End-to-end security in LoRa and NB-IoT sensor networks.

Presenters: Niek van Noort and Jason Kerssens
Supervisors: Cedric Both and Jeroen de Boer from DataDigest

Introduction

- IoT monitoring devices
  - Make use of technologies with long range, low power consumption (LoRa, NB-IoT)
- End-to-end security important
  - Confidentiality, integrity, authentication

- Long Range (LoRa):
  - Connect via a gateway to a network, unlicensed band.
- Narrowband IoT (NB-IoT):
  - Via a Mobile Network Operator (MNO), licensed band.

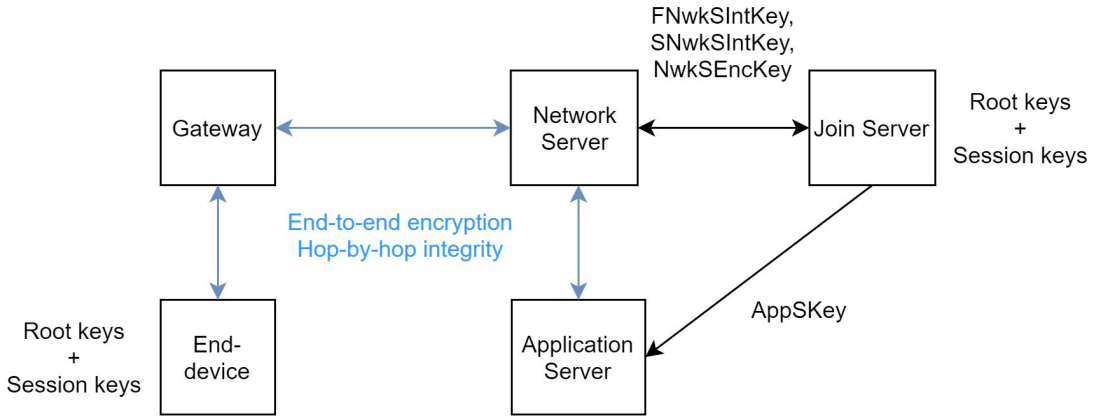
Research questions

How can end-to-end confidentiality, authentication, and data integrity be achieved with IoT devices that make use of LoRa and NB-IoT?

- What capabilities do LoRa and NB-IoT have in terms of confidentiality, authentication and integrity?
- What security risks are present in LoRa and NB-IoT, relating to confidentiality, authentication, and data integrity?
- What security measurements could be taken by an administrator of an IoT network to achieve end-to-end security?

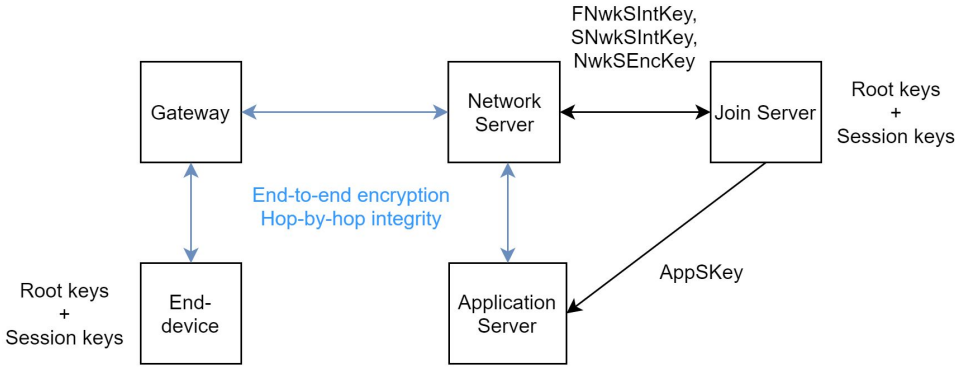
Background: LoRa

- End-device
- Gateway
- Network server
- Application server
- Join server
  - Manages end-devices wanting wanting to join the network



