LoRaWAN Authentication with RADIUS

Dan Garcia-Carrillo (University of Murcia)
Rafael Marin-Lopez (University of Murcia)
Arunprabhu Kandasamy (Acklio)
Alexander Pelov (Acklio)
LoRaWAN Authentication - LoRaWAN 1.0 Join procedure

1. Commissioning
2. Over the Air Activation (Join Procedure)
LoRaWAN Authentication - Message Definition

• The request (join-request)

<table>
<thead>
<tr>
<th>Size(bytes)</th>
<th>8</th>
<th>8</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Join Request</td>
<td>AppEUI</td>
<td>DevEUI</td>
<td>DevNonce</td>
</tr>
</tbody>
</table>

• The Response (join-accept)

<table>
<thead>
<tr>
<th>Size(bytes)</th>
<th>3</th>
<th>3</th>
<th>4</th>
<th>1</th>
<th>1</th>
<th>16(opt)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Join Accept</td>
<td>AppNonce</td>
<td>NetID</td>
<td>DevAddr</td>
<td>DLSettings</td>
<td>RxDelay</td>
<td>CFList</td>
</tr>
</tbody>
</table>
LoRaWAN Authentication with RADIUS

1. **Commissioning**
2. **Over the Air Activation (Join Procedure)**
3. **RADIUS Extension**

* MIC field empty. To be calculated by the RADIUS server.
** Optional field.
LoRaWAN Authentication with RADIUS

• New RADIUS Attributes
  – JoinRequest (containing the join-request)
  – JoinAnswer (containing the join-accept)
  – Nwkskey (containing the NwkSKey)
  – Appskey (containing the AppSKey, optional)
LoRaWAN Authentication with RADIUS

- **Open Issues**
  - The Join Request has AppEUI indicating the Organization, but to route JR and JA* through the AAA infrastructure we need to specify a realm (e.g. um.es).
  - A mechanism for matching the AppEUI to the domain name of the organization is needed.
  - Possible solution a similar approach as in [RFC7043] using DNS.
LoRaWAN Authentication with RADIUS

• Proof of concept Implementation
  - End Device (Nemeus)
    - usb key with Java app
  - Base station (ExpEmB)
    - Intel Atom, 2GB RAM
  - Lora Network server(Acklio)
    - implemented in golang
  - RADIUS(bronze1man)
    - implemented in golang

Next: Implementation in FreeRADIUS

• [LoRa Network Server] www.ackl.io
• [Radius] github.com/bronze1man/radius
LoRaWAN Authentication with RADIUS

• Acknowledgements

This work has been possible partially by:

– The SMARTIE project (FP7-SMARTIE-609062 EU Project)

– The Spanish National Project CICYT EDISON (TIN2014-52099-R) granted by the Ministry of Economy and Competitiveness of Spain (including ERDF support).