**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |
| --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) |
| Title | MAC security for IEEE 802.15.8 PAC |
| Date Submitted | March 10, 2015 |
| Source | Woongsoo NaSungrae Cho[Chung-Ang University, Korea] | E-mail:[wsna@uclab.re.kr]E-mail:[srcho@cau.ac.kr] |
| Re: | This is the original document |
| Abstract | MAC security for IEEE 802.15.8 PAC |
| Purpose | To introduce proposed MAC security for PAC |
| 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. |

Table of Contents

[1. Overview 3](#_Toc413783839)

[2. Definitions 3](#_Toc413783840)

[3. Abbreviations and acronyms 3](#_Toc413783841)

[4. General descriptions 3](#_Toc413783842)

[4.1. Concepts and architecture 3](#_Toc413783843)

[4.2. Topology 3](#_Toc413783844)

[4.3. Reference model 3](#_Toc413783845)

[5. MAC layer 3](#_Toc413783846)

[5.1. MPDU structure 3](#_Toc413783847)

[5.2. Multiple access 3](#_Toc413783848)

[5.3. Synchronization procedure 3](#_Toc413783849)

[5.4. Discovery procedure 3](#_Toc413783850)

[5.5. Peering procedure 3](#_Toc413783851)

[5.6. Scheduling 3](#_Toc413783852)

[5.7. QoS 3](#_Toc413783853)

[5.8. Interference management 3](#_Toc413783854)

[5.9. Transmit power control 4](#_Toc413783855)

[5.10. Multicast 4](#_Toc413783856)

[5.11. Broadcast 4](#_Toc413783857)

[5.12. Multi-hop operation 4](#_Toc413783858)

[5.13. Relative positioning 4](#_Toc413783859)

[5.14. Power management 4](#_Toc413783860)

[5.15. Security 4](#_Toc413783861)

[5.15.1 Security modes 4](#_Toc413783862)

[5.16. Coexistence 12](#_Toc413783863)

[5.17. Higher layer interaction 12](#_Toc413783864)

# Overview

The 802.15.8 specification shall be developed according to the P802.15.8 Peer Aware Communication (PAC) project authorization request (PAR), document number 15-12-0063r2 and Five Criteria (5c), document number 15-12-0064r1, which were approved by the IEEE-SA in March of 2012.

# Definitions

# Abbreviations and acronyms

PD PAC Device

FFPD A PD which supports whole specification including routing table and it is always relay-enabled.

RFPD It has two types. These are relay-enabled PD and relay-disabled PD. Relay-enabled is a reduced-function PD which supports routing table for specific multicast group and relay-disabled is a reduced-function PD which does not support routing table.

# General descriptions

This clause provides the basic framework of PDs. The framework serves as a guideline in developing the functionalities of PDs and their interactions specified in detail in the subsequent clauses.

## Concepts and architecture

## Topology

## Reference model

# MAC layer

## MPDU structure

## Multiple access

## Synchronization procedure

## Discovery procedure

## Peering procedure

## Scheduling

## QoS

## Interference management

## Transmit power control

## Multicast

## Broadcast

## Multi-hop operation

## Relative positioning

## Power management

## Security

Security layer provides users with privacy, authentication, and authorization across the network.

### 5.15.1 Security modes

PAC security layer provides three different security modes on the basis of security requirements of network connections.

*5.15.1.1 Security mode 1 (non-secure)*

When a PAC device is in security mode 1, it shall never initiate any security procedure.

*5.15.1.2 Security mode 2 (service level enforced security)*

When a PAC device is in security mode 2, it shall initiate security procedures after a channel establishment request has been received or a channel establishment procedure has been initiated by itself. Whether a security procedure is initiated or not depends on the security requirements of the requested channel of service.

A PAC device in security mode 2 should classify the security requirements of its services using the following attributes.

|  |  |
| --- | --- |
| Security requirement | Description |
| Authentication required | - Before connecting to the application, the remote device must be authenticated |
| Authorization required | - Access is only granted automatically to trusted PAC devices, or untrusted devices after an authorization procedure- Always requires authentication to verify that the device is the right one |
| Encryption required | - The link must be changed to encrypted mode, before access to the service is possible |

Security mode 1 can be considered as a special case of security mode 2 where o service has registered any security requirements.

