# On the Cost of Securing Information Centric Things

Marcel Enguehard
Cisco Systems & Telecom ParisTech
mengueha@cisco.com

Ralph Droms
Cisco Systems
rdroms@cisco.com

Dario Rossi
Telecom ParisTech
dario.rossi@telecom-paristech.fr

## ABSTRACT

Information Centric Networking (ICN) paradigms nicely fit the world of wireless sensors, whose devices have tight constraints. In this poster, we compare two alternative designs for securely onboarding new IoT devices in existing ICN deployments, which are based on asymmetric and symmetric cryptography respectively. While the security properties of both approaches are equivalent, an interesting tradeoff arises between properties of the protocol vs properties of its implementation in current IoT boards. Indeed, while the asymmetric-keys based approach incurs a lower traffic overhead (of about 30%), we find that its implementation is significantly more energy- and time-consuming due to the cost of cryptographic operations (it requires up to 41x more energy and 8x more time).

## 1. CONTEXT

Information Centric Networks (ICN) is gaining increasing attention in the Internet of Things (IoT) context [1], where devices are natural sources of information (sensor readings) or sinks (actuators actions). Benefits of ICN for IoT are for instance shown in [2], which carries on an experimental comparison of an almost out-of-the-box ICN stack vs a traditional IPv6 stack consisting of IEEE 802.15.4, 6LoWPAN and RPL.

Whereas in the context of fixed ICN networks, security is attached to self-verifiable data objects, we believe that the world of Information Centric Things (ICThings) requires additional security features. To begin with, given the broadcast nature of the wireless medium, in hostile environment silent attackers could eavesdrop on sensitive sensor data. Additionally, given the multi-hop nature of IoT communications, talkative attackers could instead swamp network resources, such as battery and wireless medium, by issuing bogus interest messages. It is in the interest of ICThings to provide additional security mechanisms, such as naming and communication patterns to enforce access control on ICN-based wireless sensor networks [3, 4].

ACM ISBN 978-1-4503-2138-9.
DOI: 10.1145/1235

In this poster we focus on a protocol for Information centric neighbour discovery and association, which ensures that only trusted things are authorized to send packets on the wireless network. We present a novel association protocol (in section 2) based on asymmetric keys and compare it to a recently proposed one based on symmetric cryptographic keys [4]. Our evaluation considers both security and network properties of these protocols, as well as important practical aspects such as the forecasted power consumption of the actual protocol implementation on different ICThings technologies.

We show that while asymmetric cryptography requires less ICN exchanges (about 30%), it is of one order of magnitude less efficient in terms of latency and energy-consumption due to the cost of cryptographic operations on constrained sensors. This is even true on sensors shipped with dedicated hardware for cryptographic operations.

## 2. THE DISCOVERY PROTOCOLS

In order to protect the network against intruders, sensors must be able to authenticate each other: we considered two different protocols, one based on symmetric cryptography and the other one on asymmetric cryptography.

**Symmetric Cryptography (SC).** As a reference point, we consider OnboardICNg [4], an ICN-based protocol that uses only symmetric cryptography (AES). Due to space constraints, we refer the reader to [4] for a description of the protocol. For our purposes, it is sufficient to point out that even though SC is not natively suited to authentication, it is several orders of magnitude less expensive in terms of CPU cycles than standard asymmetric cryptography [5], which makes it attractive for low-power ICThings environment. Additionally, there is a growing hardware SC support on recent sensor boards, which implies a shrinking energy footprint of cryptographic operations.

**Asymmetric Cryptography (AC).** We further design an ICN-based protocol that uses asymmetric cryptography, such as Elliptic Curve Cryptography (ECC). Compared to SC-based OnboardICNg, where every authentication session requires contact with an authentication server, AC allows nodes to authenticate each other without any third party. Local exchanges imply spatial reuse of the wireless medium, and also reduces the energy footprint due to relaying traffic toward the authentication server. This is especially critical for ICThings close to the authentication server that are more solicited and quickly deplete their batteries.

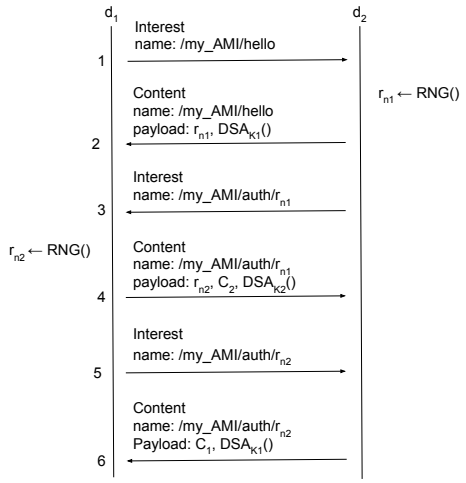


**Figure 1: ICN-based protocol for authentication using asymmetric cryptography**

At the same time, while asymmetric cryptography is rather commonly used in association with a public key infrastructure to perform authentication (e.g., in TLS), it however requires computationally expensive operations, which may not be a good fit for energy-constrained things.

Given that the design of an AC protocol with the same security properties as the SC-based OnboardICNg [4] is an original contribution of this work, we briefly sketch its inner working in fig. 1. In this scheme, each node $d_i$ has a pair of asymmetric keys $K_i$, with its corresponding certificate $C_i$ signed by a trusted third party (e.g., the authentication server). Signing a message with a key $K_i$ is noted as $DSA_{K_i}()$ and $RNG()$ is a random number generation function.To authenticate itself, a node must prove that it owns a key that has been certified by a trusted third party (messages 4 and 6). The nonces $r_{n1}$ and $r_{n2}$ protect the protocol against replay attacks by providing a challenge-response authentication. They can also be used to derive a symmetric session key, for instance with the Diffie-Hellman algorithm.

