Security for the Industrial IoT: The Case for Information-Centric Networking

IEEE World Forum on IoT
Limerick, Ireland

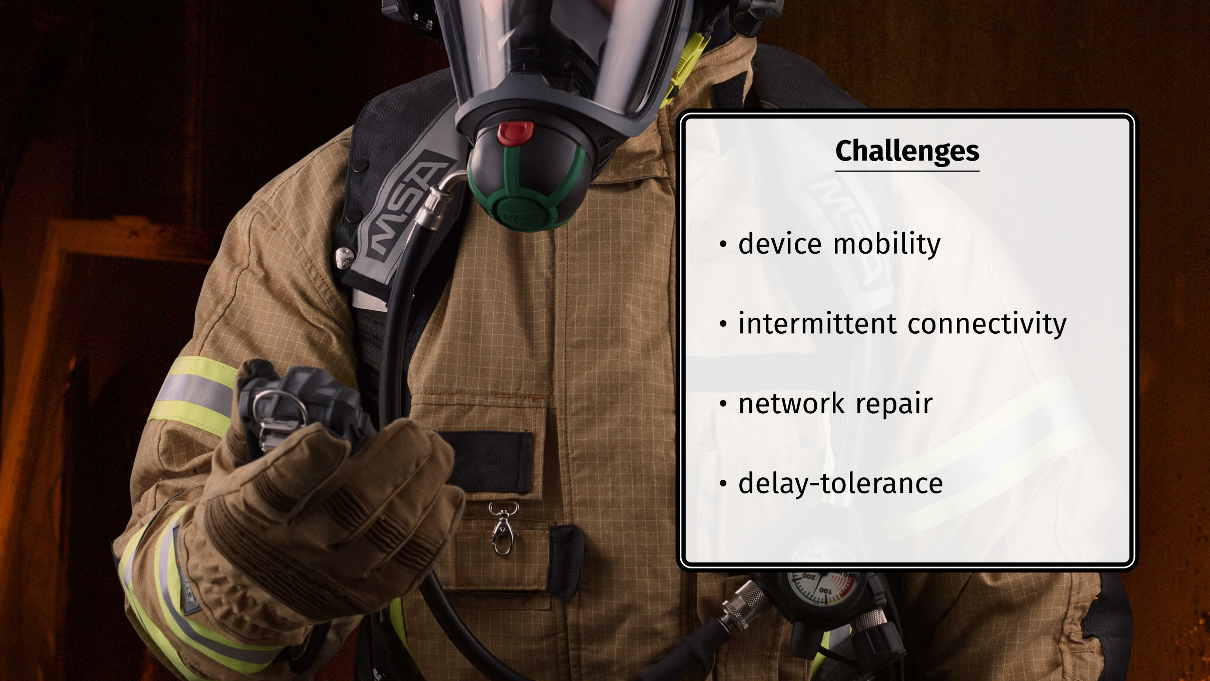
Michael Frey[1] Cenk Gündoğan[2] Peter Kietzmann[2]
Martine Lenders[3] Hauke Petersen[3] Thomas Schmidt[2]
Felix Shzu-Juraschek[1] Matthias Wählisch[3]

[1]Safety IO [2]HAW Hamburg [3]Freie Universität Berlin

April 17, 2019

Network Requirements

- wide area deployments
- time-sensitive traffic flows
- secure communication
- hardened infrastructure



Challenges

- device mobility
- intermittent connectivity
- network repair
- delay-tolerance

Agenda

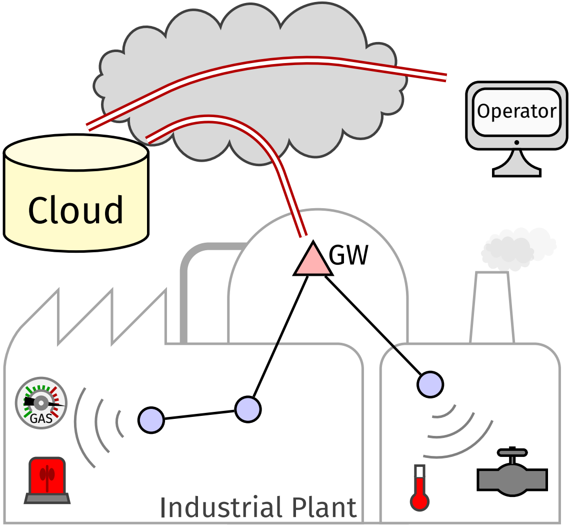
Industrial IoT Deployments: Today & Future

