November 16, 2017

Gildas Avoine
Loïc Ferreira

Rescuing LoRaWAN 1.0

Workshop CRYPTACUS

Internet of Things

- 20 billion internet-connected things by 2020 [Gartner]
- Main domains
  - smart home (Zigbee, Z-Wave, BLE, DECT ULE, Thread, etc.)
  - eHealth
  - industrial IoT => allegedly
    - the largest volume of things
    - the most sensitive use cases

Internet of Things

source: http://iot.semtech.com, 17/05/17

- 20 billion internet-connected things by 2020 [Gartner]
- Main domains
  - smart home (Zigbee, Z-Wave, BLE, DECT ULE, Thread, etc.)
  - eHealth
  - industrial IoT => allegedly { the largest volume of things / the most sensitive use cases }

- A proposal for industrial IoT: LoRa (communication layer) & LoRaWAN (security layer)
- Originally conceived by Semtech (Cycleo). Now promoted by LoRa Alliance.

- Deployed in more than 50 countries worldwide: USA (100 cities), Japan, China (300 million people), India (400 million people), France, Netherlands, South Africa, etc.
- Use cases: temperature monitoring, presence detection, remote device on/off switch, etc.

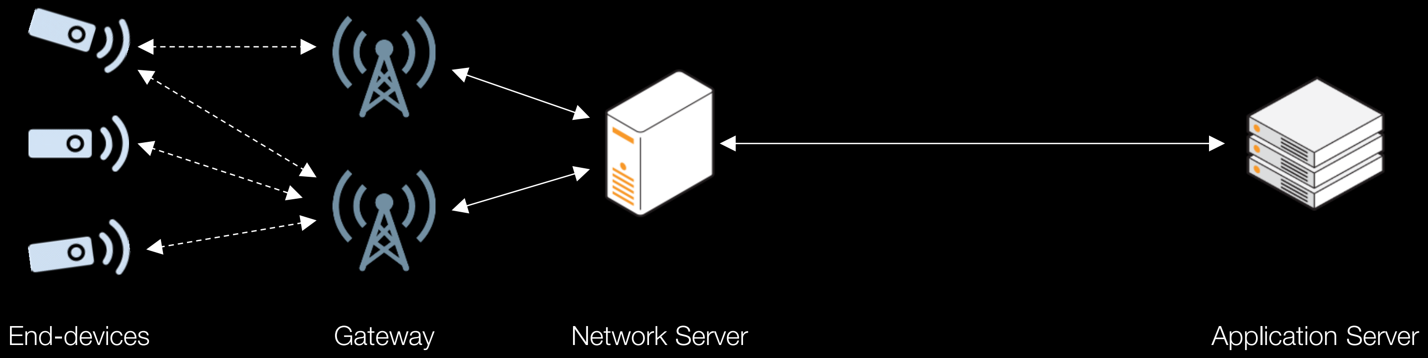
- Current deployed version: v1.0 (this talk).