## 3. NETWORK VS ENERGY FOOTPRINTS

We estimate the footprint using two different sensors, an old-generation TelosB (with 16-bit MSP430 CPU) and a new-generation OpenMote (with 32MHz ARM Cortex-M3 CPU). As for AC, we consider ECC160 whereas we use standard AES-CCM for SC. Interestingly enough, the OpenMote supports both AES and ECC operations in hardware. We collect energy costs of cryptographic operations in table 1, that are instrumental for the performance evaluation. Specifically, we contrast (i) number of messages, (ii) energy cost and (iii) latency for both schemes in table 2.

On the one hand, we observe that only 6 messages are required in AC compared to 9 in OnboardICNg – a 30% reduction. Additionally, exchanges in the AC case are confined to neighbouring devices, whereas in the SC case messages need to reach a sink point (the authorization entity). Hence, not only does AC requires fewer messages, but these messages have shorter delay and involve less hops in the network. These are all desirable properties that make AC an interesting alternative to SC-based protocols such as OnboardICNg [4]. On the other hand, we also gather that cryptographic functions dominate latency overhead for AC — by about 8x. Similarly, and energy-wise the performances are largely favourable to OnboardICNg — up to 41x.

Given this very large performance gap, it follows that the advantages in terms of the network communication cost are completely offset by the large penalties in terms of latency and energy. Although negative, this finding is worth sharing: energy constraints still practically rule out the use of ECC from the ICThings world.

**Table 1: Cost of cryptography on the TelosB and OpenMote**

| ECC160-Sign (sw) **TelosB** | AES128-Encrypt (hw) **TelosB** | ECC192-SIGN (hw) **OpenMote** | AES128-Encrypt (hw) **OpenMote** |
|---|---|---|---|
| $15\,mJ$ [6] | $14.3\,\mu J$ [7] | $11.4\,mJ$ [8] | $0.9\,\mu J$ [8] |

**Table 2: AC vs SC-based authentication protocols**

| Board | Crypto | Messages (#) | Energy (mJ) | Latency (s) |
|---|---|---|---|---|
| TelosB | AES hw | 9 | 4.3 – 6.4 | 1.4 |
| | ECC sw | 6 | 53.3 – 57.3 | 10.9 |
| Open Mote | AES hw | 9 | 0.54 – 0.89 | 0.13 |
| | ECC hw | 6 | 22.5 – 28.7 | 0.95 |

## 4. NETWORK VS ENERGY FOOTPRINTS

We report (i) number of messages, (ii) energy cost and (iii) latency for both schemes in table 2.

In particular, note that only 6 exchanges are required in AC compared to 9 in OnboardICNg – a 30% reduction. Additionally, the 6 exchanges are in the SC case confined to neighbouring devices, whereas in the OnboardICNg case messages need to reach a sink point (the authorization entity). It follows that not only does AC requires fewer messages, but that these messages have shorter delay and involve less hops in the network. These are all desirable properties that make AC an interesting alternative to SC-based protocols such as OnboardICNg [4].

We next particularize the energy footprint using two ICThings technologies, namely an old-generation TelosB board (with 16-bit MSP430 CPU) and a new-generation OpenMote board (with a 32MHz ARM Cortex-M3 CPU). As for AC, we consider ECC160 whereas we use standard AES-CCM for SC. Interestingly enough, the OpenMote supports both AES and ECC operations in hardware. We collect energy costs of cryptographic operations in table 1.

It is clear that latency is dominated by cryptographic functions for AC, and that energy-wise the performances are favourable to OnboardICNg — by orders of magnitude. Although negative, this finding is worth sharing: from a practical perspective, energy constraints actually rule out the use of ECC from the ICThings world.

## Acknowledgements (ICThanks)

This work benefited from support of NewNet@Paris, Cisco's Chair "Networks for the Future" at Telecom ParisTech (http://newnet.telecom-paristech.fr). Any opinion, findings

or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of partners of the Chair.

## 5. REFERENCES

[1] Y. Zhang, et al. Requirements and Challenges for IoT over ICN. Internet-Draft draft-zhang-icnrg-icniot-requirements-01, 2016

[2] E. Baccelli, et al. Information centric networking in the IoT: Experiments with NDN in the wild. *In proc. ACM ICN*, 2014.

[3] J. Burke, et al. Secure sensing over named data networking. *In proc. IEEE NCA*, 2014.

[4] A. Compagno, et al. OnboardICNg: a secure protocol for on-boarding IoT devices in ICN, *In proc. ACM ICN*, 2016.

[5] H. Tschofenig and M. Pegourie-Gonnard. Performance of state-of-the-art cryptography on ARM-based microprocessors. *In proc. NIST Lightweight Cryptography Workshop*, 2015.

[6] G. de Meulenaer, et al. On the energy cost of communication and cryptography in wireless sensor networks. In *In proc. IEEE WMCNC*, 2008 .

[7] J. Lee, et al. The price of security in wireless sensor networks. *Computer Networks*, 54(17):2967 – 2978, 2010.

[8] H. Shafagh, et al. Talos: Encrypted query processing for the internet of things. *In proc ACM Sensys*, 2015.