Information-centric Networking based Homenet

Ravishankar Ravindran†, Trisha Biswas‡, Xinwen Zhang†, Asit Chakraborti†, and Guoqiang Wang†
†Huawei Research Center, Santa Clara, CA, USA. {ravi.ravindran,xinwen.zhang,asit.chakraborti,gq.wang}@huawei.com
‡North Carolina State University, Raleigh, NC, USA. tbiswas@ncsu.edu

Abstract—**Information-centric networking (ICN) aims to achieve efficient, secure, and reliable dissemination of information in contrast to host-centric IP architecture. This paper presents a case for ICN based home network (homenet). Current IETF proposal for homenets is based on IPv6 which inherits fundamental problems of IP such as security, mobility, and multicasting, which are integral features of an ICN design. We highlight how these ICN virtues help in the context of homenet considering the need for a homogenous platform to handle the diversity of devices, services, and user needs. We also provide a comparison of IETF's homenet proposal and an ICN based approach in terms of service, control, and data plane features and complexity. We exemplify our discussion through a proof of concept design of an ICN based homenet and highlight its usefulness through a comparative analysis of realizing fundamental homenet features in an ICN versus IP based framework.**

I. Introduction

Home network is 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 [9] such as DLNA, ZigBee, and Z-Wave all aimed at supporting homenet services such as multimedia sharing, lighting control, climate control, and energy management. The lack of inter-operability among these standards results in high cost, inflexibility, and inter-operability issues. The IETF homenet(IETF-home) working group [14] focusses on enabling an end-to-end IPv6 based homenet reusing existing protocols such as mDNS, DHCPv6, and OSPF to support features such as auto-configuration of IP interfaces, auto-discovery of services, and policy-based routing. However, IPv6 carries forward issues of IP's host-centric model with concerns in several areas including security, mobility, and content distribution.

At a high level, the objective of home networking is to allow efficient flow of information between service producers and consumers, both while inside or outside the home environment. This aligns with the principle of information-centric networking (ICN), which motivates the exploration of ICN based design for homenets. ICN [4] principles include networking around identities of users, devices, services, and content; this fundamentally insulates applications from any topological dynamism due to these entities. An ICN framework includes features such as: receiver-oriented operation helping with security and mobility issues; in-network caching for improved response time and reduced transit traffic; security over content chunks rather than over end hosts, enabling location independence of data; fault tolerance due to natural support for multicast both for content exploration and delivery.

This paper makes case for an ICN based homenets (ICN-home), where the challenge is to network heterogenous devices with the following considerations: 1) Focus on flexible top-down service-centric model with fine grained policy management, rather than focus on connecting devices; 2) Take advantage of cheap in-network storage and computing to support features such as mobility and content distribution; 3) Empower applications to exploit multi-homing by leveraging ICN's L2 agnostic property to enable operation over LAN/BAN/PAN radio technologies; (4) Realize the vision of a unified network layer spanning end-to-end compared to the current environment of incompatible protocols. We discuss these challenges by comparing the complexity of realizing them under IETF-home and ICN-home based framework with respect to service, control, and data plane. Furthermore, as part of an ICN based homenet design to achieve zero configuration we propose ICN based auto- node and service discovery protocols enabling user interaction with devices inter-connected in adhoc or infrastructure mode.

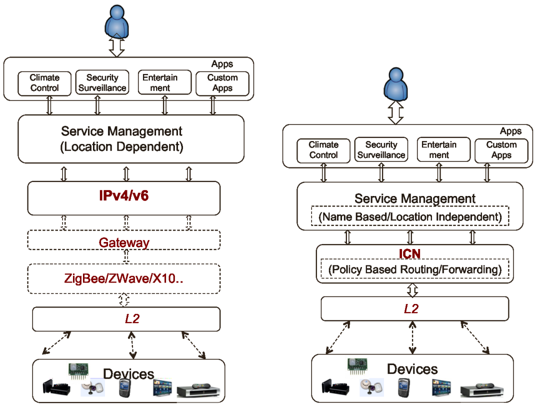
The paper layout is as follows: Section II presents a discussion of home networking challenges. Section III discusses how these challenges are being addressed under the IETF-home framework. Section IV presents the discussion in the context of an ICN-home framework. Sections V discusses the realization of an ICN based homenet prototype with proposal of protocols to achieve zero configuration, and Section VI concludes the paper.

