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

Michael Frey*, Cenk Gündoğan†, Peter Kietzmann†, Martine Lenders‡, Hauke Petersen‡, Thomas C. Schmidt†,
Felix Juraschek*, Matthias Wählisch‡

Safety IO*   HAW Hamburg, Germany†   Freie Universität Berlin, Germany‡
{first.last}@{safetyio.com, haw-hamburg.de, fu-berlin.de}, t.schmidt@haw-hamburg.de

Abstract—**Industrial production plants traditionally include sensors for monitoring or documenting processes, and actuators for enabling corrective actions in cases of misconfigurations, failures, or dangerous events. With the advent of the IoT, embedded controllers link these 'things' to local networks that often are of low power wireless kind, and are interconnected via gateways to some cloud from the global Internet. Inter-networked sensors and actuators in the industrial IoT form a critical subsystem while frequently operating under harsh conditions. It is currently under debate how to approach inter-networking of critical industrial components in a safe and secure manner.**

In this paper, we analyze the potentials of ICN for providing a secure and robust networking solution for constrained controllers in industrial safety systems. We showcase hazardous gas sensing in widespread industrial environments, such as refineries, and compare with IP-based approaches such as CoAP and MQTT. Our findings indicate that the content-centric security model, as well as enhanced DoS resistance are important arguments for deploying Information Centric Networking in a safety-critical industrial IoT. Evaluation of the crypto efforts on the RIOT operating system for content security reveal its feasibility for common deployment scenarios.

Index Terms—**DoS resilience, unprotected channel, robust communication,**

I. Introduction

Things in the Internet of Things (IoT) are often represented by small embedded controllers which possess orders of magnitude less resources (kBytes of memory, MHz CPU speed, mW of power) than regular Internet nodes, but still need to communicate using protocols that interoperate in a common infrastructure. One predominant deployment area is industrial automation and surveillance, since embedded controllers are already prevalent in this industry, and adding a networking layer can generate immediate cost and performance benefits for its users. Initial deployments rely on legacy protocols such as MQTT—convergence on a future common networking standard for the industrial IoT is still under debate.

Today's things are sensors or actuators that speak with a remote cloud or talk with each other locally. The prevalent communication for edge devices happens on wireless channels that are from low power lossy networks (LLNs) in the battery-powered world. Following the IEEE 802.15.4, BLE, or LWPAN standard, these nodes can exchange only small packets at very low rates and sleep frequently. Violating

these constraints quickly leads to successive overload, extreme packet losses, and may strongly degrade network operation and node availability. Repeated incidents have shown that the mass of IoT nodes can be both highly threatened and a threat to the global Internet.

Information Centric Networking (ICN) [1] was introduced as a networking paradigm for improved content access in a Future Internet. Ubiquitous caching is a core feature of ICN. NDN (or CCN) [2], its most popular flavor, was designed from a strong security perspective as a pure request-response scheme. It became apparent [3]–[6] that ICN exhibits great potential for the IoT. The access of named content instead of distant nodes does not only allow for a much leaner and more robust implementation of a network layer, but in particular the request-response pattern of NDN prevents overloading the receiver with data.

ICN deployment in the IoT has been studied with increasing intensity [4], [7]–[9], touching various design aspects and practical use cases. Several implementations have become available in common IoT operating systems. CCN-Lite runs on RIOT [4], [10] and on Contiki [11], NDN has been ported to RIOT [12]. Thus, grounds are prepared for opening the floor to real-world IoT applications with NDN.

In this paper, we discuss central security aspects of NDN using the example of an industrial safety system. We introduce a real-world use case which we implemented in a recent prototype and identify key security requirements in Section II. The fundamental security contributions of the ICN networking layer are derived in Section III. Section IV is dedicated to comparative analyses of NDN versus traditional IP-based approaches. We further show by measurements that the underlying crypto-complexity can be well handled by constrained IoT nodes. A summary and an outlook conclude this paper in Section V.

II. Use Case: Security and Safety in Hazardous Industrial Environments

Industrial safety and control systems are increasingly interconnected to interchange operational conditions locally and to report their status updates to external observers. A typical deployment scenario consists of IoT stub networks that are often wireless and confined to the production plant, together with gateways that uplink to an Internet service provider.

