ICN Research Group
Internet-Draft
Intended status: Informational
Expires: August 17, 2014

R. Ravindran
A. Chakraborti
G. Wang
Huawei Technologies

February 13, 2014

Contextualized Information-Centric Home Networking
draft-ravindran-cibus-homenet-01

Abstract

Home network (Homenet) is a good application scenario for ICN considering it is a point where diverse users, devices, applications, and services meet. Homenets are getting increasingly complex with the presence of application specific sensors, smart appliances, and smart networking devices such as residential gateway. Home automation today is being driven by several alliances such as DLNA, AllJoyn, ZigBee, and Z-Wave aimed at supporting homenet services such as multimedia sharing, lighting control, climate control, and energy management. These standards overlay application semantics over a host centric architectures which is inefficient, and the lack of inter-operability among these standards results in high cost, inflexibility, and management issues. Homenet is an information-centric environment where the objective is to enable consumers and producers to interact in a contextual manner independent of their underlying topology arrangement. Although the overall homenet objectives over an ICN framework versus any other are the same; ICN can distinguish itself by providing a rich service abstraction layer applicable in local scale as in BAN/PAN/LAN, and also enable intelligent interaction beyond the homenet boundary.

In this draft we share the idea of a contextualized information-centric bus (CIBUS) which builds on ICN abstractions of naming, name resolution, and content dissemination for home network by providing support for service management, context processing and monitoring, policy management, and policy based routing and forwarding. CIBUS allows applications and services to discover each other, subscribe/notify to event upon which service composition can be realized locally or in a centralize manner. Furthermore, service policies can be applied at high granularity which can be imposed in the routing and forwarding plane through ICN extensions. Some of these CIBUS features that were realized in [5] is presented here.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

During the past decade, many standalone Internet of Things (IoT) systems have been developed and deployed in different application domains such as homenets, smart grid, smart transportation, and health care. Home networks will see continuous evolution in this regard, as users introduce heterogeneous devices to access various services ranging from well known ones like entertainment, climate control, security surveillance to more personal conveniences like digitization of wine cellars etc. The requirements in this case is diverse, ranging from accommodating diverse devices, radio interfaces, service requirements, and policy control. Here we propose CIBUS, which leverages ICN semantics to allow seamless interaction among devices and services while being contextually sensitive to realize residents requirements for service composition and strict policy control.

2. Homenet Challenges

Several studies, such as [4][3], have elaborated home automation challenges, important ones include:

1) Historically, the cost of installation and maintenance deter any incremental addition of new services, economy of scale through mass technology adoption shall address this.

2) Complexity due to variety of standards and lack of inter-operability of devices where the services may have to hop between multiple protocols requiring gateways to handle protocol translation functions, standardization on a single application-centric platform leveraging cheap computing, caching, and storage that meets heterogenous requirements is the need here.

3) Poor manageability in terms of customizing services to user requirements due to complex realization of the home automation systems particularly if heterogeneous systems are in place, addressing (1) and (2) shall make this feasible.

Though these are subjective concerns, the underlying technology determines how efficiently these challenges are addressed, towards this ICN has a unique opportunity to show its value where features

like name based routing augmented with contextual expression, and leveraging distributed caching/computing resources shall address these challenges uniquely under an ICN paradigm.

Considering these challenges, following are requirements for a homenet:

2.1. Agile Service Management

Homenet services are hosted by heterogeneous devices and connectivity that generate information with different policy management requirements. Hence, services can be dynamically configurable in terms of related parameter such as scope of reachability, service lifetime, and accessibility by users or by other services anytime during its lifetime. Furthermore, services shall be able to leverge each other, hence service composition among multiple services shall be integral to the design and realiazable with minimum overhead while adhering to individual service policy requirements. Also flexibility is required to introduce services dynamically in a homenet such as by the home operator or ISP or by a third party, with its own policy requirements.