II. Home Network Challenges

Based on a recent field study, [7] cites several challenges towards home automation: 1) High cost of ownership which includes installation and maintenance deterring any incremental addition of new services; 2) Inflexibility due to variety of standards and lack of inter-operability of devices leading to situation conceptualized in Fig. 1(a), where the services may have to hop between multiple protocols requiring gateways to handle protocol translation functions; 3) Poor manageability, due to complex realization of the home automation systems; 4) Difficulty in achieving security due to lack of granular access policy enabling features offered by current systems.

Considering the need for service level agility in homenet, following are the desirable requirements:

Agile Service management: Homenet services generate information of several type with different policy management requirements. A service is expected to be configurable in terms related parameters such as reachability, service lifetime,



(a) IP stack

(b) ICN stack

Fig. 1. **IP vs ICN homenet stack.**

and accessibility by users or by other services. Service composition should be possible with minimum overhead while resolving conflicts and 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 third party.

Auto-configuration: Considering the heterogeneity of devices, the homenet platform is expected to be a zero configuration environment such as protocols to support auto- node and service discovery, and self heal due to wireless or network layer impairment events.

End-to-end homogenous platform: To support a heterogenous device environment, a platform which can accommodate disparate devices and user requirements is required. The platform should be adaptable to both unconstrained and constrained segments while supporting different modes of communication such as 1:1, 1:M, and M:1.

Mobility support: Mobility support for both service producers and consumers is required to ensure best connectivity at all times. This includes nomadic movement, seamless mobility to handle real-time applications, and vertical handovers between different access networks as residents move in and out of their home premise.

Security: Information generated by producers inside homenet is expected to be private in most cases, and accessible through strict access control.

The following section discusses how these requirements are met under IETF-home and ICN-home framework. For our discussion we follow the network setup shown in Fig. 2 proposed in IETF-home [14]. At a topological level, the IETF-home framework generalizes a home to have multiple internal routers (IR) rooted to a home gateway (HGw). The HGw connects to the ISP serving router, provider gateway (PGw), which is authorized for certain management functions such as enabling global connectivity for in-home services. Several sub-networks could span from the IR including low power and lossy networks (LLN), subnet for guest usage, or surveillance service. The HGw itself could be multihomed to several ISPs, but for our discussion we restrict to a typical single ISP setup.

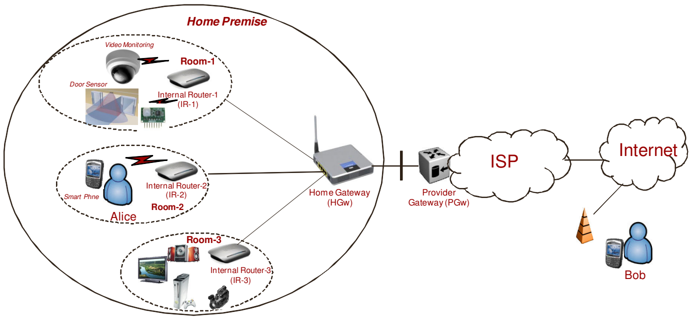


Fig. 2. **Homenet setup.**

III. IPv6 Based Homenet

High level architectural considerations to enable IPv6 based homenet solution is discussed in IETF draft [14]. Current IETF-home based homenet setup can be abstracted as shown in 1(a), where IP forms the end-to-end layer for several applications such as multimedia distribution,but requires gateway support for non-compatible applications built over protocol stacks such as ZigBee and ZWave. This setup suffers from gateway complexity, replicated protocol functions, and requires the knowledge of operating multiple protocols. The issue of network layer heterogeneity and complex gateway issue is being addressed by IETF's 6LoWPAN working group, which adapts IPv6 for LLN situations. However, this still preserves the host-centric nature of the network, over which other modes of communication such as 1:M has to be built. We continue the discussion of these issues with respect to the service, control and forwarding plane.

A. Service Plane

With the assumption of low competence of a home operator, following services are of critical importance from a service plane perspective:

Node and Service Discovery: Leveraging IPv6 framework, nodes can be configured in a stateless or stateful manner, the latter is more desired due to resiliency reasons but tradeoffs in terms of control overhead. IP address assignment is a significant part of the IETF-home architecture [14] covered elaborately for various situations including prefix delegation, HGw multi-homing, policy restrictions for guest use of services, and handling local or global reachability of services.