Current initial deployment scenarios further involve a (private) cloud which a dedicated group of trustees can access. Typical stakeholders are the operators of the systems. All parties rely on secure communication channels established between the network endpoints and the cloud. This scenario builds closed data silos for a preselected, confined group. It is visualized in Figure 1a.

Already today it becomes apparent that the number of stakeholders in emerging scenarios will widen—plant operators, emergency teams, equipment vendors, and supervisory authorities may retrieve information about current safety conditions, intermediate operational statistics, as well as long-term reports. Furthermore, even a wider public may legitimately require civil participation in affairs of common impact, as is developing from many open urban sensing initiatives [13], as well as participatory European laws. Following this demand, data silos need to break up in favour of a flexible, distributed data access that cannot easily rely on preconfigured trusted channels. Still, data might not be uniformly public, but continue to require protection. Protecting the data itself instead of the transmission channels paves the way to transparent data replication and caching—an efficient method for eliding today's silos. This heterogeneous environment built from several independent stakeholders is visualized in Figure 1b.

Industrial deployments often operate under harsh conditions. In our use case, we consider industrial environments with a threat of hazardous contaminant (e.g., explosive gas) that need continuous monitoring by stationary, as well as mobile sensors. In case of an emergency, immediate actions are required such as issuing local alarms, activating protective shut-downs (e.g., closing valves, halting pumps), initiating a remote recording for first responders and forensic purposes, and eventually may need to trigger evacuations of the plant or even the region. Such complex settings obviously involve many parties and require a level of robustness which a single uplink to a remote cloud cannot guarantee.

This use case specifically relies on a fast sensor-actuator network including embedded IoT nodes. The harsh industrial environment raises the challenges of mobile, intermittently connected end nodes, network partitioning, and enhanced reliability from safety requirements. Devices often need to connect spontaneously, and a corresponding IoT system cannot reliably establish end-to-end channels in many situations. Varying connectivity challenges and mobility, as well as external hazardous impacts are much easier mitigated in a replicative environment, where data diffuses hop-wise in an asynchronous fashion. It is easy to build such a compliant networking layer based on NDN primitives [14].

Typical industrial plants are widespread with sparse network coverage, so that mobile workers or machines face intermittent connectivity at scattered gateways. Some sensors and actuators are infrastructure bound, others are independent, battery-powered embedded devices (e.g., body equipment). Such devices are susceptible to battery drains and can process only a few packets per minute on average. They are easily challenged by various distributed denial-of-service (DDoS)

attacks. Hence networking approaches should minimize the DDoS surface and protect the embedded edge components.

Taken from real-world deployment, this study makes the case for a distributed, multi-stakeholder environment and identifies three major objectives for the networking layer:

1) Allow for ubiquitous multiparty data access without pre-established secure data channels or VPNs in the constrained IoT.
2) Provide a robustly secure networking infrastructure that is resilient to varying link conditions and mobility with the ability to recover locally from intermittent impairments.
3) Raise the barriers for DDoS attacks of constrained devices and confine the attack surface of unwanted traffic to local links.

We will show in the following, how the NDN approaches to Information Centric Networking can significantly contribute to these goals. We will also assess the shortcomings of current IoT solutions such as MQTT [15] and CoAP [16].

III. SECURITY CONTRIBUTIONS OF NDN

According to our use case, an industrial IoT deployment enhances requirements in the security and safety domain, but on the other hand narrows the utilization of ICN functions down to rather specific settings. In this section, we will discuss the three security aspects derived from our use case and identify certain benefits for NDN from its specific deployment in an industrial setting.

A. Ubiquitous data access in the constrained IoT

Sensor data need to be accessible both in the local constrained IoT, and in the remote for various stakeholders. Safety and security of the industrial monitoring system indeed largely depend on its availability even under the harsh conditions of local or regional incidents with intermittent connectivity. As critical industrial facilities are always also susceptible to malicious threats, utmost resilience against (networked) attacks is strongly desirable. Clearly, a centralized cloud-based approach falls short as tampering the cloud has proven to be a pronounced attack vector (cf. the Cloudflare attack 2013).

