Diameter Maintenance and Extensions (DIME)
Internet-Draft
Intended status: Experimental
Expires: December 1, 2016

D. Garcia
R. Marin
University of Murcia
A. Kandasamy
A. Pelov
Acklio

May 30, 2016

LoRaWAN Authentication in Diameter
draft-garcia-dime-diameter-lorawan-00

Abstract

This document describes a proposal for a Diameter LoRaWAN Application. The purpose is to integrate the LoRaWAN network join procedure with an Authentication, Authorization and Accounting (AAA) infrastructure based on Diameter.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

Low Power Wide Area Network (LP-WAN) groups several radio technologies that allow communications with nodes far from the central communication endpoint (base station) in the range of kilometers depending on the specifics of the technology and the scenario. They are fairly recent and the protocols to manage those infrastructures are in continuous development. In some cases they may not consider aspects such as key management or directly tackle scalability issue in terms of authentication and authorization. The nodes to be authenticated and authorized is expected to be considerably high in number. One of the protocols that provide a complete solution is LoRaWAN [LoRaWAN]. LoRaWAN is a MAC layer protocol that use LoRa as its physical medium to cover long range (up-to 20km depending on the environment) devices. LoRaWAN is designed for large scale networks and currently has a central entity called network server which maintains a pre-configured key named AppKey for each of the devices on the network. Furthermore, session keys such as NwkSKey and AppSKey used for encryption of data messages, are derived with the help of this AppKey. Since each service provider would operate their network server individually, authenticating the devices becomes a tedious process because of inter-interoperability or the roaming challenges between the

operators. As we know the AAA infrastructure provides a flexible, scalable solution. They offer an opportunity to manage all these proceses in a centralized manner as happens in other type of networks (e.g. cellular, wifi, etc...) making it an interesting asset when integrated into the LoRaWAN architecture.

```
                     +-------+        +-------+              +---------+
   +------+          |       |        |       |              |         |
   |      +--(LoRa)--+       +--(IP)--+       +-----(IP)-----+         |
   +------+          |       |        |       |              |         |
                     +-------+        +-------+              +---------+
   End-Device         Gateway          Network               Application
                                       Server                  Server
```

Figure 1: LoRAWAN Architecture

The End-Device communicates with the Gateway by using the LoRa modulation. The Gateway acts as a simple transceiver, which forwards all data do the Network Server, which performs the processing of the frames, network frame authentication (MIC verification), and which serves as Network Access Port. The Application Server can be handling user data OR can be used during the join procedure to accept an End-Node to the network. In this case, the Application Server is called a Join Server. This document describes a way to use standard Diameter servers as a Join Server, and to use the Diameter protocol for the interaction between the Network Server and the Application Server.

```
                     +-------+        +-------+              +---------+
   +------+          |       |        |       |              |         |
   |AppKey+--(LoRa)--+       +--(IP)--+       +--(Diameter)--+ AppKey  |
   +------+          |       |        |       |              |         |
                     +-------+        +-------+              +---------+
   End-Device         Gateway          Network                Diameter
                                       Server                  Server
                                  (+ Diameter client)
```

Figure 2: LoRAWAN Architecture with AAA and Diameter authentication. End-Device and Diameter server have a shared secret - the AppKey, which is used to derive the session keys (NwkSKey and AppSKey).

The document describes how LoRaWAN join procedure is integrated with AAA infrastructure using Diameter [RFC7155] by defining the new AVPs needed to support the LoRaWAN exchange.

1.1. Requirements Language

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 [RFC2119].

2. LoRaWAN support in Diameter

Regarding the overall functionality, the Diameter LoRaWAN Application relies on [RFC7155] , and defines new Command-Codes and Attribute-Value. Diameter nodes that intend to support this specification MUST advertise its support by including the Diameter LoRaWAN Application ID (TBD.) in the AUTH-Application-Id AVP of the Capabilities-Exchange-Request and the Capabilities-Exchange-Answer command [RFC6733]. If the NAS receives a response with the Result-Code set to DIAMETER_APPLICATION_UNSUPPORTED [RFC6733] , it indicates that the Diameter server in the home realm does not support the LoRaWAN join procedure. The NAS-Port-Type specifying the type of port on which the NAS is authenticating the end-device in this case MAY be 18 (Wireless - Other) or a new one specifically assigned for LoRaWAN (TBD.).

3. LoRaWAN joining procedure

The LoRaWAN joining procedure as described in the LoRaWAN Specification 1.0 [LoRaWAN] consists on one exchange. The first message of this exchange is called join-request (JR) message and is sent from the end-device to the network-server containing the AppEUI and DevEUI of the end-device with additionally a nonce of 2 octets called DevNonce. See Figure 3

Size (bytes)	8	8	2
Join Request	AppEUI	DevEUI	DevNonce

Figure 3: Join Request Message

In response to the join-request, the other endpoint will answer with the join-accept (JA) (Figure 4) if the end-device is successfully authenticated and authorized to join the network. The join-accept contains a nonce (AppNonce), a network identifier (NetID), an end-device address (DevAddr), a delay between the TX and RX (RxDelay) and, optionally, the CFList (see LoRaWAN specification [LoRaWAN] section 7).

