ACCEPTED FROM OPEN CALL

EZPlugIn: Plug-n-Play Framework for a Heterogeneous IoT Infrastructure for Smart Home

Pushpendu Kar and Hao Wang

Abstract

Internet of Things (IoT) introduces a very large scale of technologies. An IoT system is comprised of a large number of smart devices and sensors connected together that are often non-intrusive, transparent, and invisible. Current IoT networks using IP-based Internet architecture are facing limitations in scalability and interoperability among the devices. In this work, we propose a plug-n-play IoT framework to significantly improve the interoperability among devices so as to obtain a more flexible IoT infrastructure. To achieve the plug-n-play feature in an IoT network, we propose to modify the notion of communication among the devices by adapting the Named Data Networking (NDN) communication paradigm in the IoT infrastructure. In NDN, a device communicates with other devices and sends data requests by the name of the accessing component instead of their physical locations. Security issues in such a framework can be more easily handled than in the current Internet. But adaptation of NDN in the current communication model is a challenging task. So we have modified data structures as well as the format of exchanged messages to fit the NDN with the service based communication model. The proposed framework has been studied in a smart home environment. Simulation results show that the proposed framework has less transmission delay and better throughput compared to IP-based systems.

Introduction

The Internet of Things (IoT) describes the network of physical objects such as vehicles, home appliances and other items embedded with electronics, software, sensors, and actuators, which allows these objects to connect and exchange data. Communication among these devices and sensors need to happen anytime and anywhere for any related services. The widely spreading IoT systems are consuming increasingly more energy. Generally, communications among them happen wirelessly in an automatic and ad hoc manner. Additionally, in an IoT system, services are more complex, mobile, and decentralized. Thus, data integration in an IoT system over different environments is more difficult. In such a situation, data integration needs to be done by modular inter-operable components. Volumes of data from different sources need to be combined to extract relevant features through an infrastructure solution. The process of data combination helps to interpret data and devise their relationship for statistical analysis and decision making. Different applications cannot run on a single architecture. Therefore, different IoT systems build on different heterogeneous architectures. The interactions of IoT devices are consuming significant amounts of energy, which significantly improve the interoperability between devices. The IoT infrastructure is critical in reducing the overall energy consumption, so as to move toward greener IoT systems.

IoT is a complex technology due to different reasons. First, in this technology, different heterogeneous architectures have been developed upon existing networking technologies and applications. Various applications and environments require different networking technologies, ranges, and many other characteristics. Second, all the communication technologies in the form of fixed and mobile devices should have low costs with reliable connectivity. Finally, in IoT systems, there are many different applications having different requirements with their respective security solutions.

IoT application systems should be global for serving different industries and fields. Here, information interoperability needs to take place between enterprises, industries, regions, or countries. Interoperability in an IoT system is essential for going through layers of physical devices, communications, functions, and applications. Different languages and protocols contribute to build these layers. Domain transparent languages and protocols are required to develop the layers. These heterogeneous architectures should be open and follow some standards [1]. Also they should not restrict users to use end-to-end and fixed solutions. A comprehensive approach is needed to address the interoperability issue of IoT devices and services at several layers.

NDN, a Future Internet Architecture, changes the notion of addressing data instead of machines. The IP address abolishes the concept of a point to point communication channel, which has become obsolete. The fundamental unit of communication becomes a NAME, not a CONNECTION. All data is cryptographically signed. Every application designs its own namespace. The key research area of NDN is "how do you route namespaces?". Initially, NDN is routed over the current Internet, just as the Internet was originally routed over the telephone network, until a custom-built architecture matured. This makes the current architecture unnecessary to access and alter named resources. The backbone of our plug-n-play IoT framework is NDN. As a promising technology for future Internet architecture, NDN has introduced a new way of data retrieval in IoT [2]. In recent years, users and applications are more interested in specific data components, with much less interest in their locations [3]. Therefore, the concept of using IP addresses to locate a computer which contains a particular data item is becoming less important. The necessity of an alternative to IP addresses became more appealing and NDN is a viable solution for the challenges of IP addresses. In NDN, users send their data request without knowing who holds the data [4]. Also,

P. Kar is with the School of Computer Science, University of Nottingham Ningbo China, 199 Taikang East Road, Ningbo 315100, China (email: pushpendu.kar@nottingham.edu.cn).