Ubiquitous caching is the most striking contribution ICN makes to the security and safety of the distributed information system. Configuring the constrained nodes as well as the gateway to replicate and store IoT data for (most of) its lifetime will maximize redundancy and minimize unavailability of critical information. It is noteworthy that common IoT data is small and of limited lifetime—archives being a well-localized exception. Furthermore, flash storage in constrained nodes is the least scarce resource and typically can accommodate an 'infinite' amount of IoT data.

Local mass storage facilitates the DTN nature of ICN for the IoT. The hop-by-hop transmission of sensor readings and actuator commands increases resilience in the presence of caching. When links re-establish after mobility handovers or

(a) Current IoT deployment: Processing and sharing of data via dedicated cloud services of a single operator.

(b) Upcoming IoT deployment: Multiple stakeholders share content based on in-network caching in ICN.
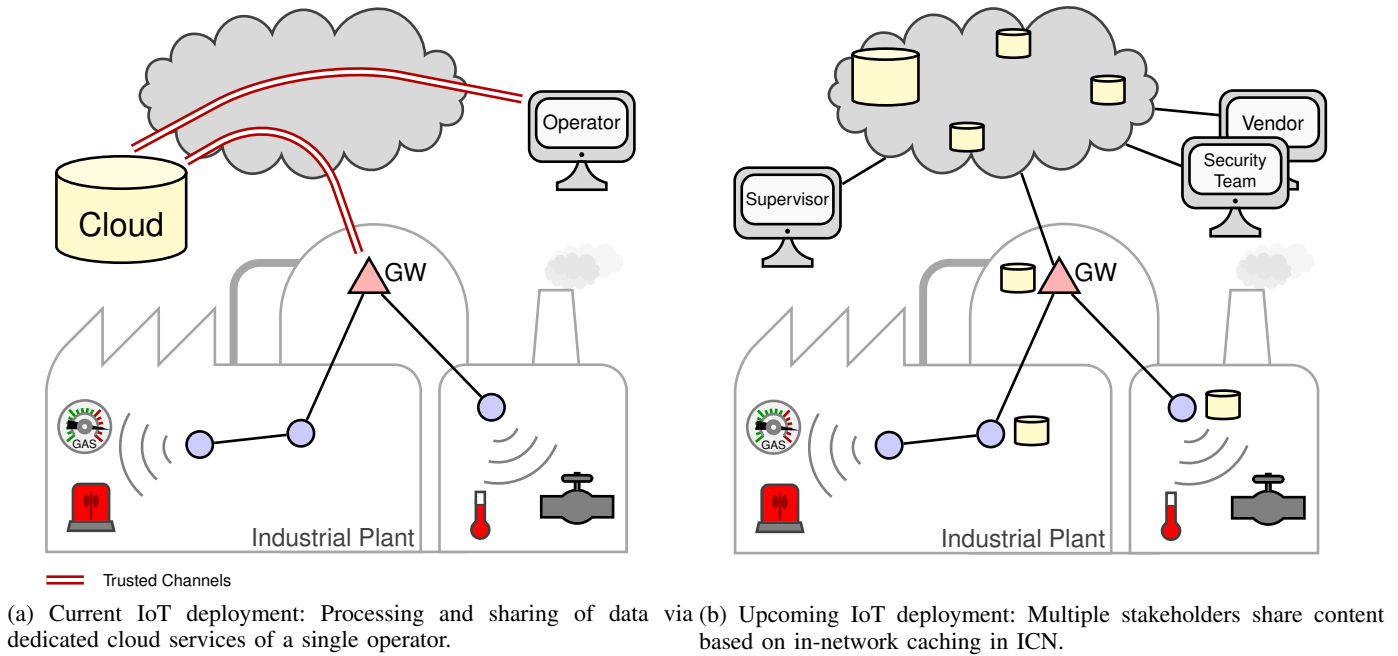
Fig. 1: Current and future deployment scenarios of the industrial Internet.

failures, the NDN network layer can easily resume the content propagation and will thus provide an efficient self-healing mechanism.

B. Robustly secure networking infrastructure

Sensors and actuators of the constrained IoT are typically challenged by maintaining an authenticated or even encrypted data channel to some remote data repository. In addition, unstable and lossy links in IoT edge networks make it hard to persist a stateful communication relation. Also for these reasons, IoT nodes are commonly deployed behind gateways that execute protocol translations (e.g., DTLS versus TLS) and thereby intercept secured channels. This sacrifices end-to-end transport security and exposes a significant attack surface at the gateway.