Once interfaces are designated addresses, service discovery is initiated. Protocols such as DNS-SD [6] and M-DNS [5] are leveraged to publish and discover services, built on link-scope multicast capability. The solutions suffer from certain drawbacks : 1) Management of non-information centric multicast address space to support such discovery mechanisms; 2) The discovery overhead for link-local scope discovery of N services is $O(N^2)$ in terms of computational overhead; 3) Lack of any form of service aggregation, such as aggregating multiple devices offering the same service to achieve efficiency of service request, management, and policy configuration; 4) Service resolution results in IP/TCP/UDP details to access the service, this raises the issue of handling dynamism of services such as mobility; 5) Difficulty of extending service discovery beyond link-local scope; proposal such as (xmDNS) [12] requires a new multicast space for site-scope service discovery.

To note, this level of configuration complexity for node bootstrapping or service discovery is orthogonal to the underlying problem of information dissemination, which is what ICN addresses making applications independent of transport layer semantics.

B. Control Plane

Homenet Routing: We focus here on routing functions required to enable service layer connectivity. Under IETF-home, as consumers and producers are overlaid over IP, service access begins with service resolution using protocols such as DNS-SD and mDNS, and then establish a session to obtain the related content. Here, basic reachability can be achieved using link state or distance vector routing protocols in a multiple subnet scenario. But these traditional protocols fall short of enforcing desirable policy rules highlighted in [13] such as need for detecting home boundary or even boundary between IR and its upstream connectivity to enforce policies such as identifying guest network, smartgrid, or LLN boundary. Other desirable routing features include: 1) Routing policies based on services offered by devices, such as ability to anycast requests to multiple producers; 2) Ability to multicast content if multiple users are viewing it; 3) Adapt routing to changing user policy requirements such as modification of accessibility property, or life time of the service.

C. Data Plane

Forwarding Considerations: General forwarding considerations in IETF-home primarily include establishing reachability to devices inside the home domain built over features such as link-local multicast to support automatic interface configuration and service discovery. Apart from the issue of service management across multiple subnets mentioned earlier, other requirements remain unaddressed such as: 1) Policy enforcement to support multi-homed devices for better QoE; 2) Management of firewall policies at the HGw based on user driven service policies; 3) Quality of service support to differentiate priority traffic related to real time sessions, life critical health monitoring, and lower priority traffic. 4) Though mobility support is not a consideration under IETF-home, mobility support is required for service producers both inside and outside the homenet. Under IETF-home framework, any form of seamless mobility support requires the use of mobile-IP based solutions which incurs inefficient control, and forwarding overhead.

The next section discusses how homenet requirements discussed in Section II can be met in an ICN framework.

IV. ICN Based homenet

ICN principles its networking around persistent identifiers, relying on the network to handle dynamism related to topology changes or mobility of end devices or services. This allows applications to use ICN primitives to access, subscribe, or search services and content without requiring to deal with location primitives.

Following ICN principles, we propose a generic service-centric homenet naming scheme. Naming begins with identifying services, then devices, and content offered by these devices. We then discuss ICN based homenet with respect to service, control, and data plane features.

A. Homenet Naming

Naming in ICN is influenced by several factors such as type of application, type of resources providing services, context, and the information being produced. Naming has several requirements, most important being persistent, resolvable, and securely binding to the content. Of these, our discussion surrounds the first two requirements, the security aspect is well discussed in [8]. Following are the naming considerations in a homenet scenario:

Contextualization: Homenet services are driven by policy requirements, basic one being scope of accessibility. At a high level, services may be restricted to only local access and/or set for global access through the Internet. Further, services may have strict access control, and temporal or physical restrictions in terms of where it can accessed in the homenet. To accommodate these needs, the naming hierarchy should accommodate expressions of policy at service, device, or content level.

