**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |  |
| --- | --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) | |
| Title |  | |
| Date Submitted | March 2, 2012 | |
| Source | Yoshihiro Ohba, Yasuyuki Tanaka ()  Stephen Chasko (Landis+Gyr)  Subir Das (ACS) | yoshihiro.ohba@toshiba.co.jp, yatch@isl.rdc.toshiba.co.jp, Stephen.Chasko@landisgyr.com,  sdas@appcomsci.com |
| Re: | This is a response to a Call for Contributions for IEEE 802.15.9 on PANA KMP support. | |
| Abstract | This document contains guidelines for supporting PANA (Protocol for carrying Authentication for Network Access) as a KMP for IEEE 802.15.9. | |
| Purpose | This document is intended for inclusion of 802.15.9 draft specification. | |
| 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. | |

1. **Background**

PANA (Protocol for carrying Authentication for Network Access) [1] transports EAP (Extensible Authentication Protocol) [2] between a PANA Client (PaC) and a PANA Authentication Agent (PAA). RFC 5191 requires PANA protocol messages to be exchanged over an UDP/IP link. In addition, RFC 6345 [3] allows a PaC to reach to a PAA via a PANA Relay Element (PRE) whereby PAA is not reachable via regular IP routing. This is targeted to environments where the PaC is, for example, residing on a resource constrained device that does not have either a direct IP link available or established an IP link with a neighboring node. .

This document provides guidelines for PANA to operate directly over 802.15.9 especially without UDP and IP headers between adjacent 802.15.9-capable nodes.

1. **PANA over 802.15.9**

The main use of PANA over 802.15.9 is for provisioning the link-layer credentials (LLCs) to the joining node, where the LLCs can be of any type including shared key and public key credentials. LLCs are used for secure link establishment between adjacent 802.15.9-capable nodes. The process of provisioning the LLCs is also referred to as bootstrapping. Bootstrapping can also be used for renewing the LLCs. A KMP used for bootstrapping is referred to as a *bootstrapping KMP*. A KMP used to secure link establishment is referred to as a *link-establishment KMP*. While PANA over 802.15.9 can be used for both bootstrapping and link-establishment, this document provides the guidelines for the use of PANA as a bootstrapping KMP. When PANA is used as an 802.15.9 KMP, a PANA PDU without IP and UDP headers is carried in a KMP payload of type “PANA” (to be allocated). 802.15.9 fragmentation is needed when the resulting KMP payload size exceeds the link-layer MTU. The role of a parent node of an 802.15.9-capable PaC depends on the topology of the network (see Table 1).

When an 802.15.9-capable PAA is an 802.15.9 neighbor of the PaC, the two nodes directly communicate with each other. In this case, the PAA is located on the parent node.. On the other hand, when the PAA is not an 802.15.9 neighbor of the PaC (i.e., in multi-hop case), the two nodes indirectly communicate via an 802.15.9-capable PRE. In this case, the PRE is located on the parent node, and PANA messages are relayed by the PRE to PAA via an UDP/IP link. . The relay operation is outside the scope of this document.

Upon successful PANA authentication, link-layer credentials are securely distributed from the PAA to the PaC using PANA payload encryption mechanism as defined in [4].

The call flows for single-hop case and multi-hop case are shown in Figure 1 and Figure 2, respectively. The message format for carrying PANA PDU over 802.15.4e between the PaC and its PAA (single-hop case) or its PRE (multi-hop case) is shown in Figure 3. A PANA PDU consists of 20-octet header followed by zero, one or more AVPs (Attribute-Value Pair), as shown in Figure 4.

Table : Network Topology and PANA Roles

|  |  |  |  |
| --- | --- | --- | --- |
| Topology | Joining Node | Parent Node | Note |
| Single-Hop | PaC | PAA | - |
| Multi-Hop | PaC | PRE | UDP/IP is used for relaying PANA message between the PRE and PAA. (Detailed relay operation is outside the scope of 802.15.9). |