Ascoel,
IR868LR - IRUS915LR

nke Watteco, Sens'O

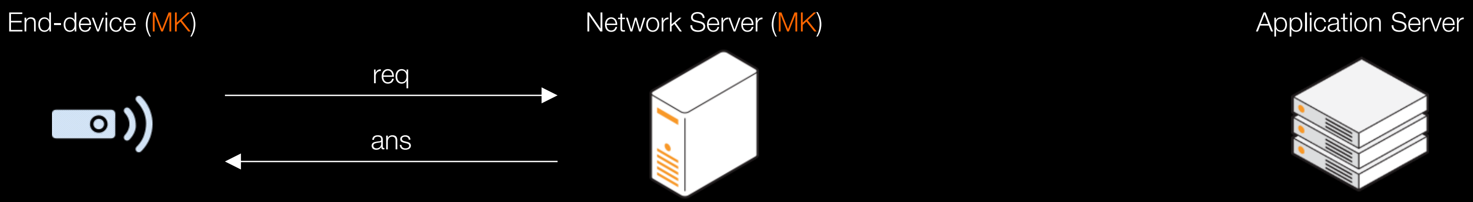
nke Watteco,
Smart Plug

Architecture



Key exchange

Key exchange

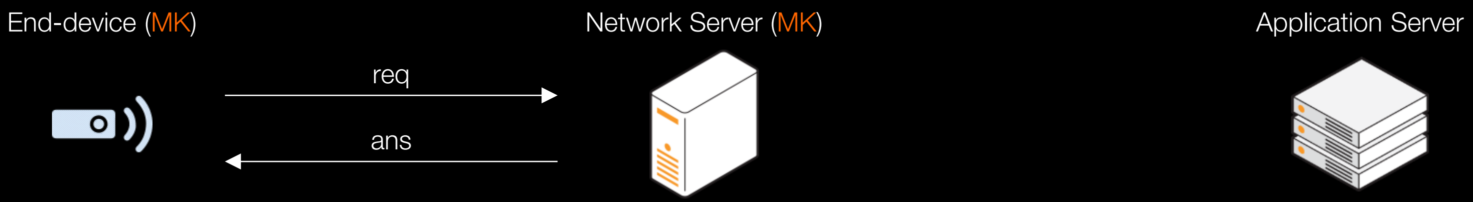


1. $rnd_C \leftarrow \{0,1\}^{16}$
2. $\tau_C = MAC_{MK}(id_{AS} \mid id_C \mid rnd_C)$
3. $req = id_{AS} \mid id_C \mid rnd_C \mid \tau_C$

Key exchange

1. $rnd_C \leftarrow \{0,1\}^{16}$
2. $\tau_C = MAC_{MK}(id_{AS} \mid id_C \mid rnd_C)$
3. $req = id_{AS} \mid id_C \mid rnd_C \mid \tau_C$
4. check req
5. $rnd_S \leftarrow \{0,1\}^{24}$
6. $\tau_S = MAC_{MK}(rnd_S \mid id_S \mid addr \mid prms)$
7. $ans = AES^{-1}_{MK}(rnd_S \mid id_S \mid addr \mid prms \mid \tau_S)$
8. check ans

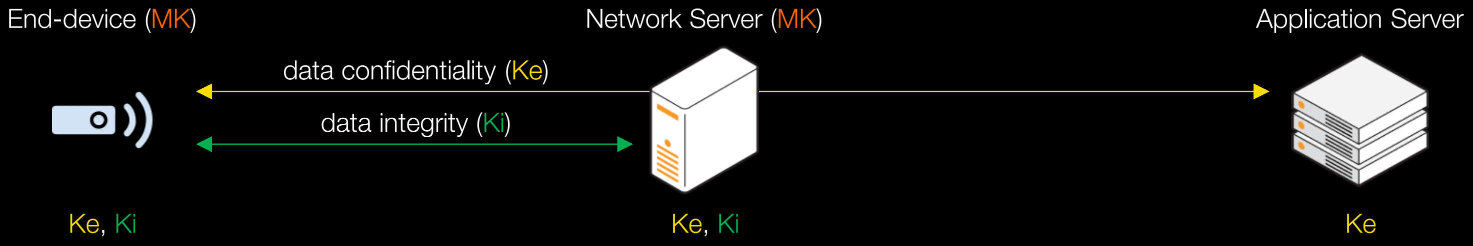
Key exchange



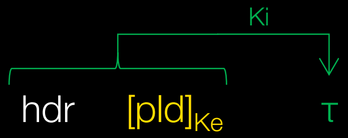
1. $rnd_C \leftarrow \{0,1\}^{16}$
2. $\tau_C = MAC_{MK}(id_{AS} \mid id_C \mid rnd_C)$
3. $req = id_{AS} \mid id_C \mid rnd_C \mid \tau_C$
4. check req
5. $rnd_S \leftarrow \{0,1\}^{24}$
6. $\tau_S = MAC_{MK}(rnd_S \mid id_S \mid addr \mid prms)$
7. $ans = AES^{-1}_{MK}(rnd_S \mid id_S \mid addr \mid prms \mid \tau_S)$
8. check ans