Information-Centric Networking for the Industrial IoT

Comparative Security Assessment

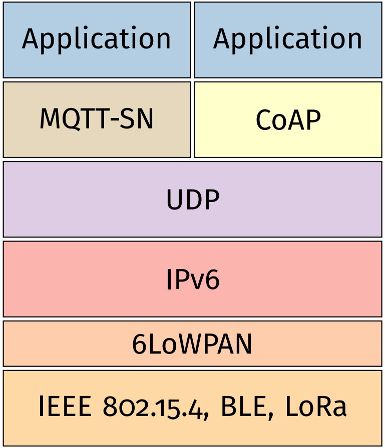
Conclusion

Industrial IoT Deployments of Today



═ Trusted Channels

Standard Protocol Stack for the Industrial IoT



Application | Application

MQTT-SN | CoAP

UDP

IPv6

6LoWPAN

IEEE 802.15.4, BLE, LoRa

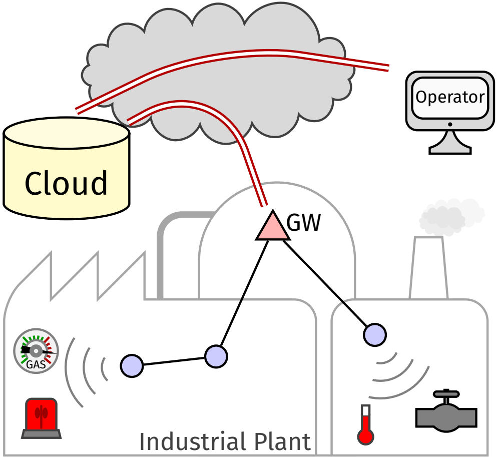
MQTT

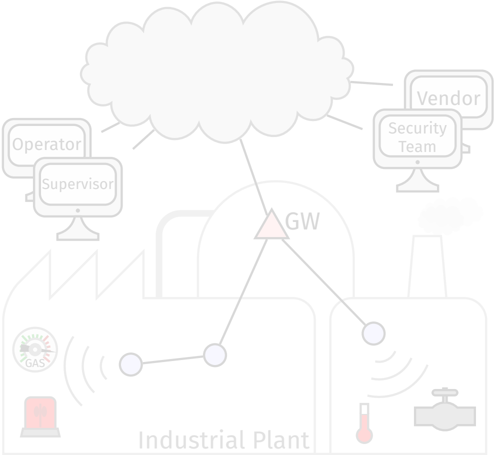
- First specification in 1999
- ISO/IEC 20922 in 2016
- Pub-sub using message broker
- MQTT-SN for sensor networks in 2007

CoAP

- RFC7252 in 2014
- REST architecture
- Supported communication schemes: polling, push, observe