2.2. Self Configuration

Considering the heterogeneity of devices and naive home users, homenet platform is expected to be a zero configuration environment with auto- node and service discovery to simple management interface for service composition with little human interventation. Self-configuration shall be achieveable in ad hoc or infrastructure envrionments. Infrastructure managment support is required particularly for global service reachability. Furthermore, self healing due to wireless or network layer impairment by taking advantage of multi-path routing and caching in the homenet shall preserve user QoE even during network disruptions.

2.3. End-to-end Homogenous Platform

To support a heterogeneous device environment, a platform which can accommodate disparate devices, radio connectivity, and protocol semantic for information exchange is required. The platform itself shall be amenable to diverse conditions such as for both unconstrained and constrained segments while supporting different modes of communication such as M:M, 1:M, and M:1. Further the platform shall also be extendible to enable access to services inside or outside the homenet.

2.4. Mobility Support

Mobility support for both service producers and consumers is required to ensure best connectivity at all times, particularly in a setup with multiple access points in a home network to maximize signal quality. Hence, support for mobility includes session continuity inside home and due to vertical handovers between different access networks as residents and non-residents move in and out of their home premise. For mobility support for homenet services inside the home premises the ISP may be involved.

2.5. Security and Trust

Trust and security is application specific. Specifically in a home scenario considering the heterogeneity which may also include untrusted devices this consideration apply at application, service, device, and content level. Information generated by producers inside homenet is expected to be private hence subjected to strict access control, this particulaly is very important when home services interact with third party applications outside the home domain.

3. State of the Art

Over the years, many stand-alone homenet solutions have emerged. These systems usually adopt a vertical silo architecture and rarely satisfy the above requirements. A recent trend, however, is to move away from this approach, towards a unified homenet platform in which the existing silo IoT systems, as well as new systems enable data and service accessiblity through the general Internet applications. Most of these systems rely on IP to interconnect devices hence relying on host-centric model even though data is shareable, or context changes can be handled locally without involving external centralized systems. Some of these systems include IETF’s Homenet effort [2] which is based on IPv6 and AllJoyn [1], DLNA alliance with abstraction layers over IP. These systems try to evolve existing frameworks missing out intelligence available through in-network computing and caching, expoliting multi-path routing, or name based security features. These features are core to ICN, which can enable the vision of a of self-organizing homenets.