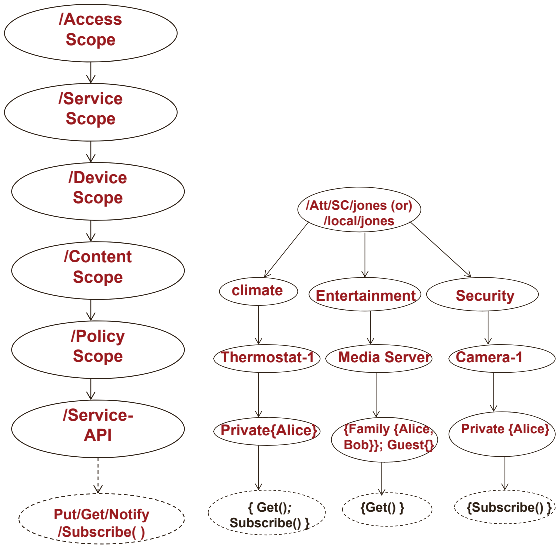
Service Accessability: The naming scheme maps to how content is aggregated and organized. In a homenet context, it implies that a consumer should be able to express contextualized requests at service, device, or at content level. For e.g. expressing request for temperature service data, should query all temperature sensors in the home network, irrespective of which local subnetwork they are in.

Extendability: Service-centric naming should be dynamic to accommodate new requirements, such as adding new service types, devices, content, or context policies.

Policy Enforcement: In order to contextualize policy enforcement, the service naming should have scope to identify service APIs with attributes indicating the service actions and parameters, and extendible to dynamic policy changes.

A hierarchical naming schema meeting the above requirements is shown in Fig. 3(a). At the first level of the naming structure hierarchy is the *access scope*, which identifies the reachability of the service within the homenet context. The second level, *service scope*, identifies service type such as entertainment, climate-control, or security. The third level, *device scope*, identifies the devices offering the service type. The fourth level, *content scope* identifies types of content served by the device. This level allows to handle different media or information type service offered by the same device. The next level, *policies*, identifies policies enforced over the consumers by the device offering the service which includes temporal/spatial and access control policies such as group context. The last level, *service API*, identifies the functional primitives and attributes used to interact with the service. Fig. 3(b) shows an example based on this naming hierarchy.

While the name tree identifies the services accessible within home, it can also be extended to include name space for



(a) Naming scheme (b) Naming example

Fig. 3. Homenet naming scheme and example

services managed directly by the ISP, or by a third party, or both.

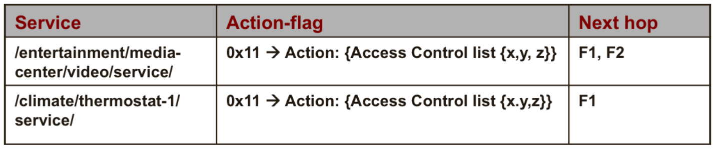
B. Service Plane

Discovery and Service Management: Node and service discovery protocol built over ICN framework enables several desirable features: 1) Natural support for multi-homed devices enabling L2 technology agnostic auto-discovery feature; 2) Unlike IETF-home scenario, multiple sub-network boundaries can be supported by imposing network layer routing policy restrictions; 3) Auto-discovery can be executed over local name space in a distributed manner, avoiding any centralized control points; 4) Data can be cached en-route to the source requesting node allowing location independence of content; 5) Secure bootstrapping as every request and response can be validated against consumer's and producer's security credentials; 6) Protocol design works for both infrastructure and adhoc based environment.

Networking over hierarchical names has both routing and management benefits. Service definitions discovered by content routers (e.g. HGw) can be correlated and aggregated over which centralized service management can be realized as shown in Fig. 1(b). This realization also allows composition of complex services and actions. During policy change events, the changes can be synchronized using a distributed service discovery protocol which includes management functions. One approach towards policy synchronization is using the *Sync* protocol [11], as another alternative design we propose a trigger driven service discovery protocol which is discussed in Section V.

C. Control Plane

Service routing: Name-based service routing can be established by publishing the services in a distributed routing control plane or resolution based on a centralized directory look-up mechanism. Considering the richness of ICN's forwarding plane, particularly CCN [10], the function of the routing control plane can extended beyond achieving reachability. Routing can be extended to distribute service announcements network wide with policy restrictions: for e.g. ICN router proxying a smart grid subnet may choose to advertise its service only to authorized neighbor(s); or the HGw/IR could impose restricted service announcements as limited to guest zones, homenet-scope, or share it with PGw for Internet access.



Service	Action-flag	Next hop
/entertainment/media-center/video/service/	0x11 → Action: {Access Control list {x,y, z}}	F1, F2
/climate/thermostat-1/ service/	0x11 → Action: {Access Control list {x.y,z}}	F1

Fig. 4. **Policy based CCN forwarding.**

D. Data Plane

Request/Response forwarding: ICN leverages both computing and storage resources in the routers to conduct intelligent information dissemination. Constructs such as embedding security in content PDU enables the feature of producing information once and consuming several times. Hierarchical naming can be leveraged to conduct efficient consumer request exploration of many sources, and content dissemination through multicast techniques at the same time. Though ICN professes PULL mode, PUSH mode can also be realized to support cases such as LLNs, where it is more efficient to notify sensor events rather than being polled periodically.