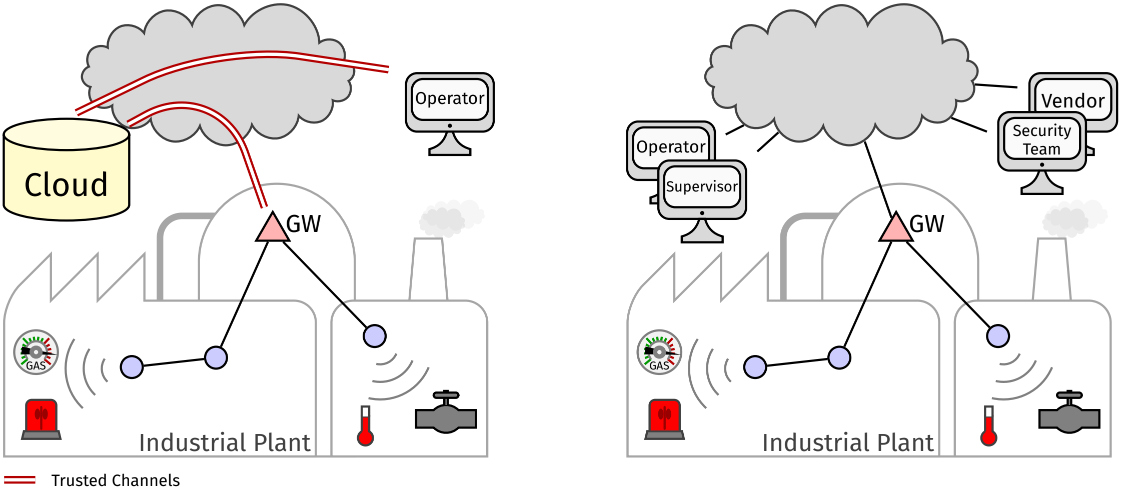
Break-up of Silos



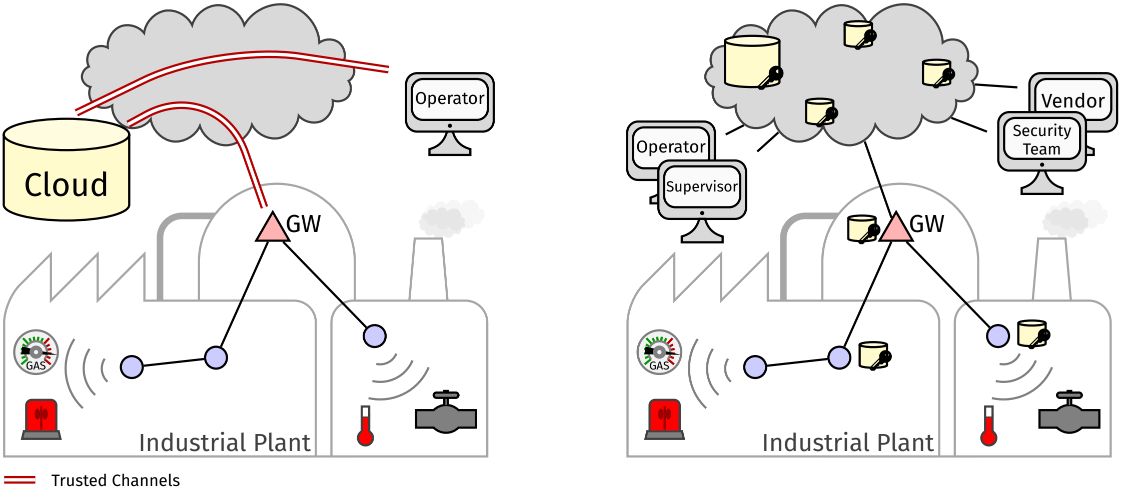


═ Trusted Channels

Break-up of Silos

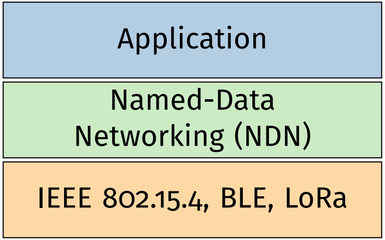


Break-up of Silos



Information-Centric Networking (ICN)

- Future Internet architecture
- Flavors: NDN, CCNx, NetInf, ...
- Content-aware, not host-aware
- Request-response paradigm
- Ubiquitous content caching
- Inherent multicast support



Application

Named-Data Networking (NDN)