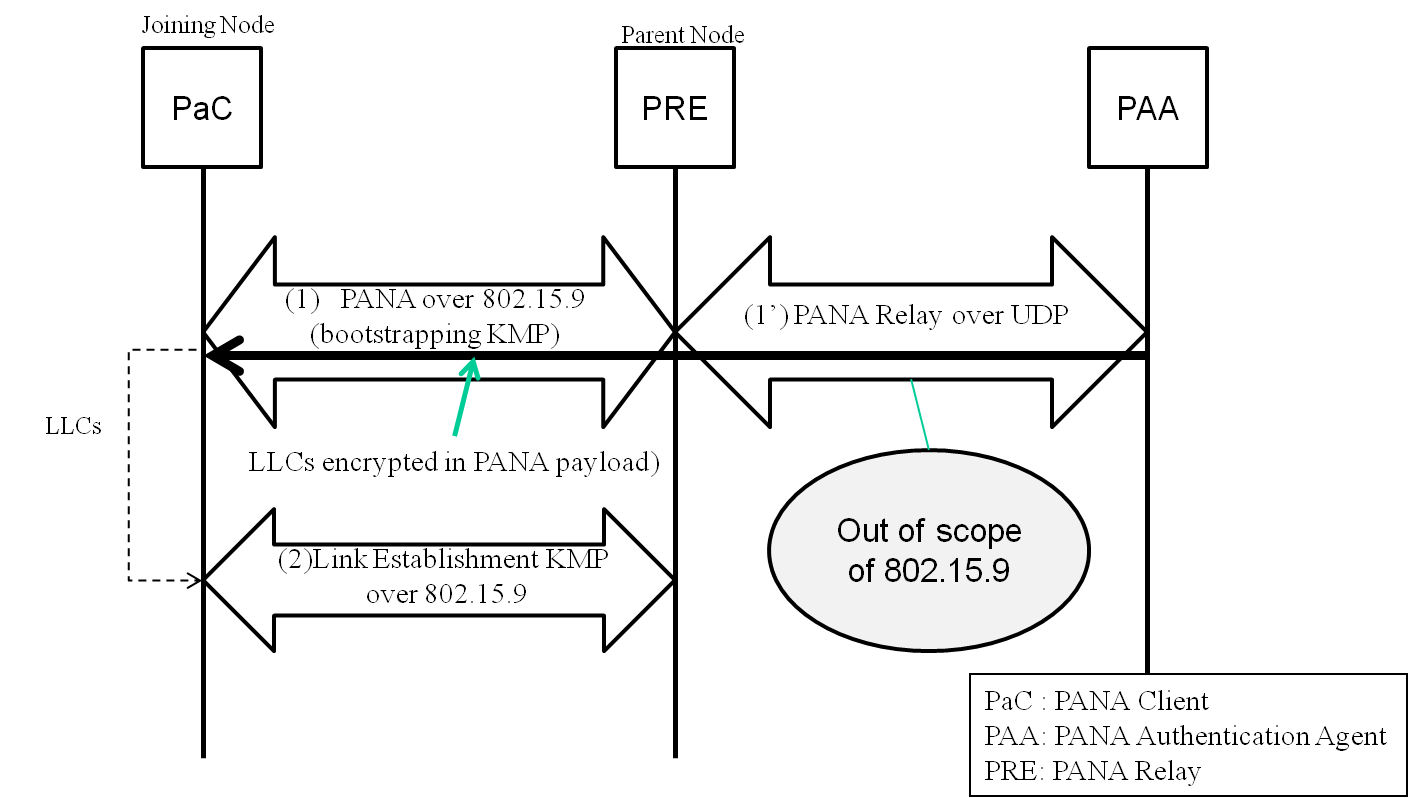


Figure : Call Flow (Single-Hop Case)



Figure : Call Flow (Multi-hop Case)

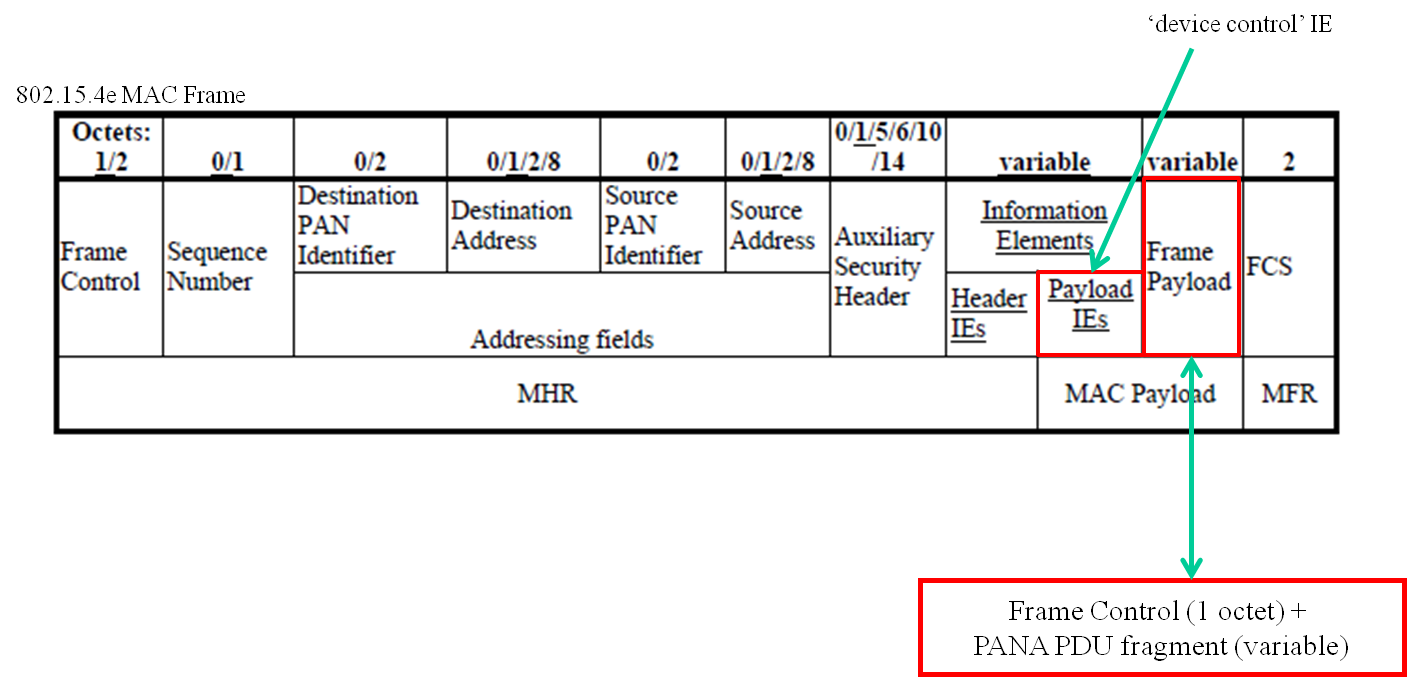


Figure : Message Format for 802.15.4e



Figure 4: PANA PDU Format

1. **References**

**[1] “Protocol for Carrying Authentication for Network Access (PANA)”,**  RFC 5191.

**[2] “Extensible Authentication Protocol (EAP)”,** RFC 3748.

**[3] “Protocol for Carrying Authentication for Network Access (PANA) Relay Element”,**  RFC 6345.

**[4] “Encrypting PANA AVPs”,** Internet-Draft, http://tools.ietf.org/html/draft-yegin-pana-encr-avp.