4. CIBUS Based Homenet

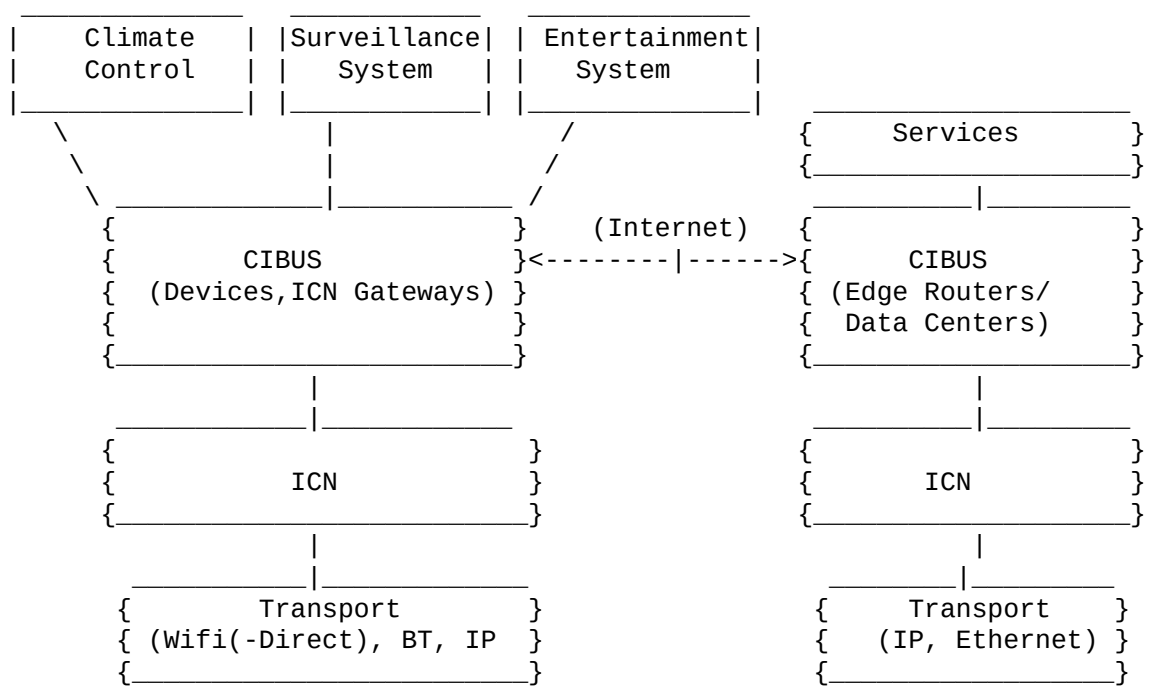

Figure 1: CIBUS as generic service platform

A high level view of CIBUS is shown in Fig. 1. CIBUS serves as a BUS for heterogenous consumers and services to interact and exchange information. It primarily enables a service management layer spanning the home network, and extending into the Internet, i.e interacting with edge service routers [6] or services in the data centers. CIBUS is a generic framework which needn't be just restricted to a home network, but span other ecosystems such as smart grids, smart transportation too. CIBUS shall support several service functions, shown in fig. 2, such as name management, auto- node and service discovery, context expression and monitoring, and policy-based service publishing and subscription. Depending on ICN functions, functions like content discovery can be features enabled through CIBUS or part of ICN layer itself.

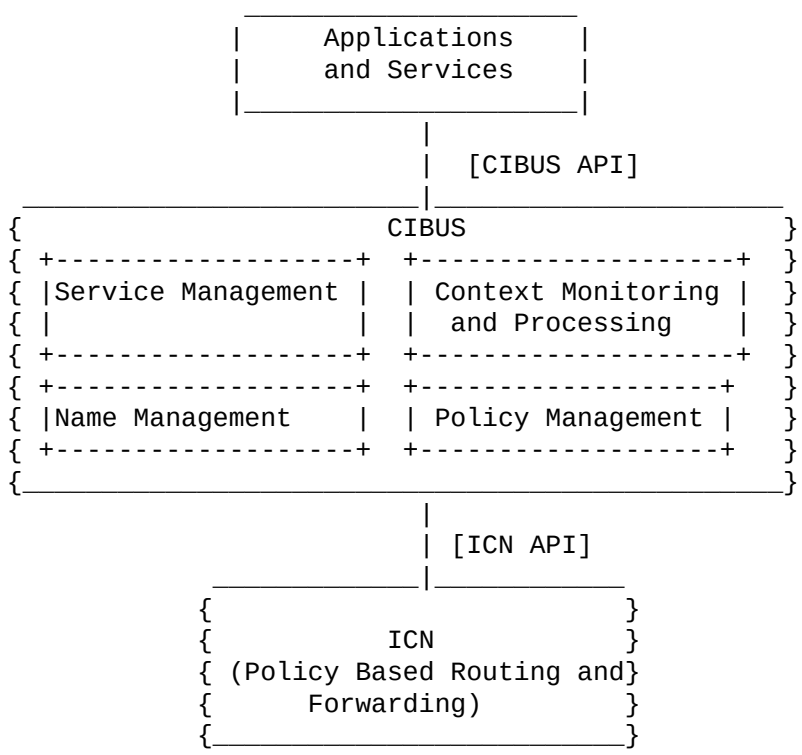

Figure 2: CIBUS functions and CIBUS/ICN API

CIBUS enable the following features in a home network scenario:

(1) Being a name based networking architecture, the applications requires zero configuration to initiate communication among producers and consumers, and can be physical topology independent considering CIBUS extends into the homenet's infrastructure. However general service access of over Internet may require ISP support.

(2) The service management layer allows consumers to discover services based on their contexts and policy requiremnents. A home gateway can be the central entity which learns services during the discovery process and which allow services to be managed in a centralized way. The service discovery component may also extended beyond the homenet [6] to connect ISP or third party services to the resident customers.