Data encryption key $Ke = ENC_{MK}(01 \mid v)$
Data integrity key $Ki = ENC_{MK}(02 \mid v)$
with $v = rnd_S \mid id_S \mid rnd_C \mid 00..00$

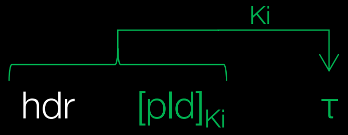
Secure channel



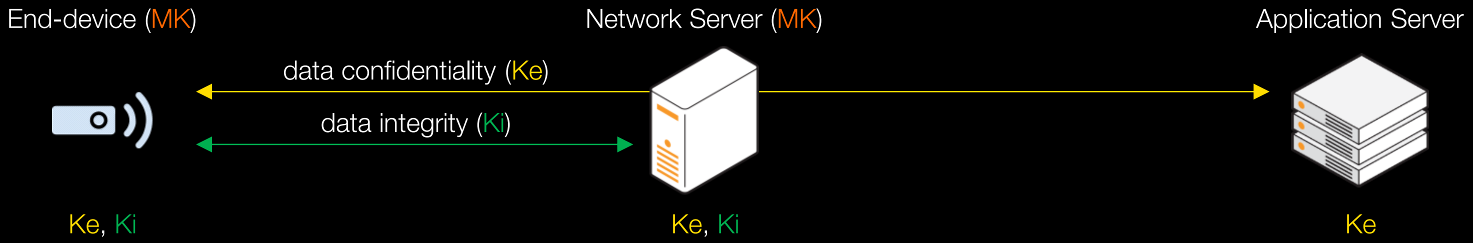
- Application frame



- Network frame

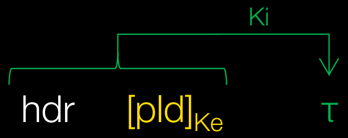


Secure channel

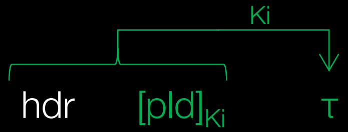


- Encryption: based on AES CCM
  - A_j (16) = 01 | 00…00 | dir | addr (4) | cnt (4) | 00 | j (1)
  - $S_j = AES_K(A_j)$ with $K = \begin{cases} Ke & \text{if application data} \\ Ki & \text{if network data} \end{cases}$
  - $ctxt = pld \oplus (S_0 \mid .. \mid S_{n-1})$