H. Wang is with the Department of Computer Science, Norwegian Uni.versity of Science and Technology, Ametyst-bygget, A213, Gjik, Norway (email: hawa@ntnu.no).

Digital Object Identifier: 10.1109/IOTM.0001.2000172

NDN is more efficient than the current Internet in managing security issues.

Considering the above mentioned facts, in this work, we propose a plug-n-play framework for a smart home environment, where users need not bother about interoperability among devices in the IoT infrastructure. They can connect a new device into an IoT system without thinking about the interoperability with the other devices, network, and applications. We outline the overall contributions of this work as follows.

- We propose a NDN based plug-n-play framework for a heterogeneous IoT network.
- We discuss the use of the proposed scheme for the heterogeneous IoT network in a smart home environment.

Related Works

Interoperability of IoT devices is an essential factor for seamless operations among themselves as well as scalability of IoT systems. There are few existing works, which have discussed these issues to some extent. Seales *et al*. [5] developed an IoT based testbed that integrates Health-IoT with cloud computing. Their developed system has a plug-n.play feature. They have integrated a body area sensor network with a cloud system over the Internet. The proposed system has used the NDN technique for improved scalability and the plug-n-play feature. Rajaraman *et al*. [6] proposed a framework, which has published Sensor/Network as a Service. The proposed service layer has helped to come up with the plug-n-play infrastructure, across platforms from different vendors, requiring interoperability among devices, which leads to the successful deployment of a large-scale system. Matthys *et al*. [7] proposed µPnP-Mesh, which has provided a low-power and low-cost method for universal plug-n-play of embedded IoT devices to industrial SmartMesh IP systems. The SmartMesh IP has provided reliable and low-power networking for industrial automation and monitoring. Mikhaylov *et al*. [8] has developed a software layer for abstraction on highly dynamic hardware. This software abstraction layer has provided the plug-n-play feature to an IoT system. Rokni *et al*. [9] proposed a method to automatically find appropriate machine learning algorithms in real-time without the need of labeled training data. Their method can find machine learning algorithms for a new sensor view by an old sensor view for which trained algorithms exist. Polap *et al*. [10] presented a smart home system to automatically diagnose the skin health condition of the occupants in a house. Their developed system has used built-in sensors and artificial intelligence methods, which have been used to analyze skin health data.

Security is an important aspect of an IoT system. Kumar *et al*. [11][12] proposed a security technique for an IoT network in a smart home environment. In the proposed security technique, they have modified the standard IPv6 protocol for addressing and authenticating smart devices in a unique way. They also used the Diffie-Hellman key exchange protocol to establish secure sessions between devices. Li *et al*. [13] proposed a machine learning based security technique to prevent energy theft from a smart meter. They combine various machine learning model into a single forcast system for predicting the power consumption. Hassija *et al*. [14] and Meneghello *et al*. [15] have reviewed different security techniques for IoT systems and discussed their advantages as well as disadvantages.

Sysnthesis: The review of the existing literature reveals that state-of-the-art IoT systems handle the interoperability and security issues by some additional patches or add-ons. However, adaptation of the NDN in the proposed framework helps to handle these issue in an inherent manner, which makes the IoT systems more robust and flexible.