ICN proposal such as CCN allows one to impose results of policy based routing to user requests. Services when published can be associated with universally standardized *action-flags*, which represents a set of well known policy enforcements rules translating to appropriate actions which is applied at the HGw and/or at the IRs. An instance of the extended CCN forwarding information base (FIB) table is shown in Fig. 4, where service prefix is first mapped to encoded action-flag(s) and then to the next hop face list. After the first service request has been authorized by the network and/or the producer, a session token can be generated by the producer with a certain TTL, which can be committed along the routing path towards the service producer. This avoids network level policy check for the subsequent Interests of the session. Another critical component of HGw is the firewall. ICN proposal such as CCN makes firewall configuration more intuitive as Interest names, which are human readable and can be mapped to human readable firewall rules in contrast to interpreting traffic in terms of IP addresses and port numbers.

ICN's name based networking supports mobility of both consumers and service producers with light weight control plane support. In general, consumer mobility is handled leveraging ICN features such as receiver-oriented networking and in-network caching. Mechanism for service producer depends on the particular ICN architecture, which in most cases maps to applying local late-binding techniques.

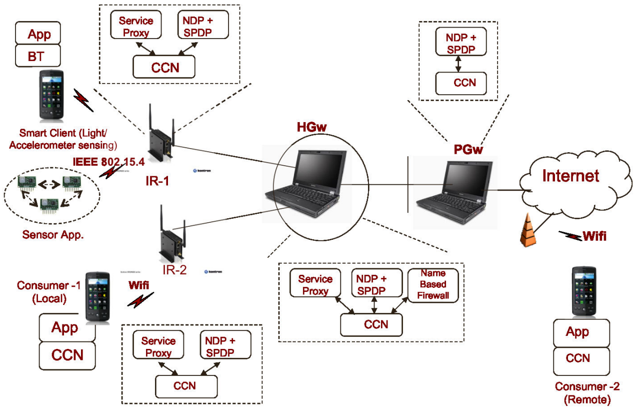


Fig. 5. **CCN based homenet prototype.**

V. Proof of Concept

Here we discuss the implementation of an ICN based homenet based on CCN. The prototype shown in Fig. 5 has following ICN objectives: 1) To realize homenet scope zero configuration neighbor and service discovery across router boundary; 2) Policy based routing and forwarding at HGw/IR, to avoid end hosts processing Interests violating policy requirements; 3) Name-based firewall implementation at HGw to impose service policies such as accessibility; 4) L2 agnostic operation of CCN to realize end-to-end publish/subscribe scenario, the IRs in the setup are enabled with multiple radios Bluetooth, IEEE 802.15.4, and Wifi.

The prototype was built over CCNx [1] realizing subset of the above features, specifically features 1,2, and 3. For 3, the policy enforced in the forwarding plane is that of reachability, where the HGw differentiates between services for only local or global access based on the face it arrives on.

As part of the prototype two protocols were developed, namely, neighbor discovery protocol (NDP) and service publish and discovery protocol (SPDP). The objective of the neighbor discovery protocol (NDP) is to discover devices or infrastructure nodes such as CCN routers in the node's neighborhood. Building over NDP, we developed service publish and discovery protocol (SPDP) to publish local services, and discover remote services dynamically triggered by consumer's request. We next discuss these protocols briefly.

Neighbor Discovery Protocol: The NDP works on the information of available active interfaces either over a CCN terminal or router. Fig. 6 shows a high level view of how NDP functions between two CCN nodes $n1$ and $n2$. In CCN, protocols listen and respond over a name space under which the information is exchanged. For NDP, we assume this name space to be rooted at $/ndp$. The neighbor discovery process is as follows:

1) As soon as NDP starts, it identifies the set of active physical interfaces, which in the example is $f2$ for node $n1$, and $f1$ for node *n2*. For each active physical interface, NDP inserts a FIB of $/ndp/pseudo\_x$ temporarily to enable neighbor discovery over face fx.

