ICN based Architecture for IoT-
Requirements and Challenges
(updated portion only)

(draft-zhang-iot-icn-challenges-00.txt)

IETF-91
IRTF/ICNRG, Honolulu

G.Q.Wang and Ravi Ravindran
(Huawei, USA)
ICN-IoT Draft Updates

• The draft was split to encourage participation:
draft-zhang-icn-iot-architecture-00.txt

draft-zhang-icn-iot-challenges-00.txt

Main Sections:
• IoT Application Scenarios and Challenges.
• IoT Requirements
• State of Art
• ICN Challenges for IoT

Main Sections:
• ICN-IoT as Unified Platform
• ICN-IoT Architecture
• ICN-IoT Service Middleware
• ICN-IoT Deployment
Contributors

• WinLab @ Rutgers U
  – Prof. Yanyong Zhang, Prof. Dipankar Raychadhuri
• Politecnico Di Bari
  – Prof. Alfredo L. Grieco
• INRIA
  – Prof. Emmanuel Baccelli
• UCLA
  – Prof. Jeff Burke
• Huawei
  – Ravi Ravindran & G.Q.Wang
1. IoT Motivation .................................. 3
2. IoT Architectural Requirements ............... 4
   2.1. Naming ..................................... 4
   2.2. Scalability ................................. 4
   2.3. Resource Constraints ....................... 4
   2.4. Traffic Characteristics ...................... 5
   2.5. Contextual Communication ................. 5
   2.6. Handling Mobility .......................... 6
   2.7. Storage and Caching ....................... 6
   2.8. Security and Privacy ....................... 7
   2.9. Communication Reliability ................. 7
   2.10. Self-Organization ......................... 7
   2.11. Ad hoc and Infrastructure Mode .......... 8
   2.12. Open API ................................. 8
# Table of Content

3. State of the Art ........................................ 8  
   3.1. Silo IoT Architecture ............................ 9  
   3.2. Overlay Based Unified IoT Solutions ........... 9  
       3.2.1. Weaknesses of the Overlay-based Approach .... 10  
4. Popular Scenarios ................................. 11  
   4.1. Homes ........................................ 12  
   4.2. Enterprise .................................... 12  
   4.3. Smart Grid ................................... 13  
   4.4. Transportation ................................. 13  
   4.5. Healthcare .................................. 14  
   4.6. Education ................................... 15  
   4.7. Entertainment, arts, and culture ............... 15  
5. ICN Challenges for IoT ............................ 16  
   5.1. Naming ....................................... 16  
   5.2. Caching/Storage ............................... 17  
   5.3. Name Resolution ............................... 17  
   5.4. Contextual Communication ...................... 18  
   5.5. Routing and Forwarding ....................... 18  
   5.6. In-network Computing ......................... 19  
   5.7. Security and Privacy ........................... 20  
   5.8. Energy Efficiency .............................. 21  
6. Informative References ......................... 21  

Modified Section since ICN-RG meeting in Paris
Section- 5 : ICN Challenges for IoT

[Changes to this Section]

• Section aims at Scenario specific ICN-IoT challenges.
• Generally all the IoT requirements listed are met by ICN.
• But IoT requires special considerations considering different scenarios with context, such as
  – Heterogeneity of devices,
  – Interfaces,
  – Constrained factors,
  – Data processing,
  – Content distribution models,
  – Self organization
Naming and Name Resolution: requirement

- **Naming**
  - Scalability due to large number of entities
  - Trust in name assignment/Chain-of-trust
  - Deployability and Inter-operability: Between IP and ICN-IoT platforms, and also between various ICN-IoT realms based on different architectures.
  - Constructible Names Versus On-demand Publishing

- **Name Resolution**
  - Scalability and mobility
  - Latency: for real-time, delay-sensitive M2M applications
  - Locality and Network efficiency: faster local resolution, actuation due to ICN-IoT feedback systems for smart grids, industrial plants etc.
  - Agility: particularly in dynamic environments like VANET
  - Control/Scoping: Particularly to address Privacy, e.g. health monitoring
Naming and Name Resolution: scenario specific challenges

- Smart Homes
  - Names to enable local/wide-area networking
  - Security/Privacy/Access control
- Smart Grids
  - Consideration include to allow network control loops, real-time control, and security
- Smart Transportation
  - Handle extreme mobility, short latency, and security
- Smart Campus
  - Efficient naming for resource/service ownership and interconnection among various heterogeneous sub-systems.
Caching and Storage: requirement

- Where to cache: Caching in constrained versus unconstrained part of the network. Latter is an open problem.
- What to cache: considering Streams of data. Caching Pub/Sub information in intermediate routers.
- Caching in the context of actuation, little meaning for authenticated requests, e.g. BMS
Caching and Storage: scenario specific challenges