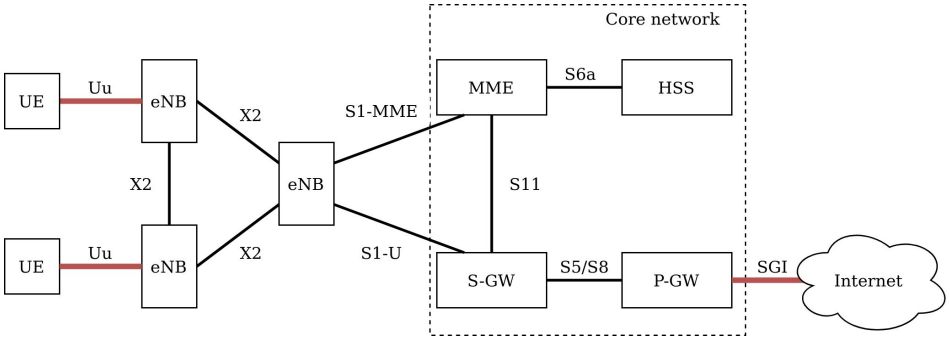
Background: LoRa

- End-to-end confidentiality
  - Symmetric-key encryption between end-device and application server
- Hop-by-hop integrity
  - Between end-device and network server, and between networks server and application server



Background: LTE

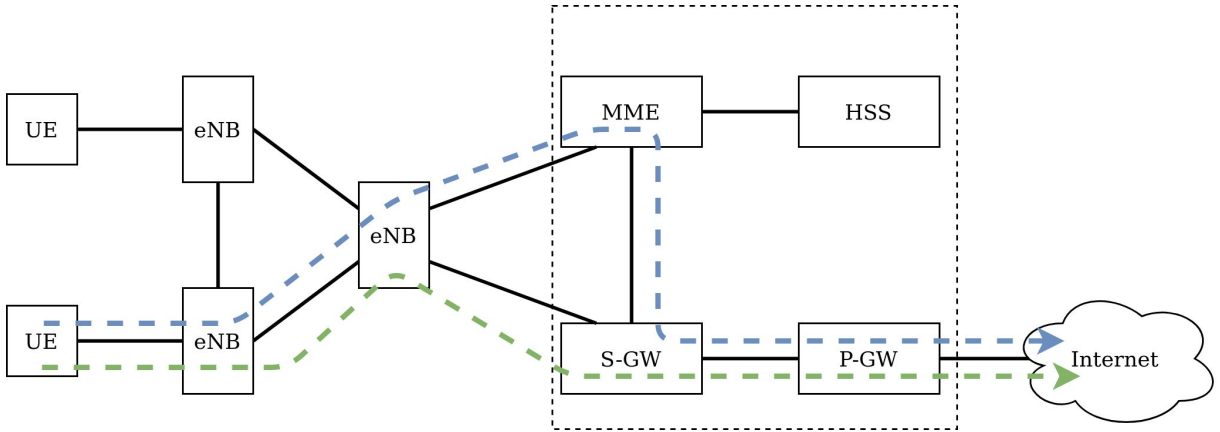
- Uu Interface (Air interface):
  - Confidentiality at the control plane and the user plane.
  - Integrity at the control plane.
- SGI interface:
  - To external networks
  - No confidentiality
  - No integrity



UE = IoT monitoring device
eNB = Cell Tower

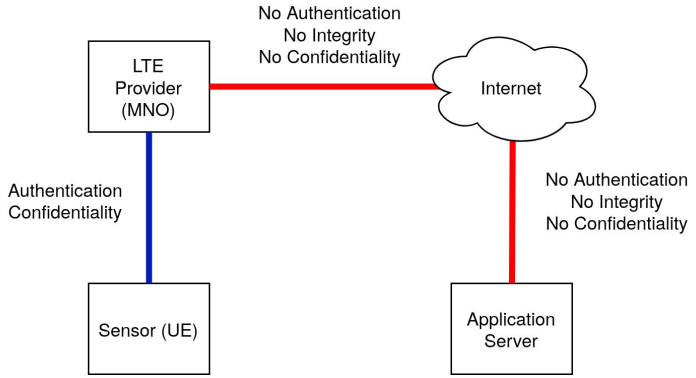
Background: NB-IoT

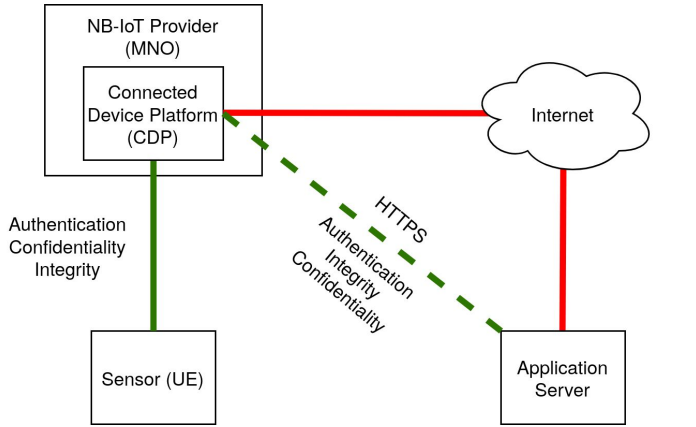
- Data via MME:
  - User data over the control plane.
  - User data integrity at the Uu Interface.
- UDP



Background: NB-IoT

- Application server
  - E.g. Monitoring platform.
- Connected Device Platform (CDP):
  - Buffer between MNO and application server.
- HTTPS
- Possible hop-by-hop security with trust in MNO.
- Datagram TLS (DTLS)





Related work

● Florian Laurentiu Coman et al.	LoRaWAN packet forging by bruteforcing the Message Integrity Code (MIC).
● Emekcan Aras et al.	Compromising LoRa root keys with physical access, jamming and replay attack by rebooting end-devices.
● Florian Laurentiu Coman et al.	DoS attacks of NB-IoT user equipment.

Methodology: LoRa

- End-device:
  - RN2483A LoRaBee module
  - SODAQ Autonomo
    - Programmable with Arduino IDE
- Gateway:
  - Robustel R3000 LG
- Network server, application server:
  - ChirpStack
- No end-to-end integrity

Methodology: LoRa

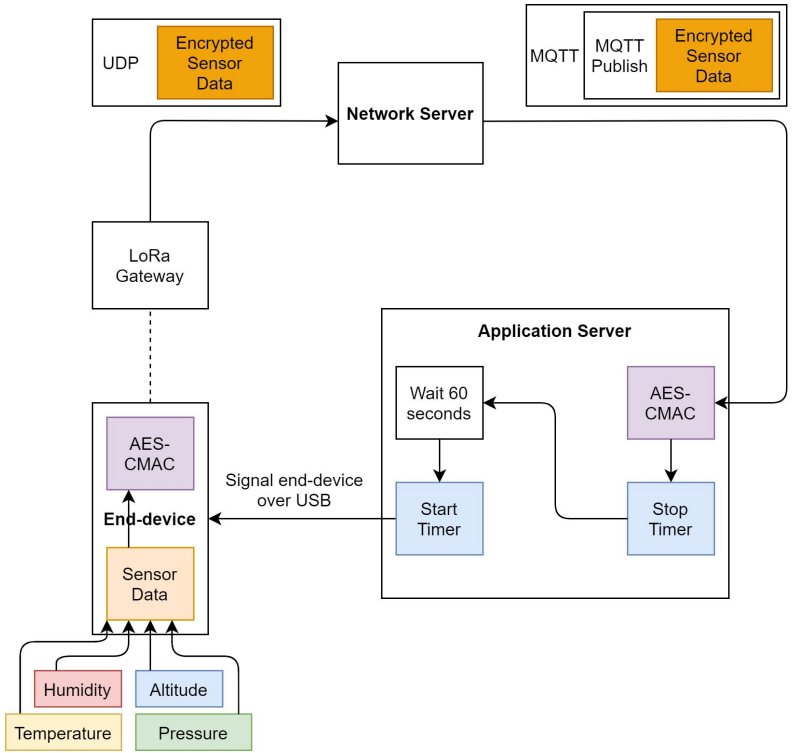
- AES-CMAC:
  - Provides integrity
  - Input: plaintext, 128 bit key
  - Output: 128 bit tag

  - AES-CMAC implementation:
    - User Equipment: WolfSSL
    - Application Server: Cryptography (Python library)

- Include frame counter in the input to mitigate certain replay attacks

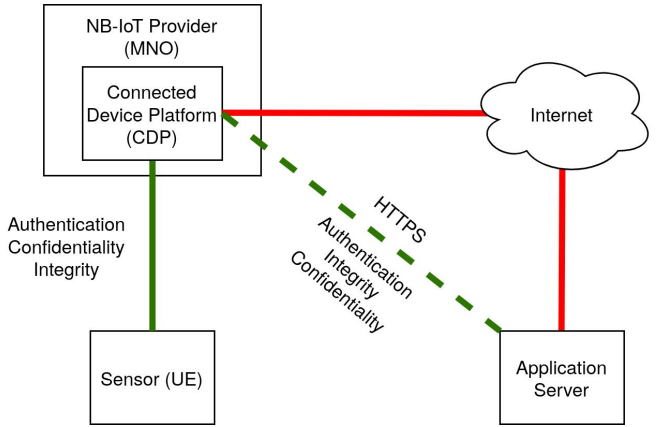
Methodology: LoRa

- AES-CMAC execution time measurement
  - Create tag
  - Verify tag
- Latency measurement
  - With and without AES-CMAC
  - 16 bytes sensor data
  - 16 bytes tag



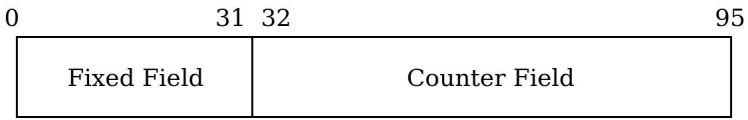
Methodology: NB-IoT

- User Equipment (UE):
  - SODAQ NB-IoT Shield
    - Programmable with Arduino IDE
  - Ublox SARA N211 02B-00
    - No DTLS support
- Mobile Network Operator:
  - T-Mobile
  - Use of CDP
- No end-to-end security.



Methodology: NB-IoT

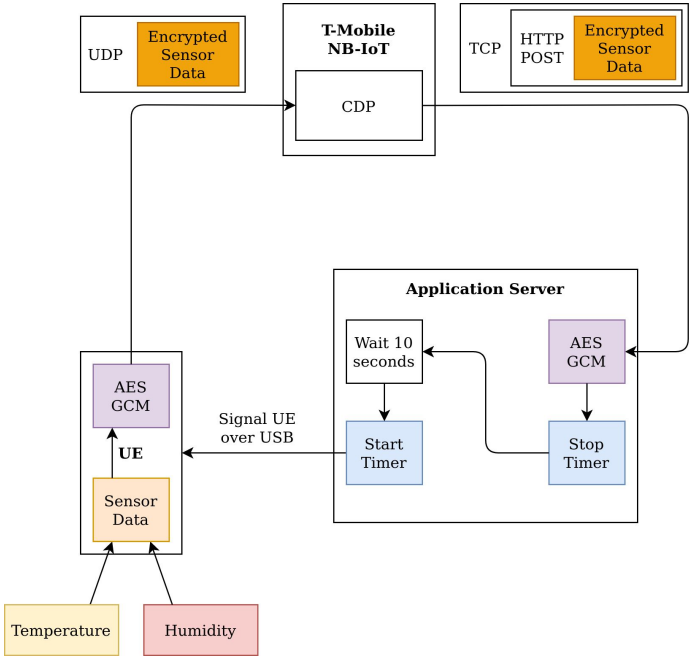
- AES-GCM:
  - Confidentiality and Integrity
  - Input: Plain text, Initialization Vector (IV), 128 bit key.
  - Output: Cipher text, 128 bit tag
  - 96 bit IV:
    - 32 bits fixed field
    - 64 bits counter field
    - An IV must never be used with the same key twice!



  - AES-GCM implementation:
    - User Equipment: WolfSSL
    - Application Server: Cryptography (Python library)

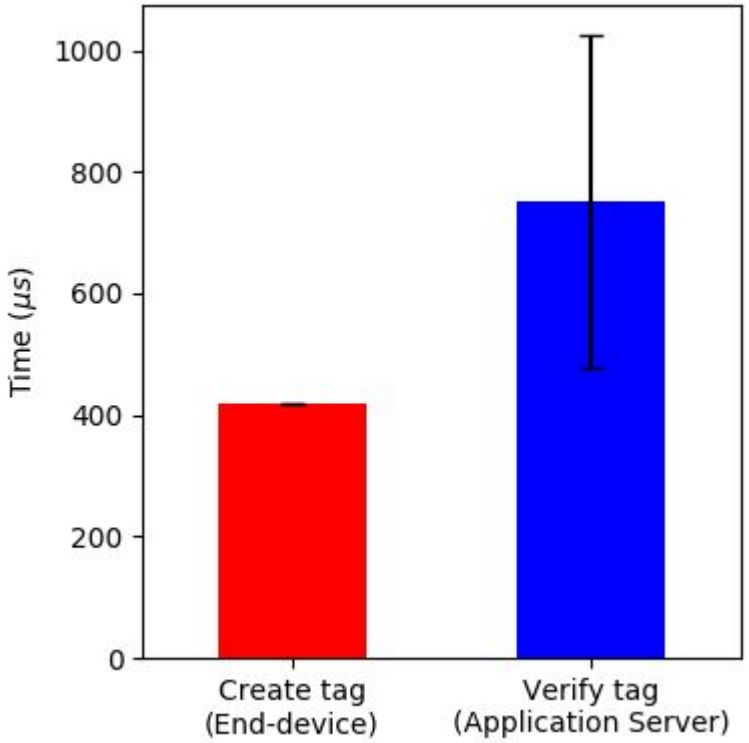
Methodology: NB-IoT

- AES-GCM execution time measurement
  - Encryption
  - Decryption
- Latency measurement
  - With and without AES-GCM
  - 8 bytes sensor data
  - 28 bytes AES-GCM tag + IV