*5.15.1.3 Security mode 3 (link level enforced security)*

When a PAC device is in security mode 3, it shall initiate security procedures before the channel is established.

5.15.2 Security parameters

PAC security layer uses the following security parameters.

|  |  |
| --- | --- |
| Parameters | Description |
| PAC\_ADDR | PAC device address (unique for each device) |
| AUTH\_KEY | Authentication key used for authentication purposes |
| ENC\_KEY | Encryption key for secure unicast |
| GENC\_KEY | Group encryption key for secure group communication |
| RAND | Frequently changing random or pseudo-random number |

5.15.3 Key Derivation

For secure communications between PAC devices in networks, several key materials are derived using the shared secret information between the devices.

Following figure shows the key derivation procedure between devices using PIN secretly shared during the peering phase.



Figure 19. Key derivation

Each key material shall be derived selectively on the basis of the security mode. For example, when a PAC device is in security mode 1, it shall never initiate any security procedure. When a PAC device is in security mode 3, it shall derive all of the above key materials, such as AUTH\_KEY and ENC\_KEY between the devices.

5.15.4 Authentication

Authentication is the process of verifying ‘who’ is at the other end of the link. In PAC security layer, authentication is performed for devices, or services.

Technically, authentication is achieved based on the stored authentication key (AUTH\_KEY) or by peering (entering a PIN).

Flowchart for authentication is shown as a follow.



Figure 20. Flowchart for authentication

*5.15.4.1 Infrastructureless authentication*

In PAC networks where there is no coordinator or AAA(Authentication, authorization, accountability) server, authentication between PAC devices are done using PIN, or certificate issued by the trusted authority.



Figure 21. Infrastructureless architecture

*5.15.4.1.1 One-way authentication procedure*

Some applications might require only one-way authentication. Following figure shows the one-way authentication procedure between PAC devices A (verifier) and B (claimant).



Figure 22. One-way authentication

When a verifier A requires to authenticate B, (1) A sends a random number A.RAND to B, (2) A and B computes a secret information SRES’ and SRES, respectively, using pseudo-random function(PRF) on inputs of A’s random number (A.RAND), PAC address of B (B.PAC\_ADDR), and authentication key shared between them (AUTH\_KEY), (3) B sends SRES, (4) A checks if SRES is equal to SRES’. If they match, authentication succeeds; if not, authentication fails.

*5.15.4.1.2 Mutual authentication procedure*

Some applications might require mutual authentication. Following figure shows the mutual authentication procedure between PAC devices A and B.

Figure 23. Mutual authentication procedure



Figure 3 Mutual authentication

When PAC devices A and B authenticate each other, (1) A sends its address (A.PAC\_ADDR) with a random number (A.RAND) to B, (2) B also sends its address (B.PAC\_ADDR) with a random number (B.RAND) to A, (3) A and B optionally computes encryption key (ENC\_KEY) on the input of all of the previously exchanged information and AUTH\_KEY. Then, they shall verify each other when they communicate using a secure channel protected by the shared ENC\_KEY.

*5.15.4.2 Infrastructure authentication*

In PAC networks where there is an AAA(Authentication, authorization, accountability) server and a dynamic coordinator, which is a PAC device with intermittent connection to the AAA server, authentication between PAC devices are done using symmetric master key, or certificate issued by the AAA server



Figure 24. Infrastructure architecture

When a PAC device A and B (coordinator) authenticate each other, the mutual authentication procedure shall progress as a following figure.



Figure 25. Infrastructure authentication

The authentication procedure consists of EAP authentication between a PAC device A and an AAA server, authentication key generation and 3-way handshake between PAC device A and B, and encryption key/group key delivery process.

