draft-icnrg-icniot-architecture-01.txt
IRTF/ICNRG, 99, Prague

Ravi Ravindran

(ravi.ravindran@huawei.com)

https://tools.ietf.org/html/draft-zhang-icnrg-icniot-architecture-01

Draft Authors

- Yanyong Zhang – Winlab, Rutgers
- Dipankar Raychaudhuri - Winlab, Rutgers
- Alfredo L. Greico - Politechnico De Bari
- Sicari Sabrina - Universita degli studi dell Insubria
- Hang Liu - The Catholic University of America
- Satyajayanth Misra - New Mexico State University
- Ravi Ravindran - Huawei
- G.Q.Wang - Huawei

Table of Content

Table of Contents

Draft History

- First presented in IETF 96
- This version revises the content considering research on the related topics in ICN-IoT

Goals of this draft

- Follows from the design considerations draft
  - draft-zhang-icnrg-icniot-01.txt
- The draft considers a typical IoT system architecture which are ICN based and middleware functions.
- We provide middleware function discussions required to achieve secure self-configuration and scalability to accommodate IoT devices.
- High level solution discussions as well as CCN/NDN and MF based specific middleware protocol solutions are discussed.

Draft Updates

- Section 1: on Strengths of ICN-IoT, changes mostly editorial
- Section 2: ICN-IoT System Architecture

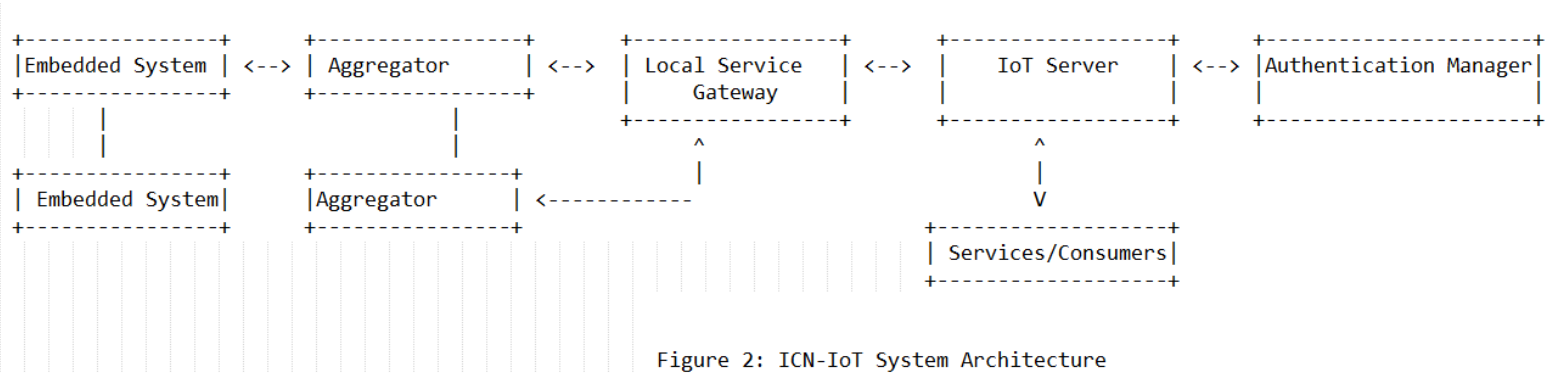

Figure 2: ICN-IoT System Architecture

  - Modified the architecture to include the Authentication Manager, which is a key component for on-boarding and validate their ES IDs at a system level
  - The AM can be co-resident with the LSG too.
  - Set up assumption is IoT application agnostic

Draft Updates

- **Section 4.1/4.2 : Device Onboarding and Discovery**
  - More discussion to the general steps involved here
    - New Device Polling
      - Device onboarding discussion, with or without authentication considering trust considerations. Also assigning a local ID (LID)
    - Mutual Authentication: Authenticating the network to the ES
    - Key Generation and Distribution
    - Protected Data Transfer
    - Discussion for both NDN and MF
    - Discussion when the ES is configured with Pre-shared Key (PSK) or an Assymetric Key
- **Section 4.3: Naming Service**
  - This discusses scenario when the ES has to be given a global name and not just a LID
    - If data is republished at the aggregator or the LSG, LID is enough
  - This follows once the device is authenticated, the name assignment is then secure.
  - The name can also be derived from the preloaded public key for self-certified ID or a URI with a binding key and certificate is offered to the ES using the naming service

Draft Updates

- **Section 4.4 : Service Discovery**
  - ES capabilities are learnt during the device discovery process
  - Here aggregators learn each others service capabilities
  - Secure Discovery discussion only by legitimate users
- **Section 4.5 : Context Processing and Storage**
  - Leverages ICN's in-network computing features
  - CCN/NDN has Named Function Networking and MF has its Compute Layer
  - Network needs to define set of contextual attributes at device function (ES, Aggregator, LSG), Device (interfaces, cache size, battery level etc.), Service level (Max, Min, Average)
  - Application contexts are then matched device/network/service level contexts to best meet the request.
  - These operations can be also be done at the application level, e.g. VMs, Containers etc.

Draft Updates

Section 4.6 Publish-Subscribe Management

- CCN/NDN being PULL based architecture doesn't naturally support PUB/SUB systems
- PUB/SUB approaches
  - Using long-lived Interests, Polling etc.
  - Other approach is long-term interests, Interest represent the flow hence not removed from the PIT.
  - Enhance the architecture, e.g. COPSS[1] introduces PUSH using a subscription table CCN/NDN
  - ICN designs that offer PUSH (like MF) can separate Data and Control plane by handling authentication and subscription information (such as service GUID or Group GUID) to the consumers and then the ICN network can push data to the subscribers
- User Registration
- Discussion on Secure Content Distribution
  - Symmetric Content Keys, Broadcast Encryption, Identity based cryptography

Section 4.7

- Security, covered mostly as part of the different middleware and content distribution functions

[1] Chen, J., Arumaithurai, M., Jiao, L., Fu, X., and K.Ramakrishnan, "COPSS: An Efficient Content Oriented Publish/Subscribe System.", ACM/IEEE Symposium (ANCS 2011) , 2011.

Draft Updates

- **Section 5.1 : Support for heteroegenous networks**
  - Inter-operability consideration between IoT systems in different ICN or IP domains
  - References InterNames[1] proposal as one of the ways to approach it
    - Here a crucial role is played by the Name Resolution Service (NRS), whose functionalities can decouple names from network locators as function of time/location/context/service, and provide ICN functionalities in IP networks.

[1] Blefari-Melazzi, A., Mayutan, A., Detti, A., and KK.Ramakrishnan, "Internames: a name-toname principle for the future Internet", Proc. of International Workshop on Quality, Reliability, and Security in Information-Centri cNetworking (Q-ICN), 2014.

Next Steps

- Comments from the chairs and audience on the next steps.