ICN-IoT

“draft-zhang-icn-iot-challenges-02.txt”
“draft-zhang-icn-iot-architecture-01.txt”

Ravi Ravindran
(ravi.ravindran@huawei.com)

IETF/ICN-RG -93, Prague

Draft Contributors

- draft-zhang-icn-iot-challenges-02.txt
  - Yanyong Zhang, (Winlab, Rutgers)
  - D. Raychadhuri (Winlab, Rutgers)
  - Alfredo Grieco (Politecnico di Bari (DEI))
  - Emmanuel Baccellli (INRIA)
  - Jeff Burke (UCLA)
  - Ravi Ravindran (Huawei)
  - G.Q.Wang (Huawei)
- draft-zhang-icn-iot-architecture-01.txt
  - Yanyong Zhang, (Winlab, Rutgers)
  - D. Raychadhuri (Winlab, Rutgers)
  - Alfredo Grieco (Politecnico di Bari (DEI))
  - Ravi Ravindran (Huawei)
  - G.Q.Wang (Huawei)

“draft-zhang-icn-iot-challenges-02.txt”

- The draft’s objective is to capture the IoT requirements, short comings of IP based realization, why ICN is a good candidate to meet those requirements.
- Specific ICN-IoT challenges are discussed and several scenarios also discussed to give a comprehensive view of the IoT landscape.
- From v-01 to v-02 Changes mostly editorial
  - Cleaning and Clarifying statements
- Swapped Sections 3&4, elevating the ICN-IoT challenges and pushing down the scenario discussions.
- More references included considering new emerging ICN-IoT projects in Smart Transportation/Smart Enterprise system, ref. to Bon Voyage project (Alfredo Grieco)
- Still awaiting updates from co-authors.
- More changes can be accommodated based on community feedback.

“draft-zhang-icn-iot-architecture-01.txt”

Table of Contents

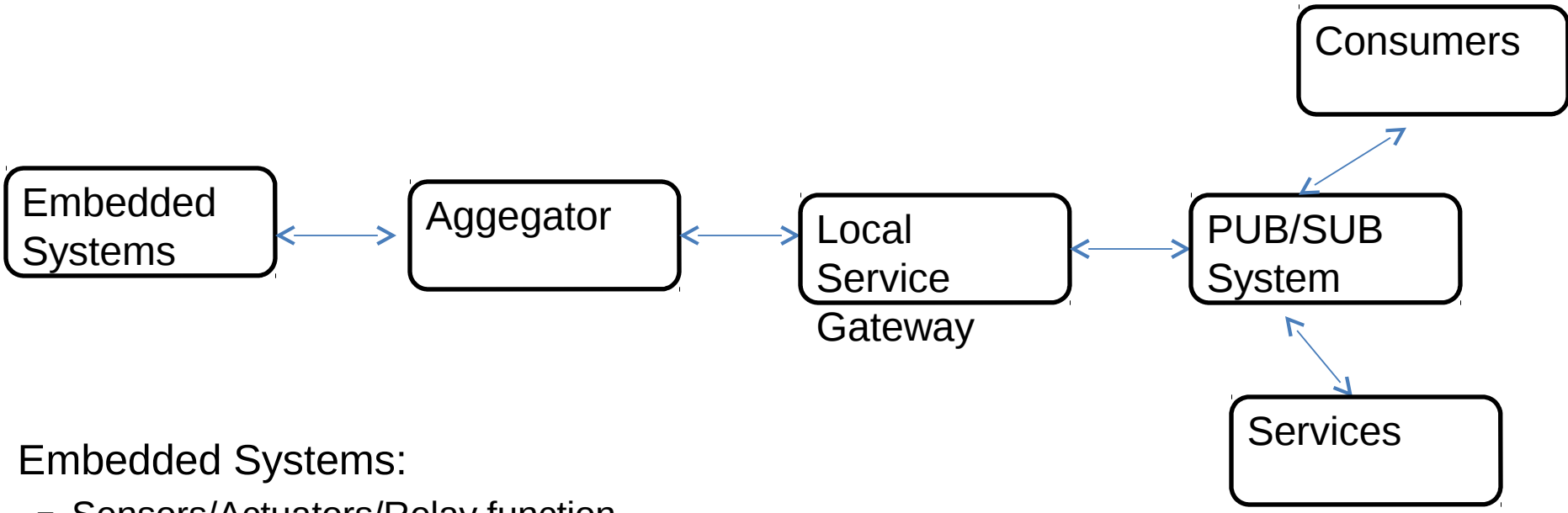
ICN Based Unified Platform for IoT

- Takes motivation from “draft-zhang-icn-iot-challenges-02.txt”
- ICN as a unified platform can efficiently inter-connect heterogeneous IoT systems, Home, V2V, Transport, Health etc.
- ICN Strengths
  - Persistent Names for IoT objects within certain scope/context.
  - Scalability – Content Distribution/local computing/Content Locality
  - Resource Constraints – Contextual delivery of data
  - Local Traffic Pattern – Localize service/content etc.

