IoT Routing Architecture with Autonomous Systems of Things

Soochang Park and Noel Crespi
Wireless Networks and Multimedia Services
Institut Mines-Telecom, Telecom SudParis
Evry 91011, France
{soochang.park and noel.crespi}@telecom-sudparis.eu

Hosung Park and Sang-Ha Kim
Computer Science and Engineering
Chungnam National University
Daejeon 305764, Republic or Korea
hspark@cclab.cnu.ac.kr and shkim@cnu.ac.kr

***Abstract*—This article presents a future-driven routing architecture for Internet of Things (IoT). This IoT is a novel concept involving a new concept regarding a set of things with the same routing and service polices, denoted by an autonomous system of things (ASoT). In IoT, an ASoT would be connected not only to the others but legacy autonomous systems (ASs) for the Internet in a wide variety of scenarios. Hence, this article firstly addresses classification of diverse features of ASoTs, and then explores new challenges especially on inter-domain routing.**

***Index Terms*—Routing architecture, autonomous systems, IoT.**

I. Introduction

We are standing on the brink of a new era with real ubiquitous computing and communication where many of gadgets, such as sensors, RFID tags, and smart electronic/electromechanical devices, surrounding us will be on the network [1]-[3]. The gadgets would disappear and weave themselves into the fabric of our everyday life to work in concert to support us in carrying out daily life activities, tasks and rituals in an easy, natural way using information and intelligence, hidden in the network connecting the gadgets. This pervasive paradigm we call *Internet of Things* (IoT) might increase value of information generated by the number of interconnection between people and gadgets, denoted by things, and transformation of the processed information into knowledge for the benefit of mankind and society [3]. That is, IoT would usher in a wide range of smart services and applications to cope with many of the challenges individuals and organizations face in their everyday lives via allowing humans and things to be connected with either anyone or anything in any place at any time [1][5].

IoT is an emerging wave for new service development and global economy growth, driven by billions of things being connected to the Internet [2]. IoT vision of pervasively connecting billions of things is able to interact with environment around us and receive information on its status that was previously not available by simply looking at a set of things [6]. In other words, while previous Intranets of Things, which is a local network of a set of things such as wireless sensor networks (WSNs), machine-to-machine (M2M), smart homes, and so on, can only extract regional information containing a specific content from the things, IoT could provide large scale, comprehensive, and historical information by collaborating between different Intranets of Things even if they have heterogeneity regarding devices, local communication technologies, and deployment goals. Therefore, IoT will achieve ’6A connectivity’ (i.e., any time, any one, any thing, any place, any service, and any network) eventually as the vision of ITU [1] and European project cluster (CERP-IoT) [4].

In IoT, an enormous number of potential devices (e.g., smart meters, sensors, tags, etc.) that are composed of Intranets of Things and would be connected each other by the Internet could support smart services and applications by/for diverse service providers with a wide range of Intranets of Things [4][7]. That is, each service provider might deploy devices, consisting of its service domain that is connected to the Internet with a wide variety of interconnection scenarios, suitable for its own service policies and objectives. This enables a common vision for the deployment of independent services and applications, characterized by a high degree of autonomous service operation, information transfer, network connectivity, and interoperability [4][6].

This article presents routing architecture of IoT with previously mentioned properties. The routing architecture shows various correlations between new components of IoT and traditional ones of the Internet. In addition, we explore new challenges the correlations bring, especially interoperability. The rest of the article goes as follows. In the next section, we address requirements of IoT. In section 3, we present our vision of routing architecture in IoT with a novel component, and we also explain inter-domain issues in IoT considering various interconnection scenarios. Finally, we present our conclusion in section 4.