Proposed Framework

The proposed framework unifies the heterogeneous IoT devices by adding a layer of abstraction in the communication protocol stack, as shown Fig. 1. The new layer is named "EZPlugIn Infrastructure". This layer basically implements the Named Service from the NDN communication stack eliminating IP address based communications in a smart home environment. The rest of the layers of the NDN communication stack are implemented by the other layers of the proposed framework. In a smart home IoT network, users do not request data. They send service requests to the devices to execute some services. Therefore, unlike the general NDN technique, in EZPlugIn, a user request contains a service name instead of content name. Each service needs to have a globally unique name. Service names follow a hierarchical structure. If a user wants to access a service, named 'service1', from a device, named 'device1', the user application generates the service name as /country/city/person1/device1/service1. A user initiates the communication by sending a service request packet, which contains the requested service name and cryptographic information for security. A device with the requested service receives the service request packet and execute the service. Thereafter, the device with the requested service sends back a service response to the user about the status (successful execution or error message) of the service through the same forwarding path of the corresponding service request packet. The structure of the service request and service response packets are shown in Fig. 2. The service request packet contains the service name, which is the name of the requested service; the selector, which defines the scope and preference of the service; and cryptographic information. The service response includes the service name, which is the same as the name of the requested service, signature and signed information for security, and service response, which may be the error message or specific information related to the service access.

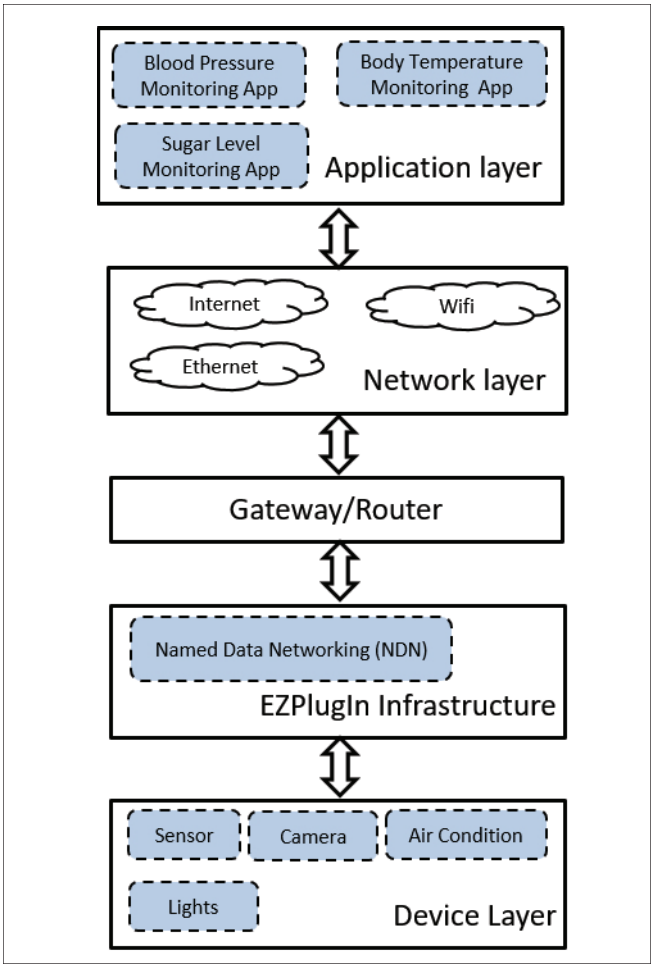

FIGURE 1. Architecture of EZPlugIn framework for smart home.

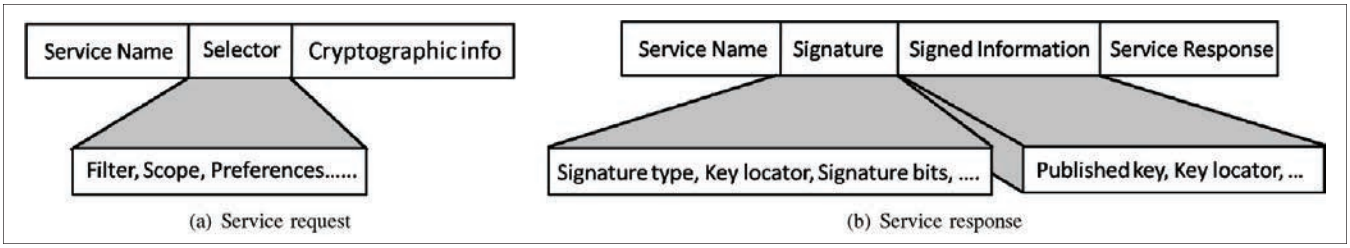

FIGURE 2. NDN packet format.