By authenticating or encrypting content instead of channels NDN circumvents these operational challenges of the IoT. As each content chunk can be hopwise replicated throughout the network without impairing its security measures, data integrity and confidentiality remain independent of transport or paths. Moreover, there is no requirement of performing synchronous actions between specific endpoints on the Internet which makes the security layer robust against link failures and network disconnects.

C. DDoS resistance

Constrained nodes on the low power lossy wireless are easy victims of resource exhaustion when receiving too many IP packets. A gateway may commonly shield the IoT nodes from the global Internet and may even perform some (general) rate limiting, but it cannot reasonably track individual resources of

nodes nor hinder the communication needs of the application use case. In addition, a malicious member of the IoT stub domain may not only jam radio channels, but utilize IP multihop forwarding to overload remote nodes. Conversely, as has been recently reported from the MIRAI incident, huge multiplicities make IoT nodes an interesting amplification tool for attackers.

A key design objective of ICN had been the reduction of this IP attack surface with respect to distributed denial of service attacks. In NDN this led to designing a request-response communication scheme without node addresses that hinders the plain transmission of unwanted content to a receiver. For a few years, it was the believe that NDN can be DDoS resistant by design, until Interest- and state-based attacks were discovered [17]. Subsequent work [18], [19] elaborated the threats of Interest flooding and overloading FIB and PIT structures by user-generated names and content requests. This has proven difficult to mitigate in general [20]. However, in a specific industrial setting of pure machine-to-machine communication with well known traffic patterns, buffers and PIT tables can be pre-configured according to well-formed communication flows. Hence, Interest flooding can be detected at the first hop and eliminated by the receiving stack (e.g., by hitting PIT limits). State-based attacks can thus be restricted to the local link which can never be protected by a network layer.

IV. COMPARATIVE ASSESSMENT

We are now ready to a qualitative security comparison of our ICN solution with the common IP-based protocols MQTT and CoAP. We also evaluate the complexity of content object security that is inherent to ICN, but for a quantitative performance analysis we refer to [21].

A. MQTT

MQTT is a message-based publish subscribe protocol, with a special focus on low bandwidth environments. A typical MQTT network involves a client that publishes data on a specific *topic*. Each topic is managed by a server (or *broker*) which distributes data about the topic to subscribers. By default, a message that has been published and distributed to the consumers by the broker is deleted after delivery. Different QoS levels allow for storing messages on the broker or advanced reliability on top of the transport protocol.

Low-end IoT devices are challenged by basic MQTT, as MQTT communicates over TCP. A lightweight version of MQTT is provided by *MQTT for Sensor Networks* (MQTT-SN) [22]. MQTT-SN is tailored to wireless domains and optimized for devices that are constrained in energy, processing, or storage. It is implemented on top of UDP and replaces topic strings by topic IDs to shorten messages.

In MQTT as well as MQTT-SN, security features depend on the broker implementation. Using username and password, or alternatively a client certificate, the broker may authenticate the client it connects to. If TLS (or DTLS) is used, the client may also authenticate the server. However, there is no end-to-end security support between publisher and subscriber. This threatens message integrity when the broker changes content, because subscribers do not have an out of the box mechanism to verify the content. To protect the payload, additional encryption efforts of application data are required on top of MQTT.

In general, MQTT assumes a trust relationship between broker, publishers, and subscribers. Usually, authentication and authorization is ignored completely, to simplify device management. This trust assumption reflects current deployment models, in which either brokers and clients are under the same administrative control, or where service contracts between end devices and a cloud network with broker service exist.

B. CoAP

The Constrained Application Protocol (CoAP) is standardized in the IETF with the aim for replacing HTTP in constrained deployment scenarios. CoAP operates on top of UDP and defines a compact protocol header. It specifies three communication schemes: (i) polling, (ii) push, and (iii) observe. Using push and observe, CoAP implements publish subscribe scenarios. In contrast to push, observe does not require explicit subscription in advance but delivers data to clients based on pre-configuration at the server side.

To enable M2M communication, CoAP implementations usually provide both client and server capabilities. Thus, without an explicit intermediary node such as a broker in MQTT, CoAP nodes may interact directly with each other.