ICN Strengths

- Context Aware Communication – Associated with Consumers/Producers/Content/Service
- Consumer and Producer Mobility Handling
- Multiple levels of data Storage/Caching
- Content based Security and Privacy
- Communication Reliability
  - High Data Availability
  - Supports delay tolerant Communication
- Applicable to both Ad hoc and Infrastructure mode.

ICN-IoT System Architecture

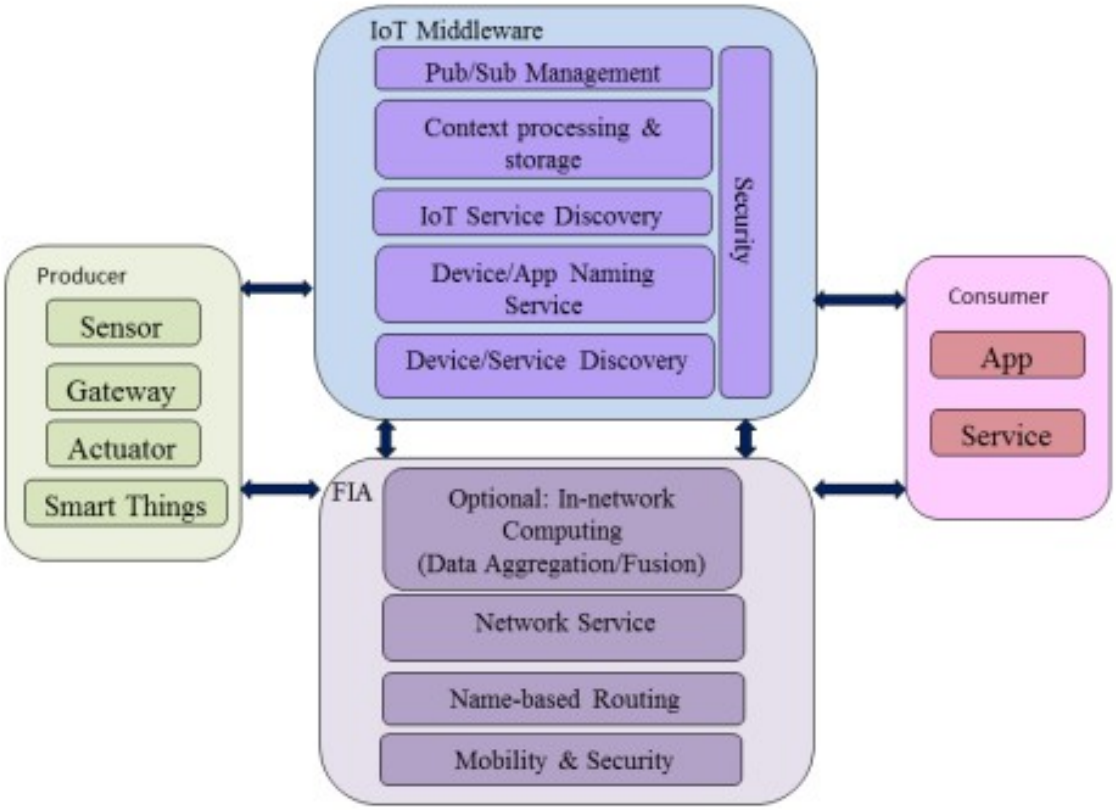


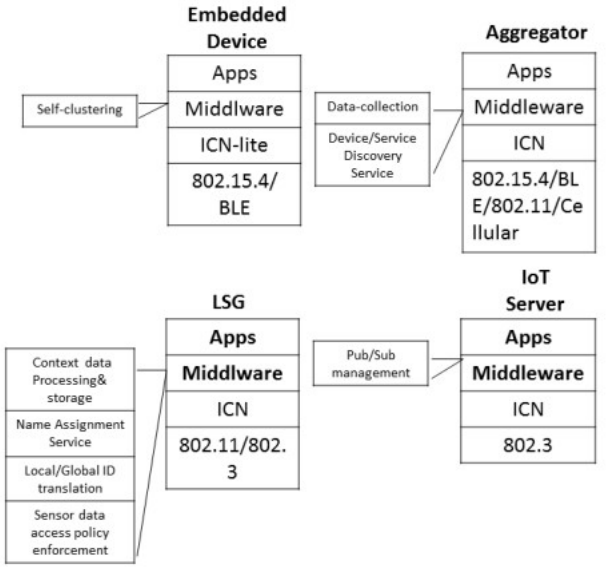
- Embedded Systems:
  - Sensors/Actuators/Relay function
- Aggregator:
  - Interconnects various IoT services in a local network
  - Bridges connectivity between resource constrained wireless sensors and infrastructure part the IoT network.
  - Could also integrate sensing and actuating services in the local network
- Local Service Gateway :
  - Bridges the local IoT services to the outside IoT Server
  - Local Naming and Translation from Global Names
  - Service Access Policies
  - Context Processing of data based on Server requirements