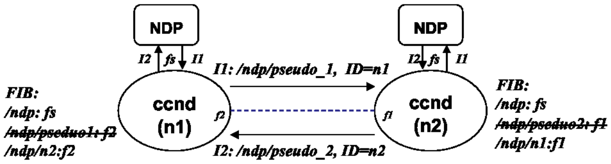


Fig. 6. **CCN neighbor discovery.**

2) NDP also inserts a FIB entry of form $/ndp$ mapping to face fs to serve any discovery Interests arriving on any of the physical interfaces.

3) NDP then expresses discovery interests periodically. When the neighboring node receives this Interest, it is forwarded to node's NDP instance, which learns about the neighboring node's identifier(ID). In order to establish bi-directional adjacency, the subsequent Interests from the local node includes the discovered neighbor's ID. This simple exchange of information shows how neighbor(s) can be discovered over a local name space, even in adhoc mode. Further the neighbor discovery could be extended to exchange more information such as security credentials and negotiate neighbor relationship required to support other services. The discovery results in removing $/ndp/pseudo\_1$ and adding $/ndp/n2$ in case of $n1$ to the FIB to conduct future information exchange with $n2$.

Service Publish and Discovery Protocol: Once an adjacency is established, service publishing and discovery can be enabled.

As in NDP, design for a local service publish and discovery protocol (SPDP) begins by defining a root name space under which Interests and Data is exchanged. We choose prefix $/spdp$. With reference to Fig. 7, the steps of SPDP are follows:

1) Service producers first register their services locally using the API exposed by SPDP. Service names follows the name structure discussed in Section IV. Published service profile contains information such as service-ID, access policies, TTL, reachability scope, and APIs to access the service.

2) Service discovery is application driven as in *App* in Fig. 7 query to discover all services or one which matches a specific criteria. The request is forwarded to the local SPDP instance which then expresses an Interest over active adjacencies. The Interest request contains the origin node-ID and a nonce to distinguish multiple requests from the same node. As the Interest is processed and forwarded hop-by-hop from one SPDP instance to another, state is saved locally corresponding to the request so that the Data with the aggregated service list D combining $D2$, $D3$, and $D4$ in the example can be sent back to the original requester.

3) As the services gets discovered, the service policies are committed to the FIB and enforced during service access. In a tree based topology as in Fig. 2, setting service routing is not an issue as only one discovery response is expected from the upstream. In case of a mesh topology, information from name-based routing protocol [3] can be leveraged to set the appropriate next hop(s).

The prototype shown in Fig. 5 implements sensing appli-

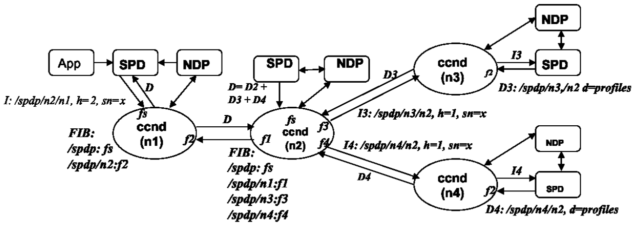
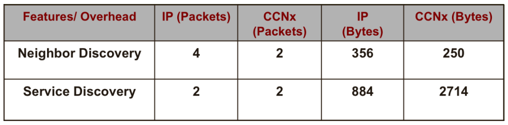


Fig. 7. **CCN service discovery.**



Features/ Overhead	IP (Packets)	CCNx (Packets)	IP (Bytes)	CCNx (Bytes)
Neighbor Discovery	4	2	356	250
Service Discovery	2	2	884	2714

Fig. 8. **IP vs CCNx neighbor and service discovery packet overhead.**

cations. Commercial M2M platform [2] is used as internal routers (IR-1 and IR-2) which aggregates to a HGw (a regular Linux PC). IR-1 proxies multiple sensor measurements from a smart phone, which is made accessible through services published as a result of NDP and SPDP instantiation, for now between IRs and HGw. The service entries in the FIB is a result of service discovery request by consuming applications. In the HGw, a name-based firewall is realized by extending CCNx's FIB logic to subject incoming requests as discussed in Section IV. As a result, Interests arriving through the PGw for a service marked private are dropped by HGw's firewall.