The security support in CoAP is more advanced compared to MQTT, even though several specifications are still under discussion in the IETF. CoAP is secured on the transport layer using DTLS or alternatively on the application layer

TABLE I: Comparison of MQTT, CoAP, and ICN with respect to security measures.

	MQTT	CoAP	ICN
Ubiquitous caching	✗	(✓)	✓
Object security	✗	(✓)	✓
Name privacy	✗	(✓)	(✓)
Infrastructure protection	(✓)	✗	(✓)
End node protection	✗	✗	✓

using specific extensions such as OSCoAP, which allows for object security in CoAP. However, it is worth noting that DTLS might conflict with constrained environments as packet sizes increase. On the other hand, current approaches for object security may conflict with privacy as not all CoAP headers are encrypted and, for example, may reveal content names.

C. Comparing MQTT, CoAP, and ICN

Caching: Caching does not only improve performance in terms of faster data delivery but also increases data availability and robustness. A common malicious scenario includes a denial of service attack. With proper replication, the origin data source can go offline without loosing data in the global network. MQTT is easily threatened by this kind of attack because of the dedicated broker service. CoAP inherently supports caching on intermediary nodes. However, this mitigation is only implemented on the application layer. In common single stakeholder scenarios, where CoAP servers are managed by a single administrative domain, this usually does not help, in particular when network providers are under attack. ICN provides ubiquitous in-network caching that is independent of individual stakeholders. Thus, attacking a specific content source is intricate.

Reliability: IoT nodes connected via low-power wireless networks suffer severely from lossy communication channels. Even the transmission of small data chunks to the gateway is frequently impaired by unstable links, and transport protocols are challenged to cope with the unstable environment in a reliable fashion. We compare NDN, confirmable and non-confirmable CoAP (c/n), and MQTT (Q0/Q1) in Figure 2. The success rate of packet delivery was measured in two
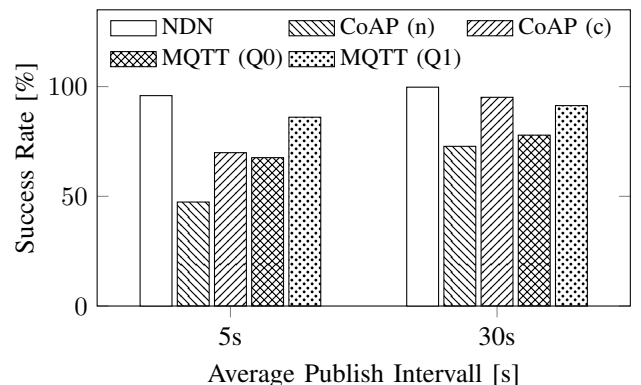

Fig. 2: Resilience of NDN vs. CoAP vs. MQTT.

large experiments of 50 nodes from the FIT IoT testbed at different publishing intervals. Low power lossy radios of the IEEE 802.15.4 standard were deployed with link-layer retransmissions set to four. Results clearly demonstrate the superior reliability of the hop-by-hop approach of NDN, while even the reliable variants of CoAP (c) and MQTT (Q1) fail significantly by 30 % resp. 15 % in the tighter scenario of publishing every 5 s. NDN always delivers more than 95 % of the packets, the success rate approaching 99.9 % in the more relaxed publishing at 30 s.

Object security: Security of content objects is crucial in inter-domain scenarios, in particular in the industrial Internet where sensors communicate sensitive information or actuators interact with critical infrastructure components based on data. Ideally, content can be forwarded by any node in the network without sacrificing security. MQTT and CoAP need additional efforts to achieve this objective. ICN, on the other hand, has been designed with democratized content distribution in mind. In-network caching is not limited to specific service nodes but envisioned to run on any network node that is willing to share resources for caching. Consequently, content security is a first principle in ICN, allowing multi-stakeholder scenarios with respect to scalable and secure content distribution. In ICN, trust is not based on contracts but technically provided by design.

Infrastructure protection: CoAP runs on top of UDP. As UDP is a connection-less protocol without congestion control, it can easily operate IP packet bursts and spoofing. Having IP spoofing in place, an attacker can initiate a reflective amplification attack, in which the attacker sends a small request towards the CoAP server that replies with a significantly larger packet to the victim (i.e., the spoofed IP address). Amplification attacks are common in the current Internet and a major threat for operators. With increased deployment of CoAP, we will experience more of such attacks in the future.