- Smart homes could use caching in gateway to access content.
- Smart Grids usage of caching to backup valuable data
- Transportation systems may implement in-network caching on vehicles for efficient information dissemination
- Smart Campus for social interaction and efficient content access.
Routing and Forwarding: requirement

- Can be classified into two categories
  - Direct and Indirect name-based routing

- Direct Name-based Routing
  - More challenging with flat names have be handled
  - Hierarchy gives natural aggregation
  - Challenges with producer mobility

- Indirect Routing
  - Uses a name resolution system to derive locators
  - Static Binding versus Dynamic Binding, later requires router to handle name-based routing
Routing and Forwarding: scenario specific challenges

- **Smart Homes**: Need support for intra-domain and inter-domain routing protocols, e.g. service reachability within or access from outside too.
- **Smart Grids**: Robustness and Resiliency, and timely delivery or data.
- **Smart Transportation**: Satisfy V2V Ad hoc communication requirements
- **Smart Healthcare**: Timely and dependable routing and forwarding
- **Smart Campus**: Inter-domain routing protocols with minimal latency.
Contextual Communication: requirement

• Intelligence information gathering for Self-Configurability
• Contexts that can be processed in the network layer
• Approaches to handle context: Naming enhancement to signal context, and retrieve content objects
• ICN-IoT Middleware to process information
• Trust related challenges
• Real-time context processing
• Challenges as the Contexts and Devices grow
Contextual Communication: scenario specific challenges

- Smart Home: Many contexts depending on application such as temperature, location, time, number of occupants etc.
- Smart Grid: depends on specific segment of the grid being considered, e.g. location, time, voltage fluctuations etc.
- Smart Transportation: Many contexts which were highly dynamic, location, time, # of vehicles, speed etc.
- Smart Healthcare: Context can be used to enhanced care, particularly during emergency situations.
- Smart Campus: Many systems inputs different contexts, hence have to be dealt differently.
In-Network Computing: requirement

- Host heterogeneous Services for network and service specific tasks.
- Meet security requirements, e.g. access control
- Context support requires in-network computing
- Process context reasoning
- Filtering noisy data, particularly for streaming data from sensors.
In-Network Computing: scenario specific challenges

- Smart Homes: Hosted on home gateways to resolve contexts
- Smart Grids: Increase the scalability and efficiency of the system
- Smart Transportation: to enable reliable and efficient communication between vehicle and infrastructure services
- Smart Healthcare: Resolve contexts, security, and improve dependability
- Smart Campus: Process Contexts from different applications.
Security and Privacy

Security and Privacy Challenges:
• Crucial to all IoT applications
• Challenges span confidentiality, integrity, authentication and non-repudiation, and availability
  – Security related processing considerations for constrained devices with very low processing and memory footprint.
  – Infrastructure – Naming by trusted entities, Protection of resources from adversaries, Man in the middle attacks involving message tampering, e.g. sensor data resulting in performance degradation of network services.
• Considerations towards network functions like Naming/Name Resolution/Caching/Routing

Scenario Specific Challenges
• Most concern about Privacy, other than ensuring entities producing and consuming information are authenticated and trustworthy.
Energy Efficiency: requirement

• Fundamentally determined by the previously discussed components.
• Trade-offs have to be analyzed specifically for each scenario based on their objectives such as performance requirements, reliability, availability etc.
Comments and Suggestion

• Draft contributions from members are welcome.
Back UP
Section 1: ICN-IoT Motivation

• Device Heterogeneity
  – Things connection to the Internet
    • Personal, Industrial, Vehicles, Sensors etc
  – Potentially 50-100B Networked Objects

• Connectivity Heterogeneity
  – Wifi/802.15.4/BT/4G/5G

• Service Heterogeneity
  – Devices of all kinds offering different services
  – Hierarchical Service Realization – Collection/Aggregation/Processing/Distribution

• Unified Platform
  – Need for a Unified Platform to allow interaction at all levels
  – Device/Service/Control/Management Plane level

• ICN can be a future Unified Platform
Section -2: IoT Architectural Requirements

- **Naming**
  - Requirement driven due to Application requirements, Secure/non-Secure, Persistance considering context changes such as Mobility or Scope

- **Scalability**
  - Due to Naming, Security, Name Resolution, Routing/forwarding aspects of the system design
  - Scale to billions on devices (passive/active), name/locator split, local/global services, resolution infrastructure, efficient context update.

- **Resource Constraints**
  - Resource constrained and sufficient devices
  - Power/Compute/Storage/Bandwidth constrains and how it affects resource constrained device operations.
  - User interface constraints with the users.

- **Traffic Characteristics**
  - Separate Local versus Wide Area traffic based on Application logic; Many-to-Many (Multicasting/Anycasting)
  - Requirement for efficient means for data aggregation service discovery, resolution, and association. Optimize for bandwidth/enery consumption for uplink/downlink communication. Provisioning requirment considering Traffic shaping needs.
IoT Architectural Requirements

• **Contextual Communication**
  • Requirements to support Contextual interaction based on location, physical proximity among devices, time, cross-contextual considerations.
  • Driven due to Short and Long term Contextual needs of applications.

