**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |  |
| --- | --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) | |
| Title | **Changes to Annex E (Dragonfly)** | |
| Date Submitted | 5 March 2015 | |
| Source | [] [] [address] | Voice: [ ] Fax: [ ] E-mail: [ ] |
| Re: | [If this is a proposed revision, cite the original document.]  [If this is a response to a Call for Contributions, cite the name and date of the Call for Contributions to which this document responds, as well as the relevant item number in the Call for Contributions.]  [Note: Contributions that are not responsive to this section of the template, and contributions which do not address the topic under which they are submitted, may be refused or consigned to the “General Contributions” area.] | |
| Abstract | [Description of document contents.] | |
| Purpose | [Description of what the author wants P802.15 to do with the information in the document.] | |
| Notice | This document has been prepared to assist the IEEE P802.15. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein. | |
| Release | The contributor acknowledges and accepts that this contribution becomes the property of IEEE and may be made publicly available by P802.15. | |

***Insert new sections E.1.1 and E.1.2, including sub-sections***

**E.1.1 Device Authentication**

Dragonfly is a true peer-to-peer protocol where either side can initiate and both sides can initiate simultaneously (the higher layer on each device believes it initiated the KMP). Therefore there is no Access Point (AP) required. Each device can be treated as an equal peer. Inclusion of an AP is seamless because one side (a station) can always initiate to the other (an AP).

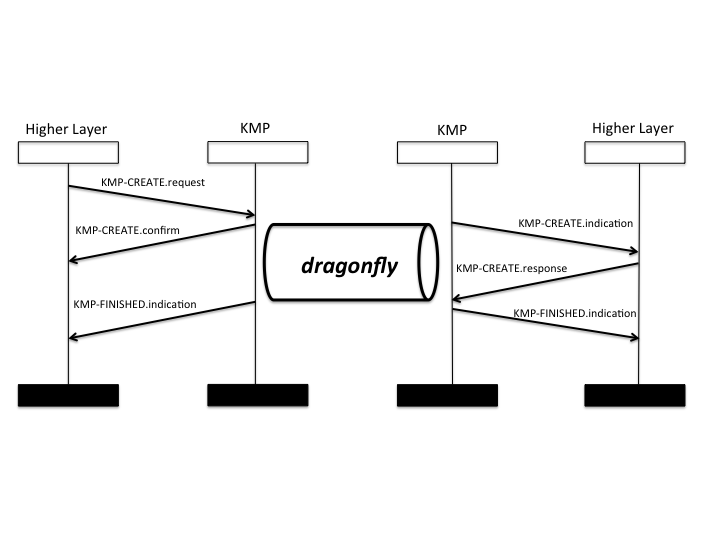
The credential used with dragonfly is always a pairwise, shared, and symmetric key, code, word, or phrase and it is identified by the MAC address of the IEEE 802.15 peer.

**E.1.2 Device Authentication and Cryptographic Key Establishment**

Device authentication does not provide for protection of frames between WPAN devices themselves. Instead, it protects its own frames and performs an authenticated key establishment protocol to establish state, including cryptographic keys, that are suitable for use with IEEE 802.15 standard ciphers (e.g. CCM\*) to protect frames sent between WPAN devices.

When used with IEEE 802.15, dragonfly the state machine and protocol definition for SAE (dragonfly in IEEE 802.11) from IEEE Std 802.11-2012 and uses frames whose format is defined in section E.3.3 (Message framing).

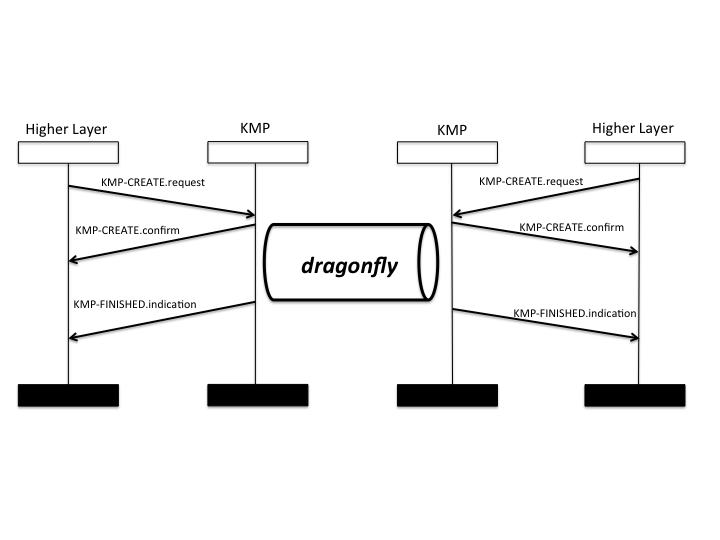
**E.1.2.1 Dragonfly Authentication in Client/Initiator to Server/Responder Mode**