MQTT makes spoofing attacks much more challenging because of TCP. However, in MQTT-SN, TCP is replaced by UDP to reduce overhead on low-end IoT devices and thus opens up the identical attack surface. On the contrary, ICN abandons the end-to-end paradigm completely and provides de-localized services off the shelf.

End node protection: End nodes are not protected in MQTT and CoAP but may receive arbitrary amounts of unwanted data. Security extensions may enable authentication and authorization but protection against unsolicited traffic requires firewall extensions, either as infrastructure middleboxes, or as dedicated local software component running on the end node. The latter conflicts with constrained resources of low-end IoT devices. An industrial Internet benefits from ICN as ICN does not support end-to-end communication. It thus protects end devices against malicious traffic without additional overhead.

Name privacy: To comply with privacy requirements, obfuscating the requested content name in the content delivery infrastructure is important. Implementing this with low overhead and strong privacy protection is one of the most challenging tasks in content delivery scenarios, yet. Neither MQTT, nor
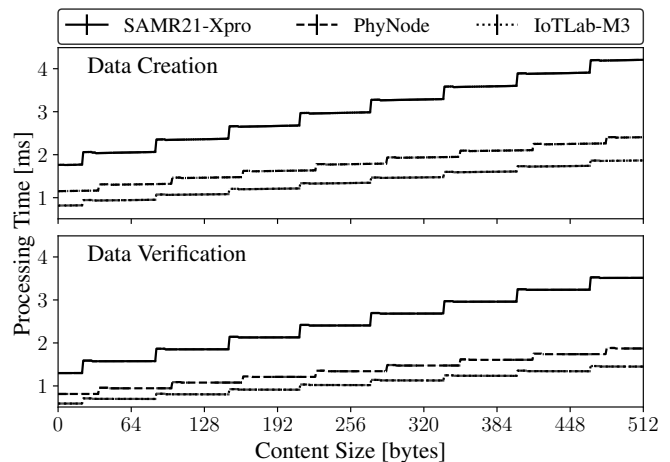

Fig. 3: Computational efforts for signing and verifying data with HMAC(SHA-256) on typical IoT nodes.

CoAP, nor ICN provide a solution out of the box until now. The hope here is that the ICN community will introduce a sufficient solution in the long-term because naming is a key component, which affects all applications on top of an ICN network layer.

D. Expenses of content security in ICN

The advantages of content object security in ICN comes at the price of signing resp. verifying every content chunk that traverses the network. In CCN/NDN, content signatures are usually generated from lightweight crypto hashes. In detail, each content chunk is hashed by SHA-256 followed by a keyed-hash message authentication code (HMAC). This message authentication is provided with our RIOT [23] version of CCN-lite, and we evaluated its performance in benchmarks on common IoT nodes. Figure 3 displays the runtime performance as a function of content size for three different IoT boards (running ARM Cortex M0, M3, and M4). Strikingly, the cost of few milliseconds per chunk is fully compliant with networking at the constrained nodes, which can send or receive a few packets per second at most. Limitations may derive from energy constraints, though. However, it is safe to conclude that signing and verifying of content is largely compliant to the constrained IoT.

HMAC runs with a pre-established secret, which in an automated environment requires a key management scheme. We devised a key distribution mechanism using identity-based cryptography that operates on elliptic curves. In detail, we implemented the twisted Edwards Curve 25519 in the Relic library on RIOT and compared with an existing short Weierstrass ECC on the Cortex M4 board running at 168 MHz. Figure 4 shows the runtime results for signature generation and verification of the key establishment that *needs to be performed only once*. Clearly, these asymmetric crypto operations are very expensive on our weak microcontroller with runtimes in the order of minutes. However, they are feasible and enable
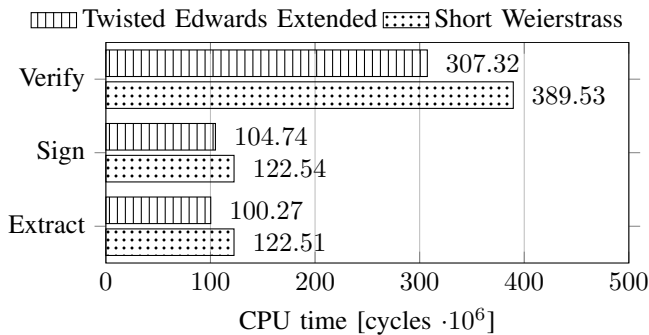
Fig. 4: Performance of identity-based elliptic curve cryptography on a PhyNode.

powerful schemes for autoconfiguration and self-management. Alternative schemes of lower complexity also exist.