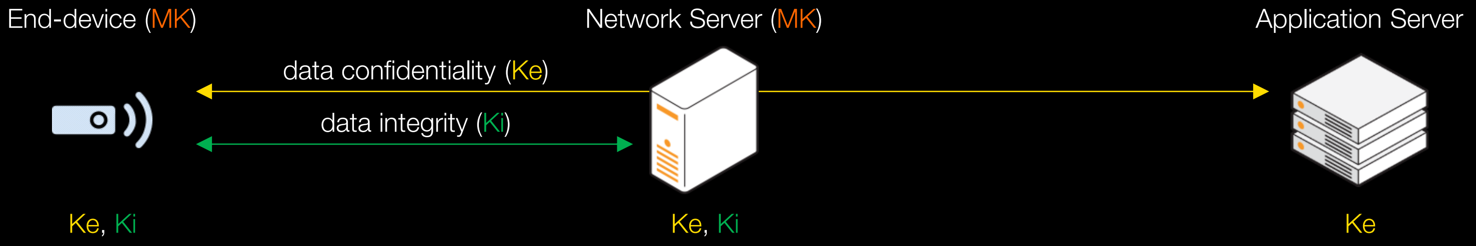
- Application frame



- Network frame

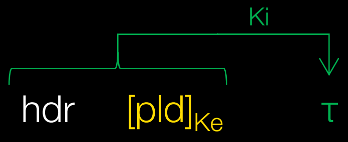


Secure channel

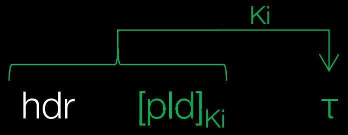


- Encryption: based on AES CCM
  - A_j (16) = 01 | 00…00 | dir | addr (4) | cnt (4) | 00 | j (1)
  - $S_j = AES_K(A_j)$ with $K = \begin{cases} Ke & \text{if application data} \\ Ki & \text{if network data} \end{cases}$
  - $ctxt = pld \oplus (S_0 \mid .. \mid S_{n-1})$
- MAC: AES CMAC
  - B_0 (16) = 49 | 00…00 | dir | addr (4) | cnt (4) | 00 | len (1)
  - $\tau = MAC_{Ki}(B_0 \mid hdr \mid ctxt)$
- Message: hdr | $[pld]_K$ | τ

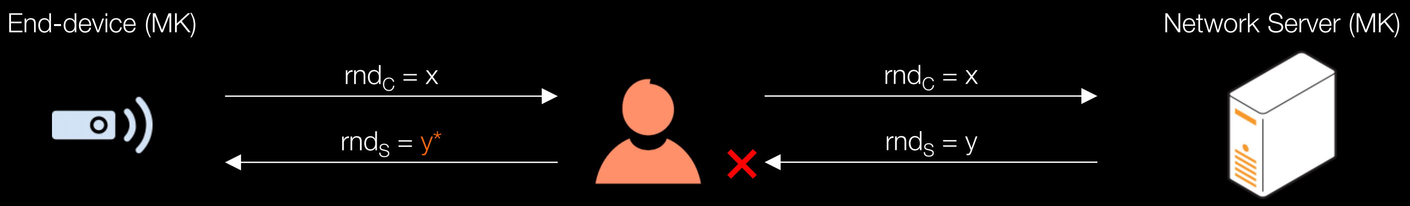
- Application frame



- Network frame



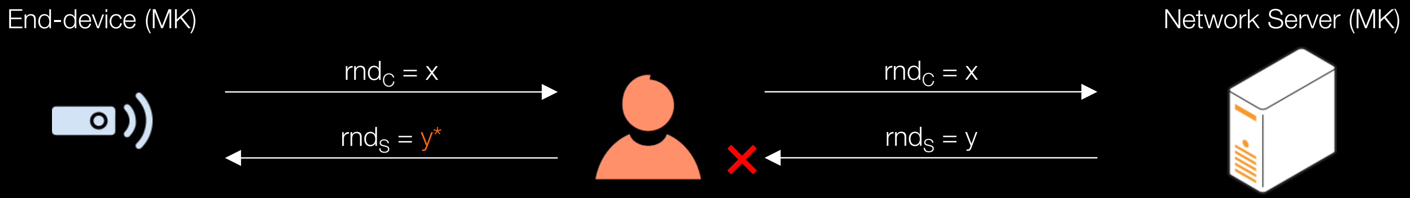
Attack: end-device disconnection



- $Ke^* = ENC_{MK}(01 \mid v^*)$
  $Ki^* = ENC_{MK}(02 \mid v^*)$
  with $v^* = y^* \mid id_S \mid x \mid 00..00$

- $Ke = ENC_{MK}(01 \mid v)$
  $Ki = ENC_{MK}(02 \mid v)$
  with $v = y \mid id_S \mid x \mid 00..00$

Attack: end-device disconnection



- $Ke^* = ENC_{MK}(01 \mid v^*)$
  $Ki^* = ENC_{MK}(02 \mid v^*)$
  with $v^* = y^* \mid id_S \mid x \mid 00..00$

- $Ke = ENC_{MK}(01 \mid v)$
  $Ki = ENC_{MK}(02 \mid v)$
  with $v = y \mid id_S \mid x \mid 00..00$

- The end-device is "disconnected".
- The NS cannot initiate a new session.
- The end-device may not expect replies from the NS.