*5.15.4.2 .1EAP authentication*

EAP (Extensible authentication protocol) authentication uses Extensible Authentication Protocol [IETF RFC 3748] in conjunction with an operator-selected EAP Method (e.g. EAP-TLS [IETF RFC 2716]). The EAP method will use a particular kind of credential – such as an X.509 certificate in the case of EAP-TLS, or a Subscriber Identity Module in the case of EAP-SIM.

The particular credentials and EAP methods that are to be used are outside of the scope of this specification. However, the EAP method selected should fulfill the following mandatory criteria listed in section 2.2 of RFC 4017: (1) mutual authentication, (2) protection against the man-in-the-middle attack. Use of an EAP method not meeting these criteria may lead to security vulnerabilities.

In the PAC authentication procedure, EAP yields the512-bit master secret key (MSK), which is delivered to a PAC device A by an AAA server.

Then the other key encryption keys (KEK) and HMAC/CMAC keys are derived from the MSK

*5.15.4.2.2 Authentication key generation*

After EAP authentication, the PAC device A and AAA server generate PMK using a truncation function as a follow.

*PMK = Truncate(MSK, 160)*

Then, the AAA server sends PMK to the coordinator B securely. On receipt of it, the coordinator B and the PAC device A generate authentication key using PMK.

*AUTH\_KEY = PRF(PMK, A.PAC\_ADDR, B.PAC\_ADDR)*

Then, PD A and coordinator B derive shared KEK, HMAC/CMAC key from the AUTH\_KEY.

*5.15.4.2.3 SA-ENC 3-way handshake*

SA-ENC 3-way handshake consists of the following messages.

(1) SA-ENC-Challenge message (A ← B): B.random, sequence number, PMK lifetime, HMAC/CMAC digest

(2) SA-ENC-Request message (A → B): A.random, B.random, sequence number, security capabilities, security negotiation parameters, HMAC/CMAC digest

(3) SA-ENC-Challenge message (A ← B): A.random, B.random, sequence number, [SA-ENC\_KEY-update,] SA-descriptor, security negotiation parameters, HMAC/CMAC digest

Integrity of the above handshake messages are protected by MAC digest against forgery attack. Optional SA-ENC\_KEY-update contains all the keying materials for the ENC\_KEY update and distribution, which is encrypted with KEK

SA-ENC 3-way handshake provides the following security guarantees:

* Full mutual authentication,
* Message (2) indicates to the coordinator B that a PD A is alive and that A possesses the AUTH\_KEY
* Message (3) indicates to the PD A that the coordinator B is alive
* The coordinator B is guaranteed that SA-ENC-Update is sent by the PD A and is fresh

*5.15.4.2.4 Encryption key delivery*

After a successful authorization, the PAC device A shall dynamically requests parameters for SA(security association) including ENC\_KEY through KEY\_Request and KEY\_Reply messages. When a secure communication is required between the devices, the connections are encrypted using the ENC\_KEY.

*5.15.4.2.5 Group key delivery*

In a network environment where the secure multicast and broadcast service (MBS) is supported, additional group key (GENC\_KEY) generation and delivery process shall be performed optionally after ENC\_KEY distribution procedure. Then, the group communication are encrypted using the GENC\_KEY.

*5.15.4.3 Authorization*

Authorization is the process of deciding if device X is allowed to have access to service Y.

Authorization always includes authentication, and grants access rights to devices on the basis of their trust levels.

|  |  |
| --- | --- |
| Device trust level | Description |
| Trusted device | - The device has been previously authenticated- An authentication key is stored- The device is marked as “trusted” in the device DB |
| Untrusted device | - The device has been previously authenticated- An authentication key is stored- But, the device is not marked as “trusted” in the device DB |
| Unknown device | - No security information is available for this device- This is also an untrusted device |

Trusted devices (authenticated) are allowed to services, but untrusted or unknown devices may require authorization based on interaction before access to services is granted.

Technically, key would be derived or given (established) to the authorized user during the authorization procedure.

Flowchart for authorization is shown as a follow.

Figure 26. Flowchart for authorization

## Coexistence

## Higher layer interaction