V. Conclusion and Outlook

The industrial IoT connects safety critical environments to the Internet, requiring a high level of reliability and security for data, infrastructure, and end devices. Multiple stakeholders in this inter-domain communication challenge security, but current protocols in the IoT are weak in meeting these demands.

In this paper, we start from a real-world use case and derive a security perspective for an information-centric industrial Internet of Things. We argue three observations. First, data should be secured intrinsically, with respect to integrity and secrecy so that it can be transparently distributed and stored by any node in the network. Second, low-end devices as deployed in the IoT should be secured from unsolicited traffic to preserve resources such as battery power and processing. Third, the delivery infrastructure requires dedicated protection to increase data availability. ICN, which abandons the end-to-end paradigm and provides in-network caching, overcomes common attack vectors in the current Internet.

In future work, real-world deployment and experimentation is needed to evaluate and harden the contributions ICN can make towards a safe and secure industrial Internet of Things.

References

[1] B. Ahlgren, C. Dannewitz, C. Imbrenda, D. Kutscher, and B. Ohlman, "A Survey of Information-Centric Networking," *IEEE Communications Magazine*, vol. 50, no. 7, pp. 26–36, July 2012.

[2] V. Jacobson, D. K. Smetters, J. D. Thornton, and M. F. Plass, "Networking Named Content," in *5th Int. Conf. on emerging Networking Experiments and Technologies (ACM CoNEXT'09)*. New York, NY, USA: ACM, Dec. 2009, pp. 1–12.

[3] S. Y. Oh, D. Lau, and M. Gerla, "Content Centric Networking in tactical and emergency MANETs," in *2010 IFIP Wireless Days*. Piscataway, NJ, USA: IEEE, Oct 2010, pp. 1–5.

[4] E. Baccelli, C. Mehlis, O. Hahm, T. C. Schmidt, and M. Wählisch, "Information Centric Networking in the IoT: Experiments with NDN in the Wild," in *Proc. of 1st ACM Conf. on Information-Centric Networking (ICN-2014)*. New York: ACM, September 2014, pp. 77–86. [Online]. Available: http://dx.doi.org/10.1145/2660129.2660144

[5] W. Shang, A. Bannis, T. Liang, Z. Wang, Y. Yu, A. Afanasyev, J. Thompson, J. Burke, B. Zhang, and L. Zhang, "Named Data Networking of Things (Invited Paper)," in *Proc. of IEEE International Conf. on Internet-of-Things Design and Implementation (IoTDI)*. Los Alamitos, CA, USA: IEEE Computer Society, 2016, pp. 117–128.

[6] E. M. Schooler, D. Zage, J. Sedayao, H. Moustafa, A. Brown, and M. Ambrosin, "An Architectural Vision for a Data-Centric IoT: Rethinking Things, Trust and Clouds," in *IEEE 37th Intern. Conference on Distributed Computing Systems (ICDCS)*. Piscataway, NJ, USA: IEEE, June 2017, pp. 1717–1728.

[7] G. C. Polyzos and N. Fotiou, "Building a reliable Internet of Things using Information-Centric Networking," *Journal of Reliable Intelligent Environments*, vol. 1, no. 1, pp. 47–58, 2015.

[8] M. Amadeo, O. Briante, C. Campolo, A. Molinaro, and G. Ruggeri, "Information-centric networking for M2M communications: Design and deployment," *Computer Communications*, vol. 89–90, pp. 105 – 116, 2016.

[9] B. Mathieu, C. Westphal, and P. Truong, "Towards the usage of ccn for iot networks," in *Internet of Things (IoT) in 5G Mobile Technologies*. Cham, Switzerland: Springer, 2016, pp. 3–24.