If no reply is received within the next ADR_ACK_DELAY uplinks (i.e., after a total of ADR_ACK_LIMIT + ADR_ACK_DELAY), the end-device may try to regain connectivity by switching to the next lower data rate that provides a longer radio range. The end-device will further lower its data rate step by step every time ADR_ACK_DELAY is reached. The **ADRACKReq** shall not be set if the device uses its lowest available data rate because in that case no action can be taken to improve the link range.

LoRaWAN 1.0.2 specification, § 4.3.1.1, p. 17

Attack: replay or decrypt

- $Ke = ENC_{MK}(01 \mid v)$
  $Ki = ENC_{MK}(02 \mid v)$
  with $v = rnd_S \mid id_S \mid rnd_C \mid 00..00$

- $A_j\ (16) = 01 \mid 00\ldots00 \mid dir \mid addr\ (4) \mid cnt\ (4) \mid 00 \mid j\ (1)$
  $S_j = AES_K(A_j)$
  $ctxt = pld \oplus (S_0 \mid .. \mid S_{n-1})$

- $B_0\ (16) = 49 \mid 00\ldots00 \mid dir \mid addr\ (4) \mid cnt\ (4) \mid 00 \mid len\ (1)$
  $\tau = MAC_{Ki}(B_0 \mid hdr \mid ctxt)$

1. Replay of $ans = AES^{-1}_{MK}(rnd_S \mid id_S \mid addr \mid prms \mid \tau_S)$
2. Reuse of rnd_C

=> Reuse of Ke, Ki, A_j, B_0

Attack: replay or decrypt

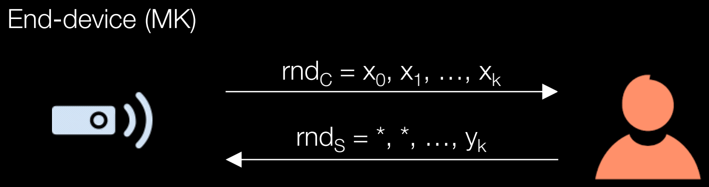
- Consequences
  - (downlink) frame replay
  - (uplink) frame decryption:

$$\left.\begin{array}{l}\text{ctxt} = \text{pld} \oplus \text{S} \\ \text{ctxt'} = \text{pld'} \oplus \text{S}\end{array}\right\} \text{ctxt} \oplus \text{ctxt'} = \text{pld} \oplus \text{pld'}$$

Attack: replay or decrypt

- Consequences
  - (downlink) frame replay
  - (uplink) frame decryption: $ctxt = pld \oplus S$, $ctxt' = pld' \oplus S$ $\Rightarrow$ $ctxt \oplus ctxt' = pld \oplus pld'$

- $Pr[hit] = 2^{-16}$
- With n previous ans messages, $Pr[hit] \approx n.2^{-16} = p$
- The attacker iterates k times: $Pr[success] = 1 - (1 - p)^k \approx k.p$
- Complexity: $k \approx 2^{16}/n$ to get $Pr[success] \approx 1$
- 8 s/key exchange => 9.1 hours (with n = 16)

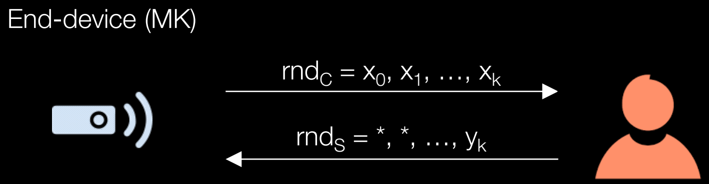


Attack: replay or decrypt

- Consequences
  - (downlink) frame replay
  - (uplink) frame decryption: $ctxt = pld \oplus S$, $ctxt' = pld' \oplus S$ } $ctxt \oplus ctxt' = pld \oplus pld'$