(3) With its configuration-less nature, ICN supports various communication modes such as 1:M, M:1, and M:M. ICN is also amenable to constrained sensor networks which can leverage computing, caching

and storage of the infrastrcture achieving the objective of homogenous layer for homenets.

(4) Being receiver-oriented, ICN allows consumers to express contexts, and producers to generate appropriate responses, therefore enabling contextual communication, further caching and multi-path routing capability enable reliable communication.

(5) Application and services can express the level of security requirement while initating node or service discovery and attachment process. This augments well understood ICN features which integrates security during data requests and responses.

Two high level APIs are identified in Fig. 2. Following functions shall be supported over CIBUS-API:

4.1. Name Management

Names can be unique within a local or global scope depending on the application or service requirement. Names can take any form permitted by ICN - flat or hierarchical. Depending on the service scope the naming process itself may require interaction with the home gateway to ensure global uniqueness. Furthermore in a home network the names could be associated with hierarchy of scopes, as in a room context wherein guests could only connect from a specific room, or services categorizes as entertainment, climate-control, or security so that devices and hosted services consume and generate information within that given scope over which desired policies can be applied.

4.2. Service Publishing

CIBUS enables services to publish and get discovered or advertise themselve considering default or configured policies (e.g. device, user, security considerations, usage constraints etc.) by the resident owner. This action the service profile available with API definitions to access a particular service feature, such as a notification service. Policies can be granular to the extent of making certain services available to certain space in the homenet to strict access policies to a set of users. These policies shall be standardized to enable interpretation and desired enforcement by CIBUS. For constrained devices, other smart devices or ICN routers in the proximity could play a role to publish services and manage the data accessibility.

4.3. Service Discovery

Services can be discovered by active probing for nodes and hosted services in the vicinity, or by local subscribtion to CIBUS for specific services of interest and making it available to applications if services themselves broadcast their availability; CIBUS shall handle both these possibilities. This process begins the moment device, application, or the user has a context change e.g. moving from outside to home environment and in the mode to associate with services of interest. Applications invoke node and service discovery by providing specific service name, filters such as context , security or other metadata of interest. The sevice discovery phase can also be used to handle routing with FIB entries pointing to the device(s) providing the service, this is feasible in home networks considering the topology is generally a tree structure.

4.4. Service Subscription

Subscriptions are triggered once an application discovers services of interest, and learns about its capabilities. CIBUS handles this by keeping track of consuming applications interested in specific service events and notifying those consumers about a new data availability, or during a change in context of the service.

4.5. Service Notification

Once services bind and valid consuming applications are authorized, the next step is to share the data generated by these services. Data can be generated periodically, event triggered, or in real-time due to consumer interaction. Moreover considerations over energy efficiency, and overhead concerns is very critical. In that sense in addition to the PULL, PUSH based notification shall be supported leveraging underlying ICN semantics. Content itself can be bound with metadata which restricts its usage to only a particular type of consuming application which can be enforced during the data dissemination process by the ICN layer.

4.6. Service Policy Management

Services itself could have many requirements. Policies includes content security or service access policies applicable at various level of interaction, such as during discovery/association phase or acesss, or during content exchange such as to establish content provenance, integrity, or privacy. Applications express policies in a standardized manner to CIBUS which can enforce it during the discovery phase or during the above mentioned service management tasks. Policies can be also be enforced as part of the routing and forwarding enhancement in the ICN layer. The policies in a home

environment is expected to evolve, hence CIBUS shall be adaptable to handle this evolution as well.

5. ICN-API

ICN-API primitives include the minimum set of APIs required to support CIBUS primitives exposed to the application through CIBUS-API. Current understood Interest/Response or Get/Put primitives to publish and request content can be extended to execute discovery or service management capabilities exposed to the application through CIBUS. For e.g. an action of service discovery in an ad hoc setting shall flood the service discovery query over all the radio interface, on the other hand Interests for a particular service or content shall only processed if service policies understood by ICN are met by the consumer Interest.