To evaluate the protocol and compare it with IP based discovery and service access protocols, a single subnet hub-spoke model is used. In the CCNx case the hub is a CCN router with NDP and SPDP protocol instance, while it is a L2 switch in the IP case. For each case, up to six IP and CCNx hosts were used for the experiments respectively. Comparison is provided with respect to neighbor discovery, service discovery, and service access performance. Fig. 8 shows the overhead in terms of number of packets and total number of bytes incurred between two nodes taking part in neighbor and service discovery. Here we observe the CCNx's overhead is lesser than IPv6 implementation, as it involves only Interest exchange. IP node discovery is based on stateless IPv6 address auto-configuration which includes a check for duplicate detection of auto-configured address. In case of service discovery in Fig. 8, IP's overhead is due to mDNS protocol, while CCNx uses SPDP. Here, though SPDP's overhead for the two node case seem higher, Fig. 9 shows the benefit when the number of nodes exceed a certain threshold. Similar caching performance due to increase in number of consumers can also be noted in Fig. 10. Although these benefits are expected and have been reported in earlier works, novelty of our implementation are: simple discovery mechanisms to aid zero configuration across multiple subnetworks; on-demand named-service routing and forwarding as a result of service discovery; and policy-based forwarding plane which benefits devices constraint of power and/or computing resources.

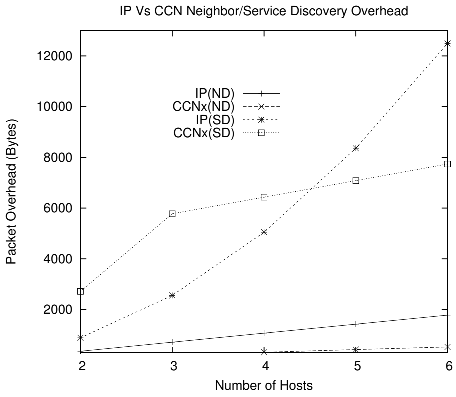


Fig. 9. **IP vs CCNx neighbor and service discovery control overhead.**

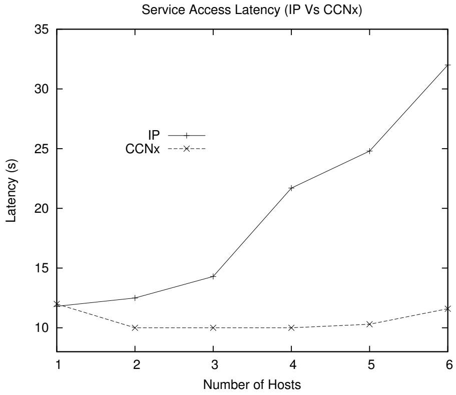


Fig. 10. **IP vs CCNx service access latency.**

VI. Conclusion

Home networks are getting complex with diverse devices and services. This paper compares an ICN based homenet design to an IPv6 based IETF proposal. We propose a service-centric homenet design applying ICN principles, one which is intuitive and allows for unified service platform realization. Later, we compare the design advantages of an ICN versus an IP based approach with respect to service, control, and data plane complexity. We conclude by an evaluation of ICN versus IP based homenet design in terms of the zero-configuration features and service access performance.

References

[1] CCNx code release: http://www.ccnx.org.

[2] M2M Kontron Platform, http://us.kontron.com/products/systems+and+platforms/m2m/.

[3] OSPFN: An ospf based routing protocol for named data networking, technical report,NDN-0003, July 2012.

[4] B. Alghren et al. A survey of information-centric networks. In *IEEE Communication Magazine*, June, 2012.

[5] S. Cheshire and M. Krochmal. Extended Multicast DNS, IETF, 2006.

[6] S. Cheshire and M. Krochmal. DNS-Based Service Discovery, IETF, 2011.

[7] C. Dixon et al. An operating system for home. In *Proceedings of NSDI*, 2012.

[8] A. Ghodsi et al. Naming in content-oriented architectures. In *Proceedings of ACM SIGCOMM Wksp*, Aug, 2011.

[9] C. Gomez and J. Paradells. Wireless home automation networks: A survey of architectures and technologies. In *IEEE Communication Magazine*, June, 2010.

[10] V. Jacobson et al. Networking named content. In *Proceedings CoNEXT*, 2009.

[11] V. Jacobson et al. Custodian-based information sharing. In *IEEE Communication Magazine*, 2012.

[12] K.Lynn and D.Sturek. Extended Multicast DNS, IETF, 2012.

[13] L.Howard. Evaluation of Proposed Homenet Routing Solutions, IETF, June 2012.

[14] T.Chown and et al. Home Networking Architecture for IPv6, IETF, June 2012.