Securing IoT Networking with ICN

Dhruti Lalaji Sawant (Matrikel Nummer: 5156829)

***Abstract*—Internet of Things (IoT) is connecting our physical world with the internet e.g. connected automibiles, e-Health, smart homes , industrial automation et cetera. Information-centric Networking (ICN) is a concept that changes the internet design which focuses on transmitting and accessing named content instead of the traditional host-based IP data. Several challenges present itself when we consider the dynamic infrastucture and deployment of IoT environment such as autoconfiguration of the names,enabling push traffic and minimising header size. However, the most significant chanllenge is to ensure the security and privacy of sensitive data transferred over the network.This report discusses the ICN-Iot middleware which provides a design level solution to the challenge of security and privacy in communication of data.**

I. Introduction

The Internet of things (IoT) is increasingly becoming part of our everyday life. Examples of IoT application markets are car-to-car communication, smart electricity grids and e-health systems. In order to protect the processed data and the privacy of the users, it is important to implement dedicated security measures in IoT devices and networks. Data in information-centric networking is delocalized and need not be retrieved via an end-to-end transport stream. Instead, hop-wise replication and in-network caching facilitate information dissemination in the IoT, and relax the demand for continued connectivity.

II. Networking in IoT

A. The Protocol stack in ICN

This is the protocol stack of the new internet paradigm ICN. Fig. 1.

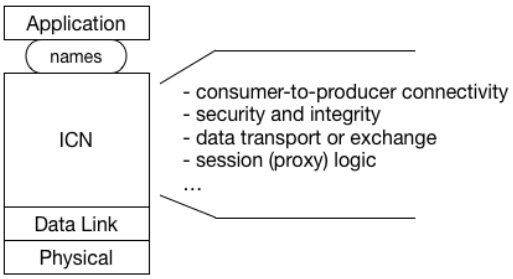

Fig. 1. Protocol stack

B. IoT Middleware architecture

The five components of the architecture:

1) Embedded system
2) Aggregator
3) Local Service Gateway(LSG)
4) ICN-IoT Server
5) Service/Consumer

Here is the middleware Fig. 2.

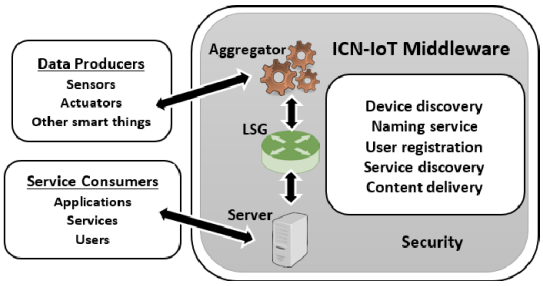

Fig. 2. Middleware architecture

III. Secure Functionalities

A. Secure device Discovery

B. Secure service Discovery

C. Secure naming service

D. User registration

E. Secure content discovery

IV. Discussion

It is not yet clear what the real world adaptation of this proposal will look like. Hence we need to look at other measures that would influce the securing of IoT networking.

V. Conclusions

For the last 35 years, the current internet system struggles with enabling a secure communication between hosts. It is therefore of utmost imprtance to ensure a proper security and privacy measures to be introduced in the early stages of network design. The ICN-IoT middleware architecture is a propasal that will ensure the security functionalities required for secure communication.

References

[1] Why IoT with ICN?. http://conferences2.sigcomm.org/acm-icn/2017/files/tutorial-ndn-ccnlite-riot/2-Why-ICN-for-IoT.pdf.

[2] Sabrina Sicari, Alessandra Rizzardi, Luigi Alfredo Grieco, Alberto Coen-Porisini. A Secure ICN-IoT Architecture. *IEEE International Conference on Communications Workshops (ICC Workshops)*, 2017.

[3] Mauro Conti,Giorgio Di Natale,Annelie Heuser,Thomas Pöppelmann,Nele Mentens. Do we need a holistic approach for the design of secure IoT systems?. *Proceedings of the Computing Frontiers Conference*, 2017.

[4] Emmanuel Baccelli,Christian Mehlis,Oliver Hahm,Thomas C. Schmidt,Matthias Wählisch. Information centric networking in the IoT: experiments with NDN in the wild. *Proceedings of the 1st ACM Conference on Information-Centric Networking*, 2014.