[10] E. Baccelli, O. Hahm, M. Günes, M. Wählisch, and T. C. Schmidt, "RIOT OS: Towards an OS for the Internet of Things," in *Proc. of the 32nd IEEE INFOCOM. Poster*. Piscataway, NJ, USA: IEEE Press, 2013, pp. 79–80.

[11] A. Dunkels, B. Grönvall, and T. Voigt, "Contiki - A Lightweight and Flexible Operating System for Tiny Networked Sensors." in *Proc. of IEEE Local Computer Networks (LCN)*. IEEE Computer Society, 2004, pp. 455–462.

[12] W. Shang, A. Afanasyev, and L. Zhang, "The Design and Implementation of the NDN Protocol Stack for RIOT-OS," in *Proc. of IEEE GLOBECOM 2016*. Washington, DC, USA: IEEE, 2016, pp. 1–6.

[13] H. Bornholdt, D. Jost, P. Kisters, et al., "SANE: Smart Networks for Urban Citizen Participation," in *2019 26th International Conference on Telecommunications (ICT) (ICT 2019)*. Piscataway, NJ, USA: IEEE Press, April 2019.

[14] C. Gündogan, P. Kietzmann, T. C. Schmidt, and M. Wählisch, "HoPP: Robust and Resilient Publish-Subscribe for an Information-Centric Internet of Things," in *Proc. of the 43rd IEEE Conference on Local Computer Networks (LCN)*. Piscataway, NJ, USA: IEEE Press, Oct. 2018, pp. 331 – 334. [Online]. Available: http://doi.org/10.1109/LCN.2018.8638030

[15] A. Banks and R. G. (Eds.), "MQTT Version 3.1.1," OASIS, OASIS Standard, October 2014. [Online]. Available: http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/os/mqtt-v3.1.1-os.html

[16] Z. Shelby, K. Hartke, and C. Bormann, "The Constrained Application Protocol (CoAP)," IETF, RFC 7252, June 2014.

[17] M. Wählisch, T. C. Schmidt, and M. Vahlenkamp, "Bulk of Interest: Performance Measurement of Content-Centric Routing," in *Proc. of ACM SIGCOMM, Poster Session*. New York: ACM, August 2012, pp. 99–100. [Online]. Available: http://conferences.sigcomm.org/sigcomm/2012/paper/sigcomm/p99.pdf

[18] P. Gasti, G. Tsudik, E. Uzun, and L. Zhang, "DoS and DDoS in Named Data Networking," in *Proc. of ICCCN*. IEEE, 2013, pp. 1–7.

[19] M. Wählisch, T. C. Schmidt, and M. Vahlenkamp, "Backscatter from the Data Plane – Threats to Stability and Security in Information-Centric Network Infrastructure," *Computer Networks*, vol. 57, no. 16, pp. 3192–3206, Nov. 2013. [Online]. Available: http://dx.doi.org/10.1016/j.comnet.2013.07.009

[20] S. Al-Sheikh, M. Wählisch, and T. C. Schmidt, "Revisiting Countermeasures Against NDN Interest Flooding," in *2nd ACM Conference on Information-Centric Networking, Poster Session*, ser. ICN 2015. New York: ACM, Oct. 2015, pp. 195–196.

[21] C. Gündogan, P. Kietzmann, M. Lenders, H. Petersen, T. C. Schmidt, and M. Wählisch, "NDN, CoAP, and MQTT: A Comparative Measurement Study in the IoT," in *Proc. of 5th ACM Conference on Information-Centric Networking (ICN)*. New York, NY, USA: ACM, September 2018. [Online]. Available: https://conferences.sigcomm.org/acm-icn/2018/proceedings/icn18-final46.pdf

[22] A. Stanford-Clark and H. L. Truong, "MQTT For Sensor Networks (MQTT-SN) Version 1.2," IBM, Protocol Specification, November 2013. [Online]. Available: http://mqtt.org/new/wp-content/uploads/2009/06/MQTT-SN_spec_v1.2.pdf

[23] E. Baccelli, C. Gündogan, O. Hahm, P. Kietzmann, M. Lenders, H. Petersen, K. Schleiser, T. C. Schmidt, and M. Wählisch, "RIOT: an Open Source Operating System for Low-end Embedded Devices in the IoT," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 4428–4440, December 2018. [Online]. Available: http://dx.doi.org/10.1109/JIOT.2018.2815038