Unlike the normal NDN, in EZPlugIn, the routers and gateway do not maintain a Content Store (CS) cache for storing the user's data as it handles user commands to implement their service request on the devices instead of data content. In this method of service access, the gateway and other routers in the network maintain the following tables.

- Pending Service Request Table (PSRT): The PSRT keeps an entry for each incoming service request. It maintains the entry until the corresponding service response arrives. It may also remove the entry earlier, if the entry lifetime expires. These PSRT entries are used to select a downstream path toward the user. Finding entries in a PSRT is done by exact matching of service names. A PSRT has two fields: service name and interface. Service name is the name of the requested service, and interface is the next hop downstream entity from where the service request has arrived.
- Forwarding Information Base (FIB): The FIB keeps next hop(s) and other information for each reachable service name prefix. The NDN based routing protocols populate the FIB and are used to forward the service requests to the specific device. The FIB has two fields. One field is the service name, which maintains reachable prefixes of an absolute service name; the other field is the list of interfaces, where the service request can be forwarded by the matching prefix. Figure 3 presents the FIB table inside a NDN gateway.

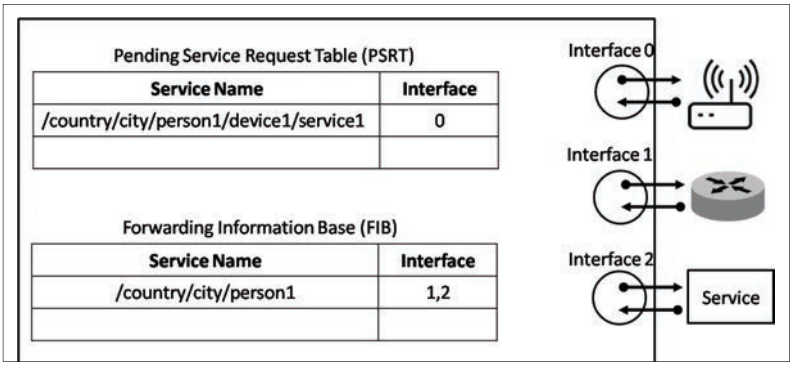

FIGURE 3. Forwarding table of a NDN node.

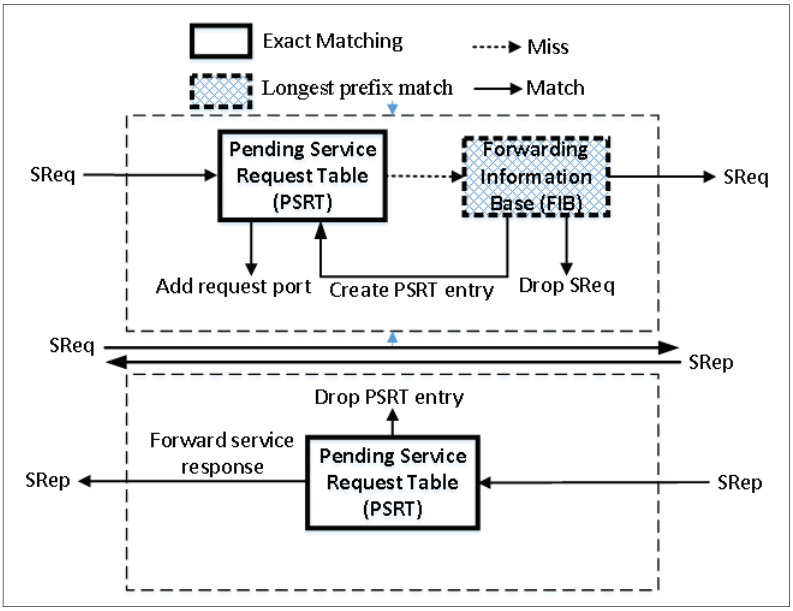

FIGURE 4. Design of gateway in EZPlugIn.

The design of a NDN gateway in the proposed system is presented in Fig. 4. When a user wants to access a service from a smart home device, they send a service request from their personal application. If a service request arrives at a NDN router or gateway, the contained service name is searched in the PSRT to find a matched entry. On finding a matched entry in the PSRT, the incoming interface is aggregated with the list of existing interfaces. After the arrival of the corresponding service response, all the requested users receive a service response. If there is no matching entry of the service request in the PSRT, the service request is passed to the FIB of the router or gateway to perform a longest prefix match. For example, in a service request having service name /a/b/c/d/e, the prefixes are '/a', '/a/b', '/a/b/c', '/a/b/c/d', '/a/b/c/d/e'. The service request is forwarded to next hop of the corresponding longest prefix match and a new PSRT entry is created with its incoming interface for the matched prefix. If no matching prefix is found, the service request may be flooded to all the outgoing interfaces or discarded based on the forwarding policy.

After execution of the requested service, a device returns a service response. When a service response is received by an NDN router or gateway, the whole PSRT is searched to find a matched service name. If a PSRT entry with the matched service name is found, the service response is forwarded to the all incoming interface(s) mentioned in the list. Thereafter, the PSRT entry is deleted. Due to lifetime expiration, if no matching entry is found in the PSRT, the service response is dropped. The underlying network (wired as well as wireless) uses the physical address (MAC address) of the devices. However, instead of using the IP address, the network uses the content centric approch to establish communication among the devices. Figure 5 presents the application of the proposed framework in a smart home environment.

How EZPlugIn Supports Plug-n-Play of Devices?

The conventional IoT network in a smart home uses the IP address to communicate with users over the Internet. All the networking components and devices have their own fixed IP address or dynamically assigned IP address. Assignment of an IP address requires a lot of configuration settings of the networking components and devices when the network is initially formed as well as when a new device is connected to the net-

work. In addition to this, an IP-based network prevents seamless interoperability of networking components and devices among different vendors and service providers due to the use of specific configurations and address range. An IoT network in a smart home connects different devices with the network from different vendors and operators, which essentially requires interoperability for plug-n-play of devices. The limitations of an IP-based IoT network are the major hindrance for scalability and interoperability among networking components and devices.

Our proposed scheme, EZPlugIn, uses the NDN technique, where the concept of address-based communication has been eliminated. Here, a user accesses services from devices connected in the network by the name of the service itself instead of the address of the device where the service physically exists. Elimination of the address requirement from communication of devices and access to the services by their name makes it possible to connect the devices to the network without further network configuration, which can improve their interoperability. This leads to plug-n-play of devices using our proposed scheme.

Why EZPlugIn Is Secure?

IP communication technology provides security for channels between senders and receivers, which can be compromised by an intruder using some malicious intrusion mechanisms. However, the use of NDN communication technology in our proposed scheme provides security for each service request by embedding cryptographic information in the request and the corresponding response. It also helps to support access control and confidentiality. Therefore, there is no requirement of a trusted server and directories for implementation of access control policies. As the service request can itself hold the decryption key, it is not necessary to distribute the key. The proposed EZPlugIn scheme supports both symmetric and asymmetric public key cryptography. If the service parameters are encrypted using symmetric keys, they can be decrypted by a secret key, which can be received from the service request itself. A service provider can verify a service request from a user by its signature and returns an encrypted secret key using a user's public key, which is only visible to the user. Therefore, the proposed EZPlugIn scheme is much more secure than the state-of-the-art IoT network in a smart home.

Comparison

In the existing literature, a few frameworks have been developed for IoT systems which can provide the plug-n-play feature among the devices, and the heterogeneous devices also can work interoperably among themselves. However, all these frameworks implement an additional layer in their communication stack to support plug-n-play and interoperability by unifying data models and interactions among devices. However, this additional unification process incurs extra communication overhead in the process of communication between the devices. The unification process also makes the system more vulnerable to the attackers.