ICN-IoT System Architecture

- IoT Server
  - Centralized PUB/SUB System maintains mapping between IoT producers and the Subscribers of the service.
  - Name based networking, in-network computing, Caching allows scalable content distribution avoiding server bottlenecks.
- Services/Consumers
  - Instances interact with the IoT server to subscribed data.
  - Enables Heterogenous IoT service interaction

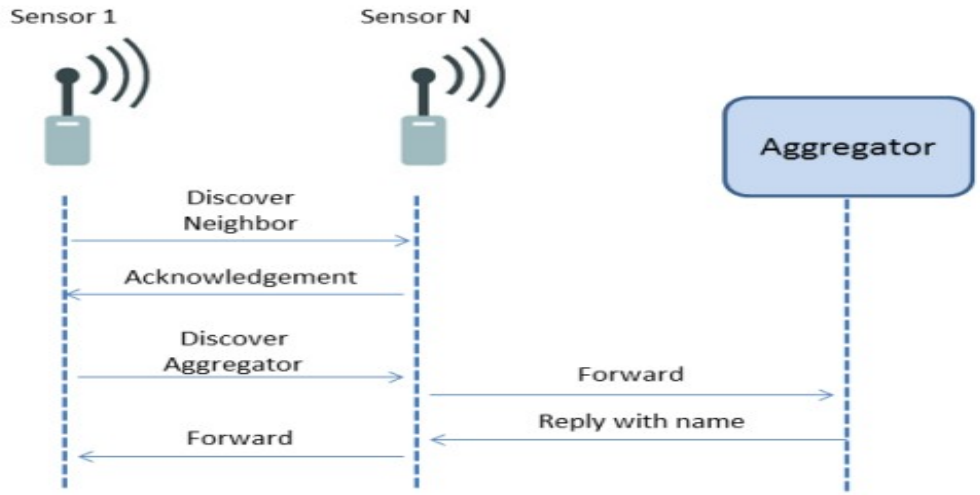
ICN-IoT Middleware Architecture





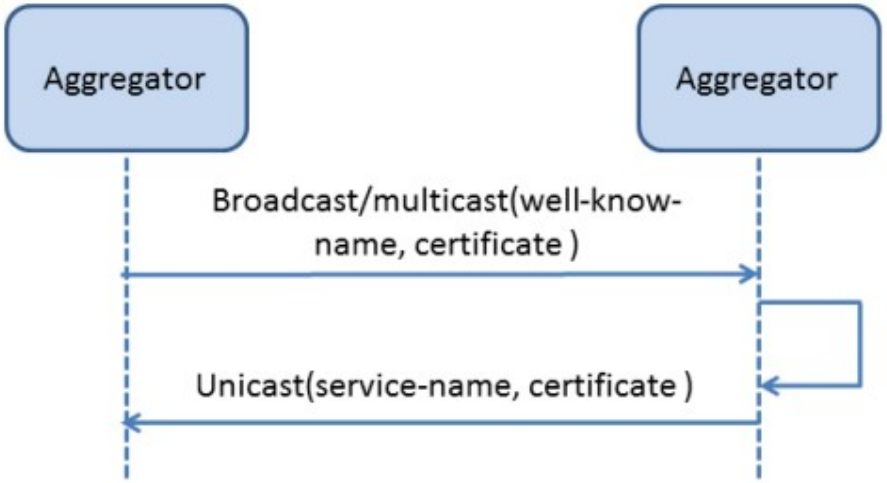
- ICN-IoT Middleware allows efficient inter-connection of distributed heterogeneous IoT services and devices in local and global scale.
- Bridges the gap between ICN functions and IoT applications, by enabling discovery, naming, data processing etc.
- Middlware functions are distributed among different system components.
- Requirements are heterogenous considering the IoT system, so challenge for the middleware functions is to meet these diverse requirements in terms of security, latency, service avaiability
- For each function in the draft, we define its purpose, how ICN networking helps, and solution discussion considering NDN/MF.

Device Discovery



- Contextual and Secure association of devices in proximity. Includes Discovery, Authentication and Naming.
- Application-centric device Discovery provides virtual separation among IoT devices belonging to multiple heterogeneous services
- Can be PULL or PUSH based, in PULL for e.g. the Aggregator broadcasts a well known name, also known to the IoT device. In PUSH, the IoT device announces its presense to the network.
- Discovery for Ad hoc Resource Constrained and Resource Rich devices require different considerations
  - Most likely the Resource rich devices will have direct reacheability to the local service gateway. Fo r resourc e constrained as in multi-hop sensor networks, the reacheability to the aggregator is through intermediate sensors or relay nodes.