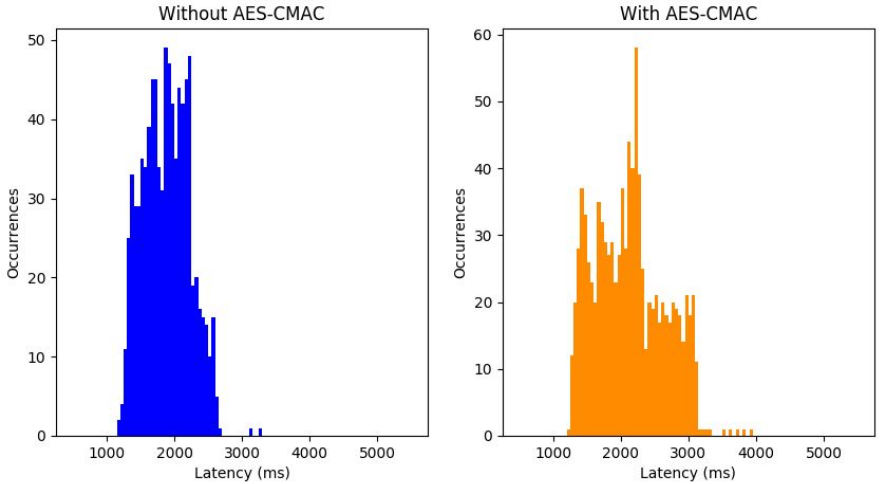
Results: LoRa

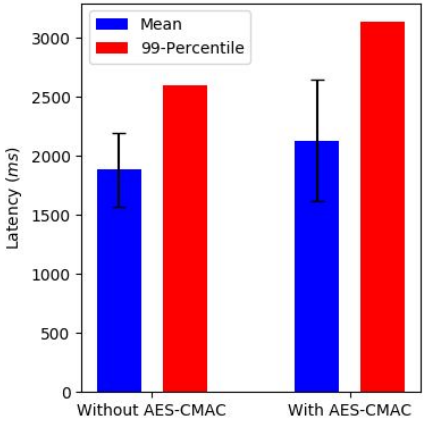
- Create tag: 418μs
- Verify tag: 750μs



Results: LoRa

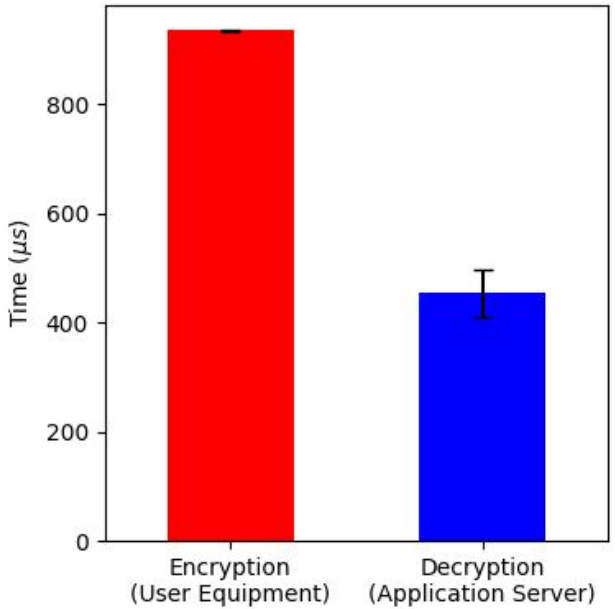
- Mean
  - Without CMAC: 1884 ms
  - With CMAC: 2132 ms
- 99-percentile
  - Without CMAC: 2597 ms
  - With CMAC: 3139 ms





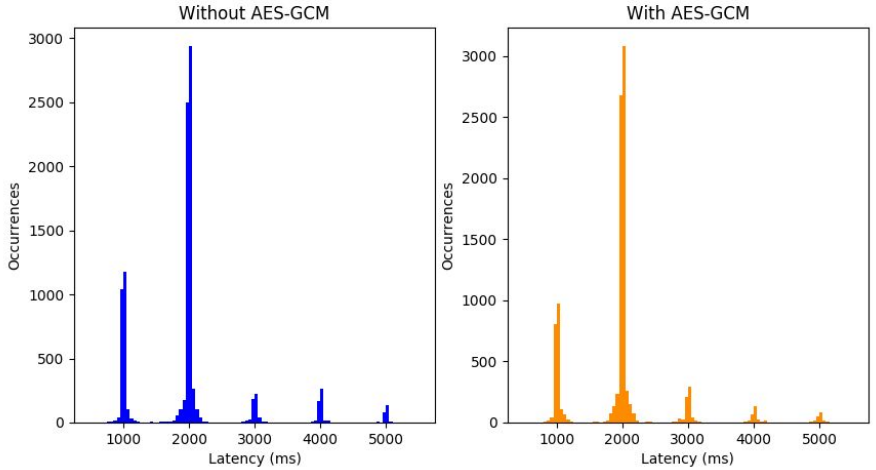
Results: NB-IoT

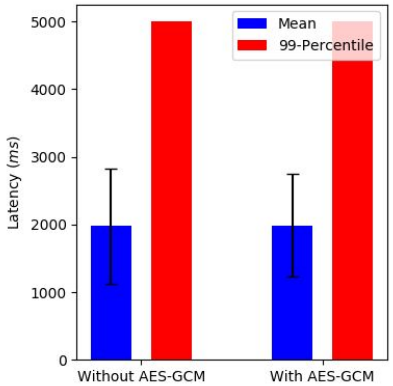
- Encryption: 935 μs
- Decryption: 453 μs



Results: NB-IoT

- Spikes separated by one second.
- Mean:
  - With AES-GCM: 1982 ms
  - Without AES-GCM: 1984 ms
- 99-Percentile: 5007 ms
- No significant effect on the latency





Conclusion

- LoRa
  - Supports end-to-end confidentiality and hop-by-hop integrity.
  - End-to-end integrity can be implemented
  - AES-CMAC does affect the latency significantly

- NB-IoT:
  - No standard end-to-end security.
  - Confidentiality and integrity is possible in an hop-by-hop manner.
  - Depending on MNO and user equipment, DTLS can be used.
  - End-to-end security can be implemented at the application layer.
  - AES-GCM has no significant effect on the NB-IoT latency.

Future work

- Power Consumption
- DTLS
- Other technologies (Sigfox, LTE-M)