LP-WAN BOF

Application-level protocols, AAA, Management, Security

Alexander Pelov (a@ackl.io)

Rafa Martin Lopez (rafa@um.es)
Dan García Carrillo (dan.garcia@um.es)

LP-WAN network access control

- Only authenticated and authorized nodes should access the network → network access control.
- After authentication and authorization key distribution and management is required to protect the link.
- In general, authentication (if any) is based on a (simple) Pre-Shared Key (PSK) which is configured between the network and the node.
- LP-WAN raises specific requirements
  - Management of the authentication and authorization of high number of nodes.
  - Severe constraints in different areas (Bandwidth, throughput, medium availability, etc.)
  - Different time scale

What can the IETF offer to this area?

- **Authentication, Authorization and Accounting** (AAA) framework and protocols (RADIUS and Diameter)
- AAA deals with high number of users in Authentication, Authorization and Accounting operations.
  - This framework already used in cellular networks and big Wi-Fi deployments (e.g. eduroam)
- It provides a clear "**Guidance for Authentication, Authorization, and Accounting (AAA) Key Management**"
- The Extensible Authentication Protocol (EAP) as a framework to support flexible authentication and precise key management. EAP is well integrated with AAA.
- Technology independent
  - The IETF may provide a common framework/solution to solve authentication, authorization and key management for different LP-WAN technologies (independent of the technology).

AAA

- LP-WANs are trying to solve
  - Can we live with a PSK or we need anything more flexible and scalable?
  - What should AAA model be for LP-WAN?
    - LoRaWAN are currently pondering on redefining their "join" process, which is… authentication!
- IETF toolbox
  - ANIMA/6TiSCH-like
  - EAP-over-CoAP
  - Adapt RADIUS + Diameter
    - Timers / bandwidth / etc. constraints

Rafa Martin Lopez (rafa@um.es)
Dan García Carrillo (dan.garcia@um.es)

Management: state of the art

- L2 MAC commands are inflexible
  - There are just so many combinations you can specify in a documentation
    - E.g. in LoRaWAN, there are 3 orthogonal parameters – Spreading Factor (5 values), Coding Rate (4 values) and Bandwidth (3 values). State space = 5 x 4 x 3 = 60 combinations. The MAC commands allow for 8 predefined ones (+ 8 TBD).
  - No way to validate a configuration automatically, ensure atomicity
  - By definition – L2 dependent. One management tool per technology.
- Application management left up to end-device developer + business application developer
  - Example: change timers 2 years after deployment
- Device lifecycle left to end-device developer

Management: what can the IETF offer?

- Management protocols for complex / advanced features
  - Simple MAC layer to ensure compatibility
  - Scaling up in numbers (to billions) and in time (years) will require more flexibility
- Integration to existing infrastructures
  - Compatibility with Network Management Services
- Profile / optimize current management protocols

Security in LP-WAN is different! Take it into account

- LP-WANs have particular problems
  - Asymmetric links
    - Uplink-only
      - SIGFOX: 140 messages uplink, 4 messages downlink
    - Mostly uplink, low-rate symmetric, multicast
    - Pre-provisioned security credentials
      - New key derivation, encryption, integrity
    - Mobility / roaming
  - Low-throughput networks
    - 50 bps + duty cycling
    - Rethink many security assumptions and models
      - OTP is now a thing! 140*12*365*20 = 12 MB
      - DOS attacks not really a thing
      - Which cypher suites ?
  - Sleepy nodes
    - No RTC
  - Key management (as always)
    - Re-keying
- We have parts of the solutions
  - COSE, ACE, …
  - And the right people

LP-WAN Applications are different

- Limited number of data flows on each end-device
  - Typically 2 flows (control + one app)
- Traffic type
  - Uplink only ; Mostly uplink
    - Could be symmetric or mostly downlink!
  - Multicast would be (really) nice
    - The holy grail: OTA
- Applications "run" on a different scale
  - End-device time-scale
    - Devices could exist for many years
    - Low message rate
  - Business-app time scale
    - Can change frequently (several times each year)
    - High message rate

Current LP-WAN protocol stacks avoid the question

- L1 + L2 (app dispatch) + APP data
  - Acknowledgements?
  - Timers?
  - Longevity?
  - Sleepy nodes?
  - Downlink?
  - Fragmentation?
- There is an implicit APP protocol!
  - L2 + IP + Transport + APP protocol + APP data

IETF value proposition (I/II)

- Profiling the application protocols for LP-WAN
  - L2 / L7 Interplay
  - Acknowledgements
    - Implicit L2 acknowledgements
      - Upon receiving a single L7 acknowledgement, assume N L2 acks
    - Implicit L7 acknowledgements
      - Upon receiving N L2 acks, assume M L7 acks
      - (ROHC+ ?)
  - Duty cycling
- Timers
  - Backhaul links over satellite links
- CoAP specific
  - Use message sequence number as Message ID?
  - …

IETF value proposition (II/II)

- Address LP-WAN technology open questions
  - AAA, Management, Security, Applications, …
- We can help build sustainable technology
  - Protect existing work and ecosystem
  - Maintain momentum and velocity
  - Avoid solution divergence…
    - Which leads to unmanageable siloes
  - Produce BCP, minor adaptations, possibly some standard track work (e.g. compression of IP+UDP +CoAP)