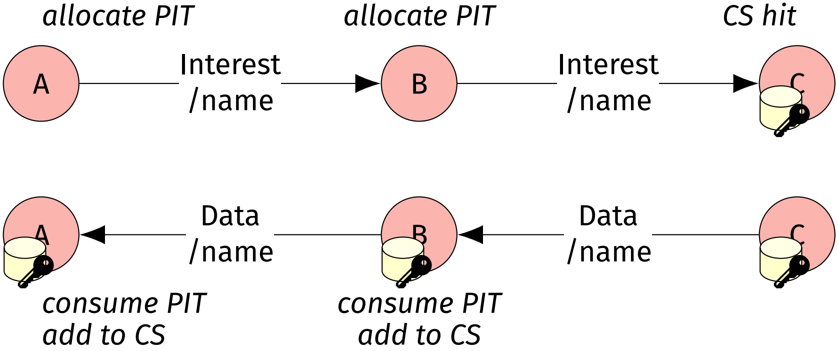
IEEE 802.15.4, BLE, LoRa

ICN in IoT

- Reduced network stack complexity
- Hop-by-hop flow balance
- Hop-wise retransmissions

NDN Primitives

- FIB: Forwarding Information Base contains names
- PIT: Pending Interest Table to hold open request state
- CS: Content Store for seamless in-network caching



Comparative Security Assessment

1. Caching
2. Reliability
3. Object security: authenticity & integrity
4. Infrastructure protection
5. Name privacy

Caching

- Enhances content availability
- Increases robustness against network failures and denial of service attacks

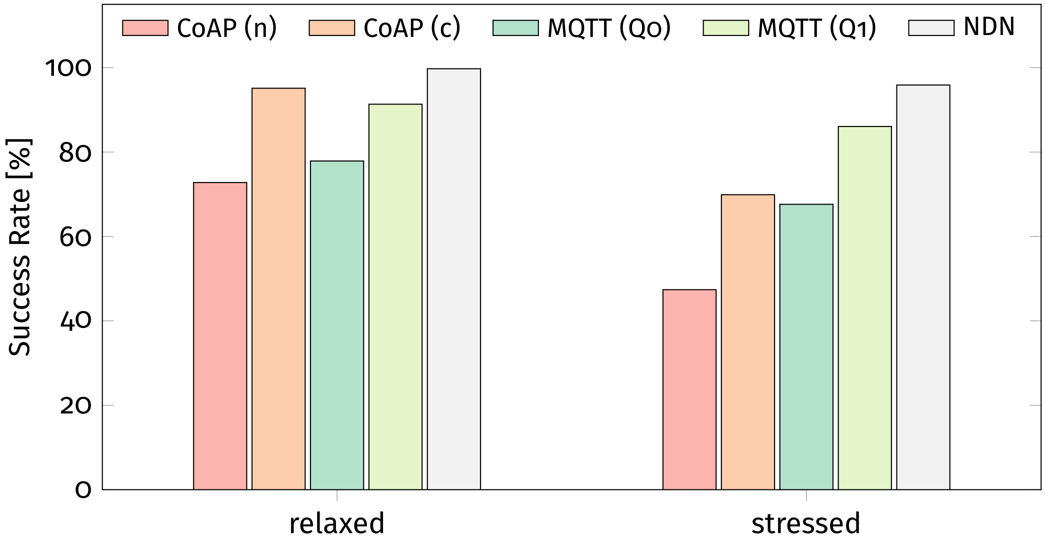
MQTT-SN	**CoAP**	**NDN**
✗	(✓)	✓
no caching supported	support on application layer	support on network layer

Reliability

Experiment Setup

- FIT IoTLab Testbed: 50 class 2 devices ($\approx$ 50 kiB RAM / $\approx$ 250 KiB ROM)
- Multi-hop topology using DODAG rooted at gateway (convergecast)
- Relaxed scenario: $\approx\ 1.6\ \frac{data\ packet}{s}$ traverse gateway
- Stressed scenario: $\approx\ 10\ \frac{data\ packet}{s}$ traverse gateway