- $Pr[hit] = 2^{-16}$
- With n previous ans messages, $Pr[hit] \approx n.2^{-16} = p$
- The attacker iterates k times: $Pr[success] = 1 - (1 - p)^k \approx k.p$
- Complexity: $k \approx 2^{16}/n$ to get $Pr[success] \approx 1$
- 8 s/key exchange => 9.1 hours (with n = 16)

- Remark on the duty cycle
  - Not a security mechanism
  - Not applied in all countries
  - Not verified through the LoRa Alliance certification process



To fully test the End Device the DUT needs to run a test application (in a test mode) running on top of the MAC layer and must disable any duty cycle restrictions as well as suspend its normal application software. The LoRa Certification testing will not do any duty cycle testing. The required test

LoRa Alliance End Device Certification Requirements for EU 868MHz ISM Band Devices, D. Hunt, N. Jouko, M. Ridder, v1.2, 2016

Attack: targetting the NS

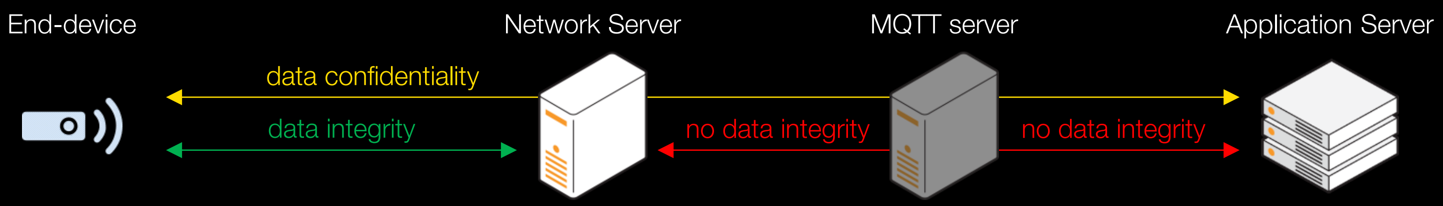
- Disconnection and "replay or decrypt" doable against the NS.

- Disconnection
  - The NS must keep track of a "*certain number*" of previous req messages.
    => Use of "forgotten" or "unknown" req messages.

- "Replay or decrypt"
  - $|rnd_S| = 24$ bits => $Pr[hit] \approx 2^{-24}$
  - addr is "*arbitrarily*" generated => $Pr[hit] \approx 2^{-49}$
  - The attacker chooses rnd_C first (then the NS replies).
  - Use of n req messages: $Pr[success] \approx n/2^{24}$ (if addr is unchanged)

- Consequences
  - (uplink) frame replay
  - (downlin) frame decryption

Lack of data integrity



- Encryption in CTR mode
  - Change plaintext by flipping ciphertext bits => end-device or AS is deceived
  - Truncate encrypted payload => hide information from end-device or AS
  - Possible payload decryption under assumptions (easier in uplink direction)

Recommendations

- Constraints: keep interoperability between patched and unmodified equipment

- rnd_S replaced with 24-bit counter (1 counter per end-device)
- $addr = H(rnd_C \mid rnd_S \mid id_C)$
- Key confirmation by NS (using an existing LoRaWAN command)
- Provide end-to-end data integrity (application layer)

Conclusion

- Low cost security => low power attacks
- LoRaWAN 1.0 published without security analysis

- Upcoming version: v1.1 (includes some recommendations related to v1.0)
- LoRa Alliance: call for a public review of LoRaWAN 1.1 from the academic community

Thank you

References

[LoRaWAN1.0] N. Sornin, M. Luis, T. Eirich, T. Kramp, O. Hersent. *LoRaWAN Specification* (Jul 2016), LoRa Alliance, version 1.0.2

[Gartner] Mark Hung (ed.). *Leading the IoT – Gartner Insights on How to Lead in a Connected World*, Gartner, 2017. https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf