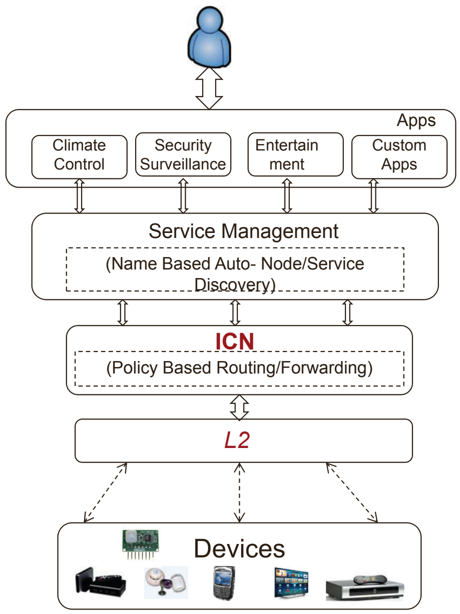
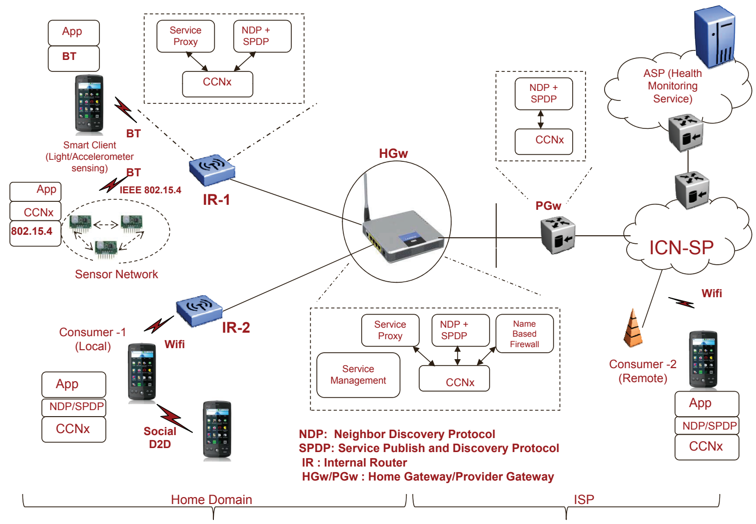


(a) ICN based homenet architecture.



(b) CCNx based homenet prototype.

Figure 1: ICN based homenet architecture and prototype.

(HGw), and each is deployed with CCNx [1]. The HGw connects to an ISP's provider gateway (PGw). The IRs provide 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.

Zero-configuration discovery protocol: We develop two name-based CCN protocols, namely, neighbor discovery protocol (NDP) and service publishing and discovery protocol (SPDP). The objective of NDP is ad hoc and contextual association of devices, while SPDP allows efficient discovery of services over ICN. Further details on these protocols can be found in [3].

Policy-based routing: ICN-based homenet uses policy based routing and forwarding, wherein service entries in the FIB of the CCN router are a result of service discovery requested by consuming applications. In the HGw, a name-based firewall is realized by extending CCNx's FIB logic to subject incoming requests to policies associated with services. For example, if a service is marked for private access, i.e. valid only within the homenet scope, any interest from outside is dropped by the HGw.

Device-to-device communication: While demonstrating the applicability of ICN towards different scenarios, our prototype supports location based service publishing and social-aware device-to-device (D2D) interaction.

2.2 Demonstration Scenarios

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 (IR-1) as shown in Figure 1(b), and published for public access.

Trusted D2D interaction: This application demonstrates ICN-based ad hoc trusted and social device-to-device interaction. Two devices discover each other 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.

3. REFERENCES

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

[2] B. Ahlgren, C. Dannewitz, C. Imbrenda, D. Kutscher, and B. Ohlman. A survey of information-centric networking. *Communications Magazine, IEEE*, 50:26 – 36, 2012.

[3] R. Ravindran, T. Biswas, X. Zhang, G. Wang, and A. Chakraborti. Information-centric networking based homenet. In *IFIP/IEEE ManFI Workshop on Management of the Future Internet*, May, 2013.