When one device initiates Dragonfly to another device which is in a quiescent state, the Dragonfly KMP is used in client/server (aka initiator/responder) mode. In this mode new key exchange is created by a KMP-CREATE.request from the higher layer. The receipt of a Dragonfly message (EAP-pwd-Commit) at a peer device on which the Dragonfly KMP has not already been created will generate a KMP-CREATE.indication to the higher layer. When Dragonfly has completed the KMP will issue KMP-FINISHED.indication messages to the higher layer. This is shown in figure TBD-1.

**Figure TBD-1 --- Initiator/Responder Mode of Dragonfly KMP**

**E.1.2.2 Dragonfly Authentication in Peer-to-Peer Mode**

When both devices simultaneously initiate Dragonfly to each other, the Dragonfly KMP is used in peer-to-peer mode. In this mode each higher layer views itself as the “initiator” of the protocol and the key exchange is created on each side by a KMP-CREATE.request. Receipt of a Dragonfly message (EAP-pwd-Commit) at a peer that has already created a Dragonfly KMP instance will not generate a KMP-CREATE.indication. Instead the protocol will advance as dictated by the state machine. When Dragonfly has completed, the KMP will issue KMP-FINISHED.indication messages to the higher layer. This is shown in figure TBD-2.



**Figure TBD-2—Dragonfly KMP in Peer-to-Peer mode**

***Change existing E.3.3 to E.3.4 and replace current E.3 to E.3.2 with the following:***

**E.3 Dragonfly and 802.15 Specifics**

The Dragonfly key exchange is transport agnostic and will run over any medium that can encapsulate its messages, including KMP Information Elements.

**E.3.1 Algorithm Negotiation**

Dragonfly requires the negotiation of a domain parameter set in which to perform public key cryptography, referred to as a “group” and negotiation of a random function. The random function is used to provide security to the Dragonfly exchange and also as a base on which to build a key derivation function (KDF).

The group and random function are encoded, as integers, into the first Dragonfly message exchanged. The group is based on a registry maintained by IANA for IKE (RFC 2409). This registry maps a 16-bit number into a complete domain parameter set. This registry contains domain parameter sets for secure groups based on Finite Field Cryptography (FFC) as well as Elliptic Curve Cryptography (ECC). Dragonfly can use either. The random function can be either inferred from the selected group or specified directly (see E.3.3.1).

**E.3.2 Key Derivation**

The random function that is negotiated is used to create a key derivation function. Any key derivation function can be used but it is recommended that a hash algorithm be used for a random function and that the KDF be based on RFC 5869.

**E.3.3 Message Framing**

Dragonfly KMP messages are distinct payloads, each identifying a message exchange inside the Dragonfly protocol, the *Commit* exchange and the *Confirm* Exchange. When carried in a KMP Information Element, the payload follows the KMP ID value in the first KMP Fragment.

**E.3.3.1 Dragonfly Commit message**

The Dragonfly Commit message is the following format:

0 1 2 3

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Group Description | RESERVED | KMP Registry |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| |

~ Element ~

| |

~ +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| | |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ ~

| |

~ Scalar +-+-+-+-+-+-+-+-+

| |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

Where “Group Description” is an index into IKE’s (RFC 2409) IANA-maintained group registry, “RESERVED” are always set to zero upon transmission and ignored upon receipt, and “KMP Registry” indicates the following to use as random function (for both H() and CN() in IEEE Std 802.11-2012) as well as a KDF:

0: Use group

1: HMAC-SHA-256

2-255: Reserved for 802.16 assignment

When “KMP Registry” is “Use Group” the random function shall be based on the size of the prime, p, that defines the group identified by “Group Description” according to the following:

HMAC-SHA-256: len(p) <= 256

HMAC-SHA-384: 256 < len(p) <= 384

HMAC-SHA-512: len(p) > 384

The scalar and element in the Dragonfly Commit message are encoded according to the rules in section 11.3.7.2.4 (Element to Octet string conversion) and their lengths can be inferred by the chosen group.

**E.3.3.2 Dragonfly Confirm message**

The Dragonfly Confirm message is the following format:

0 1 2 3

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| |

~ Confirm ~

| |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

The length of the Confirm field depends on the random function chosen.