• **Handling Mobility**
  • Movement of Static Assets versus very dynamic V2V environments
  • Requirements due to Data Producer/Consumer/IoT Network mobility; Disconnection between data source and destination pair (unreliable wireless link). Meet application requirements.

• **Storage and Caching**
  • Linked to privacy and security of requirements of IoT applications.
  • Pervasive versus Policy driven requirements for storage and caching
  • Requirement on efficient resolution of cached content while adhering to policy requirements

• **Security and Privacy**
  • Trust Management, Authentication, Access Control at different layers of the IoT system
  • Privacy related to both Content and Context of its generation.
IoT Architectural Requirements

• Communication Reliability
  – Requirement considering mission critical, and non-mission critical applications
  – Implication on QoS, Routing, Context, and System Redundancy (device, storage, network etc.)

• Self Organization
  – Able to self organize – discovery or heterogenous and relevant devices/data/services based on context.
  – Scalable Platform to support pub-sub services while supporting mobility, in-network caching, name-based routing.
  – Private Grouping/Clustering based on privacy and security requirements.

• Adhoc and Infrastructure Mode
  – Devices could operate in either of these modes
  – Energy efficient topology discovery and data forwarding in adhoc mode and scalable name resolution in infrastructure mode.

• Open-API
  – To foster large scale inter-operability in terms of Push/Pull/Pub-Sub operation between consumers, producers, and IoT services.
Section-3: Legacy IoT systems

• Silo IoT Architecture: (Fragmented, Proprietary), e.g. DF-1, MelsecNet, Honeywell SDS, BACnet, etc.
• A small set of pre-designated applications.
• Moving towards Internet based service connectivity (ETSI, One M2M Standards).

Vertically Integrated
Section-3: State of the Art

- Internet Overlay Based Unified IoT Solutions, inter-connecting multiple publishers and consumers
- Coupled control/data functions
- Centralized and limits innovation
Section 3- Weakness of the Overlay Approach

• System not designed in a holistic manner to inter-connect heterogeneous devices, services, and infrastructure.

• Relies on IP for transport which has inherent weakness towards supporting a unified system.

• Cannot satisfy many requirements:
  – Naming : Resources coupled with IP address
  – Security : Channel based security model, inflexible trust models
  – Scalability – Using IP addresses as identifiers; affect on routing table size. Lack of unified application level addressing and forwarding.
  – Resource Constraints : Push versus Pull
  – Traffic characteristics – point to point, requirement for multicast
  – Contextual Communication, as all the information is at the server
  – Mobility – Session based
  – Storage and Caching
  – Self Organization
  – Ad hoc and Infrastructure mode
Popular Scenarios

• For each of the these scenarios, we discuss the general and IP based overlay challenges.

• **Home Challenges**
  – Topology independent service discovery
  – Common protocol for heterogenous device/application/service interaction
  – Policy based routing/forwarding
  – Service Mobility as well as Privacy Protection
  – Inter-operate with devices with Heterogenous naming, communication and Trust models
  – Ease of use
  – Foreign Devices
Section -4: Popular Scenarios

• Enterprise
  – Campuses, industrial facilities, retail complexes
  – Complex environments which integrate business and IT systems
  – H2M, M2M interaction
  – Efficient secure device/data/resource discovery
  – Inter-operability between different control systems
  – Reliable communication
Section-4: Popular Scenarios

• **Smart Grid**
  
  – Data flow and information management achieved by using sensors, actuators enabling substation and distribution automation
  
  – Challenges include reliability, real-time control, secure communication, and data privacy
  
  – Scale to large number of heterogenous devices
  
  – Real time data collection, processing, and control
  
  – Resiliency to failures
  
  – Critical infrastructure hance security in terms of malicious attacks, intrusion detection and route around failures
Section-4: Popular Scenarios

Transportation

– Increasing sensors in vehicles in general
– Networking in-vehicle network/applications with external network/services for safety, traffic conditions, entertainment etc
– Challenges span: Fast data/device service discovery and association, efficient communication with mobility, trustworthy data collection and exchange, inter-operability with heterogenous devices, security.
Section 4- Popular Scenarios

• Healthcare
  – Realtime interaction
  – High reliability and strict latency requirements
  – Trust, Security, Privacy and Regulations
  – Heterogeneous devices and Inter-operability

• Education
  – How IoT systems can enhance learning about environments with increasing instrumentation of environments
  – Simplying communication between devices, applications and services, moving away from host oriented approaches
  – Security
  – Real-time communication
  – Heterogenous devices, manufacturers, and siloed approach limits innovation

• Entertainment  Arts and Culture
  – Integrating multiple smart systems to create new experiences
  – Time synchronization
  – Simplicity for experimentation and development
  – Security
Thank You