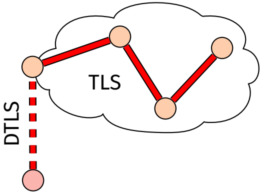
Reliability: Experimental Results

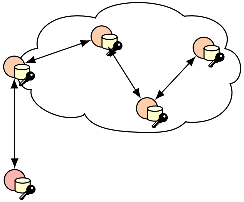


Object Security: Integrity & Authenticity

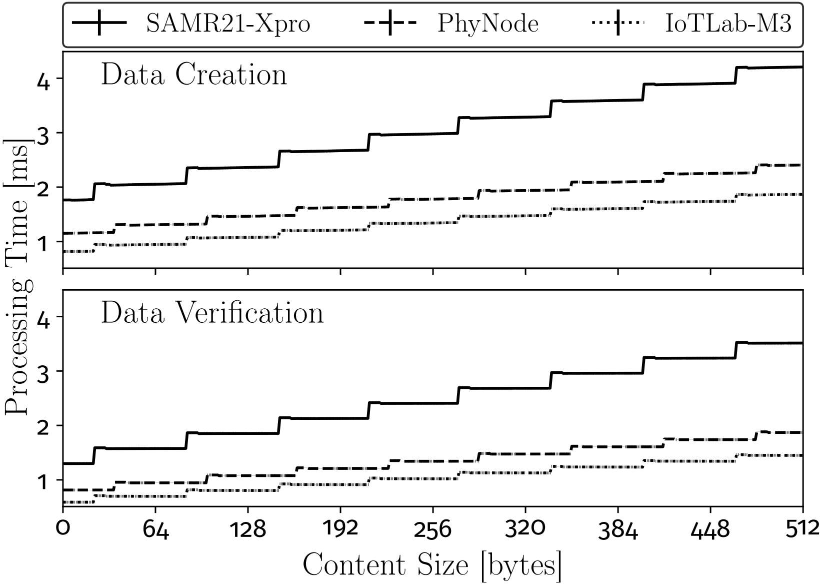
- Protects content on gateways during protocol translations (e.g., DTLS ⇒ TLS)

MQTT-SN	**CoAP**	**NDN**
✗ no protocol feature	(✓) future support OSCORE, draft-16	✓ digital signatures for each content



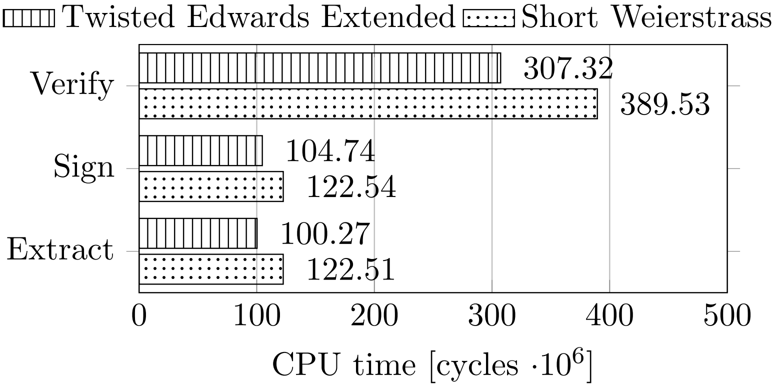


Object Integrity in NDN: Expenses of HMAC



Object Authenticity in NDN: Identity-Based Security

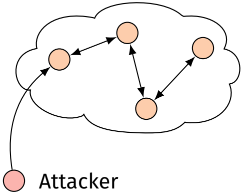
- Trust anchor generates TAPrivKey & TAPubKey
- Obtain private key: TAPrivKey $\bigoplus$ /name
- Obtain public key: TAPubKey $\bigoplus$ /name

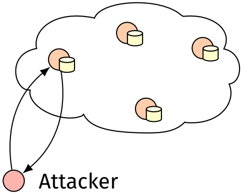


Infrastructure Protection

- Protection against reflective amplification attacks

MQTT-SN	CoAP	NDN
✗	✗	✓
prone to IP spoofing	prone to IP spoofing	no ent-to-end notion
UDP, connectionless	UDP, connectionless	de-localized content
no congestion control	no congestion control	flow balance





Conclusion

ICN Benefits

- Resilient to intermittent connectivity
- Increased content availability
- Hardened network infrastructure
  - in-network caching
  - no end-to-end paradigm
- Seamless multi-party data access

ICN is a viable solution for secure and lightweight Industrial IoT deployments