Service Discovery



- Once the device is discovered and named. The service discovery is initiated.
- Service discovery is application-centric using well known names.
- Also secure service discovery using flat secure IDs can be enabled e.g. using Group Keys.
- The draft discusses Peer-to-Peer and Master-Slave modes of service discovery in the context of
- Peer-to-Peer is when two aggregators want to discovery each others service. Master-Slave is when a aggregator relies on other services, hence actively discovers them.

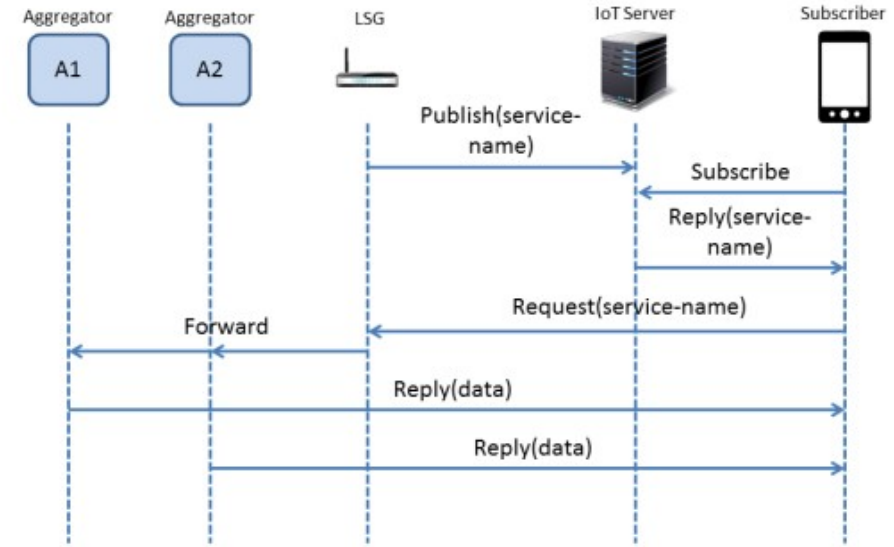
Naming Service

- Naming service assigns and authenticates sensor and device names.
- Naming service has to be secure to avoid any spoofing attack.
- Devices can be pre-loaded with some identity information (secureID, Keys, Certificate) from the owner or the manufacturer
- During device discovery, the device contacts the gateway service with its pre-loaded device ID and signature. The LSG generates a new name, and binds this name to its public key with a certificate.
- For resource constrained devices, the Aggregator can be a trusted service proxy to the device. In this case another name can be assigned locally by the Aggregator.
- For devices with only device-ID, other contextual information can be used to authenticate the device, before issuing it a name. Other trust models like web-of-trust can also be applied.
- Further for resource constrained devices, light weight crytographic primitives like symmetric cryptography can be used.

Context Processing and Storage

- Leverage in-networking computing and storage feature of ICN to process IoT data at multiple levels.
- Context processing is specified by individual applications, and therefore, scenario specific, and no uniform protocol can be specified.
- For Context processing of IoT data, key requirements include
  - First, the unconstrained part of ICN-IoT needs to have means to expose sensor/device context information to the rest of the system, such as its location, information semantics.
  - Second, the IoT server needs to allow applications to specify their contextual requirements.
  - Third, the unconstrained part of ICN-IoT needs to be able to map the higher-level application-specific contextual requirements to lower-level device-specific contextual information.
  - Fourth based on the higher level requirements and lower level measurement, context processing can be applied at the aggregator, LSG, and the IoT server before dessiminating it to the consumers.

PUB/SUB System



- Is responsible to inter-connect the IoT informaton producers to consumers. In addition it applies polies to information dissemination.
- Many Pub/subs models are possible, two are discussed:
- **Data-Control Separation mode**, here there is no PUB/SUB state in the forwarding plane. The IoT server assigns group names for resources and pushes the information to the LSG and the Consumers. Then the producers can push the updates to the consumers, or in NDN, consumers can PULL on partial names.
- **Randezvous Mode**: where forwarding plane maintains a data structure of “content descriptors” from consumers [COPSS], in the context of NDN. The IoT server exposes the Randezvous Service, Consumers can Subscribes to topics, and content is PUSHED to them.

[COPSS] Jiachen, C., Mayutan, A., Lei, J., Xiaoming, Fu., and KK.Ramakrishnan, "COPS
An efficient content oriented publish/subscribe system", ACM/IEEE ANCS, 2011.

Summary

- More detailed discussion in the draft on the middleware components.
- Researchers in this space are welcome to contribute to this draft.