Size (bytes)	3	3	4	1	1	16 (Optional)
Join Accept	AppNonce	NetID	DevAddr	DLSettings	RxDelay	CFList

Figure 4: Join Accept Message

4. Protocol Overview

4.1. Protocol Assumptions

For the proposal of Diameter LoRaWAN Application next we describe some assumptions regarding the LoRaWAN specification. The first is that the AppKey is only shared between the AAA server and the end-device. The outcome of the successful join procedure (i.e. NwkSKey and AppSKey) are sent from the AAA server to the network-server. This allows for the end-device to exchange message with the network-server, once the join procedure is finished, as specified in LoRaWAN [LoRaWAN].

4.2. Protocol Exchange

The join procedure between the end-device and the network-server entails one exchange consisting on a join-request message and a join-response message. In Diameter-LoRaWAN the network-server implements a Diameter client to communicate with the AAA Server. Upon reception of the LoRaWAN join-request message, the network-server creates a Diameter-LoRaWAN-Request, with the Join-Request AVP containing the original message from the end-device, and the Join-Answer AVP with all the fields, except for the MIC that will be calculated by the AAA Server, since is the one that holds the AppKey. Once the AAA Server authenticates and authorizes the end-device, sends back the Join-Answer with the MIC generated as specified by the LoRaWAN specification. Furthermore, as a consequence of a successful join procedure, the AppSKey (optional) and NwkSKey are generated and sent along in AppSKey AVP and NwkSKey respectively. The NAS receives the Diameter-LoRaWAN-Answer, obtains the content of the Join-Request AVP and sends it to the end-device, storing in association with that end-device the NwSKey and the AppSKey.

```
                        network-server                            AAA
end-device                   (NAS)                               Server
-----------                ---------                            -------
    |                         |                                    |
    |  JR[MIC]                |         Diameter-LoRaWAN-Request   |
    |------------------------>|                  Join-Request AVP  |
    |                         |                  Join-Answer AVP*  |
    |                         |----------------------------------->|
    |                         |                                    |
    |   gen                   |                                    |  gen
    |    |                    |           Diameter-LoRaWAN-Answer  |   |
    |    |                    |      Result-Code=DIAMETER_SUCCESS  |   |
    |    v                    |                   Join-Answer AVP  |   v
    | AppSKey                 |                      AppSKey AVP*  | AppSKey
    | NwkSKey                 |                        NwSKey AVP  | NwkSKey
    |                         |<-----------------------------------|
    |  JA[MIC]                |                                    |
    |<------------------------|                                    |
    |                         |                                    |
```

Figure 5: Protocol

4.2.1. Join-Request AVP

This AVP contains the original Join-Request message. This AVP will only be present in the Diameter-LoRaWAN-Request.

4.2.2. Join-Answer AVP

This AVP is used in both Diameter-LoRaWAN-Request and Diameter-LoRaWAN-Response messages. In the first case it contains the Join Answer message with all the needed values by the network-server so the AAA server that holds the AppKey is able to create the MIC, that in this case is not present (marked with an *). In the second case, it contains the message with the MIC generated by the AAA server.

4.2.3. AppSKey AVP

This AVP contains the AppSKey, an application session key specific for the end-device. This AVP will only be present in the Diameter-LoRaWAN-Response and its optional.

4.2.4. NwkSKey AVP

This AVP contains the NwkSKey, an network session key specific for the end-device. This AVP will only be present in the Diameter-LoRaWAN-Response.

5. Diameter-Radius Interaction

TBD.

6. Acknowledgments

This work has been possible partially by the SMARTIE project (FP7-SMARTIE-609062 EU Project) and the Spanish National Project CICYT EDISON (TIN2014-52099-R) granted by the Ministry of Economy and Competitiveness of Spain (including ERDF support).

7. Security Considerations

TBD.

8. IANA Considerations

This document has no actions for IANA.

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC6733] Fajardo, V., Ed., Arkko, J., Loughney, J., and G. Zorn, Ed., "Diameter Base Protocol", RFC 6733, DOI 10.17487/RFC6733, October 2012, <http://www.rfc-editor.org/info/rfc6733>.

[RFC7155] Zorn, G., Ed., "Diameter Network Access Server Application", RFC 7155, DOI 10.17487/RFC7155, April 2014, <http://www.rfc-editor.org/info/rfc7155>.

9.2. Informative References

[LoRaWAN] Sornin, N., Luis, M., Eirich, T., and T. Kramp, "LoRa Specification V1.0", January 2015, <https://www.lora-alliance.org/>.

Authors' Addresses

Dan Garcia Carrillo (Ed.)
University of Murcia
Campus de Espinardo S/N, Faculty of Computer Science
Murcia 30100
Spain

Phone: +34 868 88 78 82
Email: dan.garcia@um.es

Rafa Marin-Lopez
University of Murcia
Campus de Espinardo S/N, Faculty of Computer Science
Murcia 30100
Spain

Phone: +34 868 88 85 01
Email: rafa@um.es

Arunprabhu Kandasamy
Acklio
2bis rue de la Chataigneraie
35510 Cesson-Sevigne Cedex
France

Email: arun@ackl.io

Alexander Pelov
Acklio
2bis rue de la Chataigneraie
35510 Cesson-Sevigne Cedex
France

Email: a@ackl.io