On the other hand, our proposed framework does not implement any additional layer in the communication stack; rather, it replaces the existing IP layer from the communication stack with the Named Service. The proposed framework provides plug-n-play and interoperability among the devices by accessing data using the content name instead of their physical address.

This technique only modifies the data access method between the devices rather than unifying the data model and interaction between devices. Therefore, the proposed framework does not incur additional energy consumption and communication overhead on the IoT system. In addition, in the proposed framework, data packets are encrypted instead of channels between devices being encrypted as in previous IoT frameworks. Therefore, the proposed IoT framework is more secure than the earlier systems.

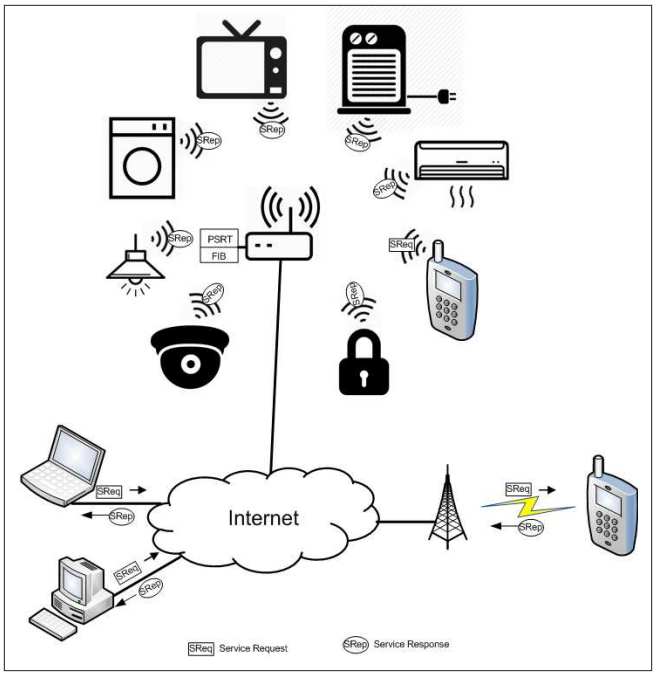

FIGURE 5. Smart home architecture with NDN.

Performance Evaluation

The proposed system is simulated by the open source NS-3 based NDNSim simulator. For simplicity, we have simulated the proposed system using a small number of nodes. We compared the performance of the proposed system with a traditional IP based system.

Simulation Setup

The simulation environment of both the proposed NDN-based system and IP-based system contains three home appliance nodes, three mobile nodes, one controlling node, one Internet node, and one gateway node. The home appliance nodes are linked to the controlling node; the mobile nodes are linked to the gateway node; the controlling node is linked to the router node; and the router node is linked to the gateway node. All these links are p2p. The mobility range of the home appliance nodes and mobile nodes are considered as 50m. In a NDN-based system, communication between home appliance nodes and the controlling node is performed by the NDN communication technique. The mobile nodes are the remote devices to control the home appliances remotely over the network. However, the transmission between the controlling node and the mobile nodes is using a traditional IP based p2p network, so the results of the mobile nodes are being ignored. We have considered that the proposed system and the IP-based system both have the same number of nodes for comparing their performance, but the IP-based communication technique and CSMA are used to replace the NDN network and the connection to mobile nodes from the gateway node.

Results and Discussions

The comparison of the average transmission delay of the NDN-based and IP-based systems is presented in Fig. 6a. The figure shows that the average transmission delay of the home appliance nodes in both systems are near similar. However, the controlling node of the IP-based system has more average transmission delay than that of the NDN-based system. The possible reason is that the home appliance nodes in both systems are handling their respective traffic, whereas the controlling node is handling multiple traffic, which is done more efficiently in NDN than in an IP network.

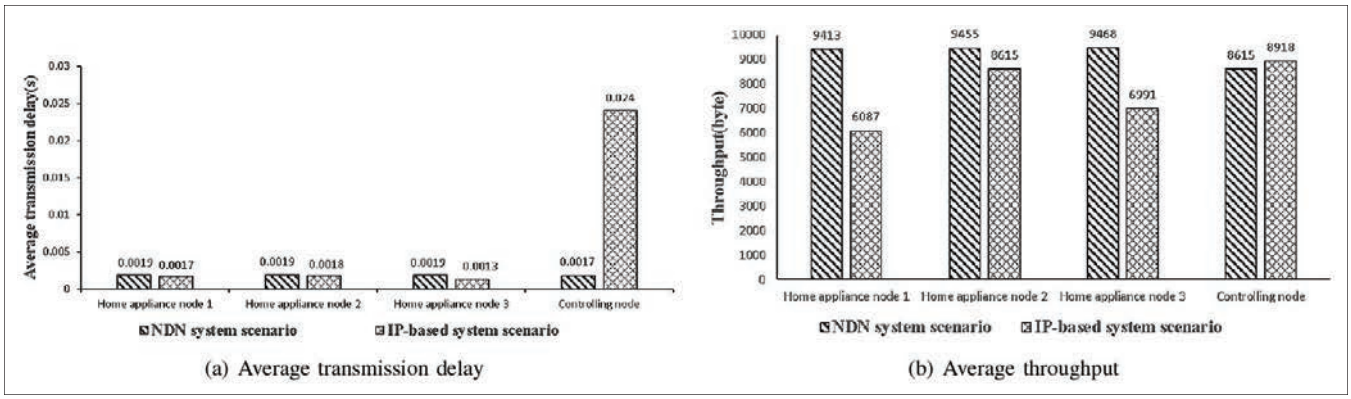

FIGURE 6. Simulation results

The comparison of the average throughput of the NDN-based and the IP-based systems is presented in Fig. 6b. The figure shows that the home appliance nodes have more average throughput in the NDN-based system than in the IP-based system. However, the controlling node of the NDN-based system has less average throughput than that of the IP-based system. This is because the home appliance nodes in the NDN-based system individually are able to send more data in less time, but the controlling node of the IP-based system needs to send more data in less time to maintain the traffic.

CONCLUSION

IP-based IoT networks are facing serious problems in scalability and interoperability while they are used to connect heterogeneous devices in a smart home environment, which incurs a large amount of energy consumption for device interactions. These problems of an IoT network in a smart home environment raise the need for a new plug-n-play framework to connect heterogeneous devices in an IoT network. In this work, we proposed a plug-n-play framework, which makes it possible to construct an IoT network of heterogeneous devices as well as connect new devices to the network without thinking about their interoperability with the other existing devices. To develop this framework, we have modified the communication paradigm in the IoT network by adopting NDN instead of conventional IP-based networking. With this technique of communication, a user can access a service from a connected device by using the service name instead of the address of the device that hosts the service. This new communication paradigm eliminates further network configuration setup of devices before they connect to the network.

Provider mobility induces overhead and scalability issues in NDN. In the future, we plan to extend our work for a mobile Internet of Things network. We also plan to develop a prototype model of an IoT network for a smart home using our proposed framework.

ACKNOWLEDGEMENT

The authors would like to extend sincere thanks to University of Nottingham Ningbo China for supporting this research project under Faculty Inspiration Grant (I01190900047).

