IEEE Std 802.11-20xx

B.4.3 IUT configuration

*Add description for eBCS transmitter and receiver support*

B.4.<ANA12> eBCS features

*Describe table that contains:*

* *eBCS Info frame transmission*
* *eBCS Info frame reception*
* *eBCS Data frame transmission*
* *eBCS Data frame reception*
* *eBCS public key frame authentication*
* *eBCS TESLA-public key frame authentication*

Annex C

C.3 MIB details

*Add the following line to “dot11smt”.*

-- dot11eBCSConfigTable ::= { dot11smt <ANA13> }

*Add the following lines to appropriate place.*

-- \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

-- \* dot11eBCSConfigTable TABLE

-- \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

dot11eBCSConfigTable OBJECT-TYPE

 SYNTAX SEQUENCE OF Dot11eBCSConfigEntry

 MAX-ACCESS not-accesible

 STATUS current

 DESCRIPTION

 “The table contains enhanced broadcast service configuration objects.”

 ::= { dot11smt <ANA13> }

*Describe “Dot11eBCSConfigEntry” according to the amendment.*