Extending a set of well understood contexts and policy functions to ICN reduces processing requirement of CIBUS. Towards this, policy aware routing and forwarding in ICN is useful in home setting where consumer Interests can be filtered by the ICN nodes even before reaching power constrained sensor devices; name based firewall in the home gateway is another application of this. Considering simple tree topologies in home network, routing itself can be configured during service discovery, with certain contextual policies enabled in the forwarding , these policies shall be managed through self-expiry or due to explicit action by the service.

6. CIBUS Prototype

A subset of the CIBUS features was realized in our prototype [5]. The prototype setup includes multiple internal routers (IRs) are rooted to a home gateway (HGw), and each is deployed with CCNx. The HGw connects to an ISP’s provider gateway (PGw). The IRs provides gateway support to connected resource-constrained sensors. The prototype demonstrates the following functionalities: (1) Home-wide zero-configuration through name-based neighbor and service discovery protocols across router boundary; (2) Context and policy based routing and forwarding at the HGw/IRs, where routing tables are set as the result of the service discovery protocol; (3) Name-based firewall at the HGw, where flows are inspected based on service names rather than ports and IP addresses; (4) Layer-2 agnostic operations realizing end-to-end ICN operations over any L2 technology.

Following scenarios as part of the CIBUS realization:

- Health Monitoring Service: In this scenario, a consumer discovers a health monitoring service through the HGw. The user then subscribes to this service. The interaction between the consumer

and the service results in another service instantiation on the consumer device, which makes the health monitoring data accessible to the healthcare service provider. The consumer device service is published for public access.

- Sensor Service: A set of wireless sensor motes are deployed which generate data of temperature, light, and humidity. This data is made accessible through a sensor service. The service is proxied by the internal router, and published for public access through the HGw.

- Trusted D2D Interaction: This application demonstrates ICN-based ad hoc trusted and social device-to-device interaction. Two devices discover each other (node discovery) and their services through the neighbor and service discovery protocols. Data access is restricted through group-ID based access control, and data confidentiality is enforced using a group key.

7. Conclusion

ICN enables a rich waist for contextual information exchange. Applications require more abstractions to handle efficient communication in different environments, for this we propose a contextualized information-centric BUS (CIBUS) which spans devices and infrastructure both local in homenet and beyond to the Internet. CIBUS allows heterogeneous devices, applications, and users to participate in context driven conversations in secure and reliable manner leveraging ICN features. In the context of homenets this enables several desirable features such as context based service publishing and subscription, zero-configuration based node and service discovery, and policy based routing and forwarding. Furthermore the CIBUS is applicable to both ad hoc and infrastructure settings, and can deal with diverse devices and services in or outside the home boundary.

The draft provides fucntional requirements of CIBUS to support the heterogeneity in homenets. Framework realization require considerations towards standardized representation of service profiles, context expression over CIBUS and ICN APIs to support devices, applications, and services.

8. Informative References

[1] AllJoyn, Plaform., "https://www.alljoyn.org/.", 2013.

[2] Homenet WG, IETF., "http://tools.ietf.org/wg/homenet/.", 2013.

[3] Mortier, R., Rodden, T., Lodge, T., and D. McAuley, "Control and understanding: Owning your home network.", COMSNETS , 2012.

[4] Dixon, C., Mahajan, R., and S. Agarwal, "An Operating System for the Home.", NSDI , 2012.

[5] Biswas, T., Chakraborti, A., Ravindran, R., Zhang, X., and GQ. Wang, "Contextualized information-centric home network.", Proceedings of the ACM SIGGCOMM , 2013.

[6] Ravindran, R., Liu, X., Chakraborti, A., Zhang, X., and G. Wang, "Towards Software Defined ICN based Edge Cloud Service.", Proceedings of IEEE CloudNet , 2013.

Authors' Addresses

Ravishankar Ravindran
Huawei Technologies
2330 Central Expressway
Santa Clara, CA 94582
USA

Email: ravi.ravindran@huawei.com

Asit Chakraborti
Huawei Technologies
2330 Central Expressway
Santa Clara, CA 94582
USA

Email: asit.chakraborti@huawei.com

Guoqiang Wang
Huawei Technologies
2330 Central Expressway
Santa Clara, CA 95050
USA

Email: gq.wang@huawei.com