REFERENCES

[1] A. Al-Fuqaha *et al.*, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Commun. Surveys Tutorials*, vol. 17, no. 4, June 2015, pp. 2347–76.
[2] D. Saxena *et al.*, "Named Data Networking: A Survey," *Computer Science Review*, vol. 19, 2016, pp. 15–55.
[3] W. Shang *et al.*, "Named Data Networking of Things (Invited Paper)," in *Proc. IEEE First International Conference on Internet-of-Things Design and Implementation (IoTDI)*, April 2016, pp. 117–28.
[4] L. Zhang *et al.*, "Named Data Networking," *SIGCOMM Comput. Commun. Rev.*, vol. 44, no. 3, Jul. 2014, pp. 66–73.
[5] C. Seales *et al.*, "PHINet: A Plug-n-Play Content-centric Testbed Framework for Health-Internet of Things," in *Proc. IEEE International Conference on Mobile Services*, June 2015, pp. 368–75.
[6] V. Rajaraman *et al.*, "Enabling Plug-n-Play for the Internet of Things with Self Describing Devices," in *Proc. 14th International Conference on Information Processing in Sensor Networks*, 2015, pp. 374–75.
[7] N. Matthys *et al.*, "μPnP-Mesh: The Plug-and-Play Mesh Network for the Internet of Things," in *Proc. 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*, Dec. 2015, pp. 311–15.
[8] K. Mikhaylov and A. Paatelma, "Enabling Modular Plug & Play Wireless Sensor and Actuator Network Nodes: Software Architecture," in *Proc. IEEE SENSORS*, Nov 2015, pp. 1–4.
[9] S. A. Rokni and H. Ghasemzadeh, "Plug-n-Learn: Automatic Learning of Computational Algorithms in Human-centered Internet-of-Things Applications," in *Proc. 53nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, June 2016, pp. 1–6.
[10] D. Polap *et al.*, "An Intelligent System for Monitoring Skin Diseases," *Sensors*, vol. 18, no. 8, 2018.
[11] P. Kumar and L. Chouhan, "A Secure Authentication Scheme for IoT Application in Smart Home," *Peer-to-Peer Networking and Applications*, 2020.
[12] P. Kumar and L. Chouhan, "Design of Secure Session Key Using Unique Addressing and Identification Scheme for Smart Home Internet of Things Network," *Trans. Emerging Telecommunications Technologies*, 2020, p. e3993.
[13] W. Li *et al.*, "A Novel Smart Energy Theft System (SETS) for IoT-based Smart Home," *IEEE Internet of Things J.*, vol. 6, no. 3, 2019, pp. 5531–39.
[14] V. Hassija *et al.*, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures," *IEEE Access*, vol. 7, 2019, pp. 82 721–82 743.
[15] F. Meneghello *et al.*, "IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices," *IEEE Internet of Things J.*, vol. 6, no. 5, 2019, pp. 8182–8201.

BIOGRAPHIES

PUSHPENDU KAR holds a B.Tech., a M.Eng., and a Ph.D. degree, all in computer science. He is an assistant professor with the School of Computer Science, University of Nottingham Ningbo China (China campus of the University of Nottingham UK). Prior to this, he was a research fellow with the Department of ICT and Natural Sciences, Norwegian University of Science and Technology, Norway. He was also a postdoctoral research fellow with the Department of Electrical and Computer Engineering, National University of Singapore, and the Energy Research Institute, Nanyang Technological University, Singapore. His research interests include mobile ad hoc networks, wireless sensor networks, Internet of Things, and content-centric networking. He is a recipient of the Erasmus Mundus Postdoctoral Fellowship of the European Commission, the European Research Consortium for Informatics and Mathematics Alain Bensoussan Postdoctoral Fellowship of the European Union, and the Science and Engineering Research Board Overseas Postdoctoral Fellowship of the Department of Science and Technology, Government of India. He is an IEEE Senior Member.

HAO WANG holds a B.Eng. degree and a Ph.D. degree, both in computer science. He is currently an associate professor in the Department of Computer Science, Norwegian University of Science and Technology, Norway. He has authored or co-authored over 160 papers in peer-reviewed conferences and journals. His research interests include big data analytics and industrial Internet of Things, high-performance computing, and safety-critical systems. He served as a TPC Co-Chair for IEEE CPSCom 2020, IEEE CIT 2017, and ES2017, and as a reviewer for prestigious journals, such as IEEE TKDE, TBD, TETC, T-IFS, and ACM TOMM. He is a member of the IEEE IES Technical Committee on Industrial Informatics. He is a senior member of IEEE and a member of ACM.