II. 6A Connectivity

The 6A connectivity elements that give understanding characteristics of IoT paradigm were brought in [4] by European project cluster for IoT (CERP-IoT) firstly to explain about the ultimate stage of IoT; however, none of these elements were defined and sufficiently explained in the literature. In this section we address definitions of 6A connectivity elements. Some of these elements could be coined together according to their functionality

978-1-4799-3459-1/14/$31.00 ©2014 IEEE

- *Any TIME, Any PLACE*: The notion of ubiquitous and pervasive computing implies a connected world where smart gadgets will merge in aspects of everyday life invisibly, and communication networks will connect these gadgets seamlessly to facilitate anytime/anywhere communications. That is, these spatiotemporal connectivity elements indicate availability to get interoperability with all system entities including people and objects as well as services. Also, it means that services should support nomadicity, mobility, and global roaming to users.
- *Any ONE, Any THING, Any NETWORK*: Ubiquitous and pervasive computing suggests building an infrastructure of equivalent entities in which each entity provides, consumes data, and interacts with others. Those entities are considered as the main actors in such infrastructure. The actors collaborate to initiate and use services offered within this infrastructure. People, devices, and services including interconnection between them via any access networks or the Internet can be referred to as actors. Building this infrastructure of any ONE and any THING using any NETWORK remains the biggest challenges for driving future ubiquitous and pervasive computing.
- *Any SERVICE*: Relying on ubiquitous and pervasive computing infrastructure that allows on the go connectivity to any kind of entities (i.e., persons, devices, and services) using any available network, smart services can be provided with a better level of QoE. By understanding entities' situations, surrounding environments, and requirements, services can be provided to fulfill their goals and needs. This notion is the ultimate goal of the ubiquitous and pervasive computing.

III. Routing Architecture

This section proposes a novel component for IoT architecture, and this component could support achievement of the 6A connectivity requirements of IoT paradigm. Since routing as the control plane to provide data communication on IoT architecture is the core of main technologies, we address novel requirements for IoT paradigm in the routing architecture perspective, then present a novel component to solve problems and extend the traditional Internet element with various connection scenarios of elements on the Internet as one system, IoT architecture.

A. Autonomous System of Things

In this subsection, first we define a novel component of the Internet of Things (IoT) future-driven. The component denotes an *Autonomous System of Things* (ASoT). It is the very similar concept to an autonomous system (AS) on the Internet in that single operator configures infrastructure (i.e., a set of routers) and operates it by the same routing policies with its own decision. Here is the definition of ASs in the Internet mentioned in [8].

An autonomous system is a set of routers that shares the same routing policies. Various configurations for autonomous systems are possible, depending on how many exit points to outside networks are desired and whether the system should permit transit traffic. The Internet is a conglomeration of autonomous systems that define the administrative authority and the routing policies of different organizations.

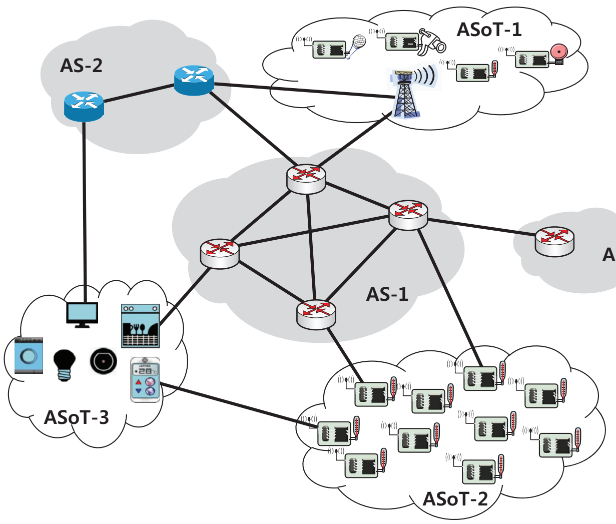

Fig. 1. IoT Routing Architecture

These independent ASs are made up of routers that run Interior Gateway Protocols (IGPs), such as Routing Information Protocol (RIP) [9], Open Shortest Path First (OSPF) [10], and Intermediate System-to-Intermediate System (IS-IS) [11] within their boundaries, and interconnect via an Exterior Gateway Protocol (EGP), or Border Gateway Protocol (BGP) [12]. IGPs direct packet forwarding paths for intra-domain routing inside a AS; an EGP on the other hand is exploited for inter-domain routing among ASs with a wide variety of connection scenarios. That is, exterior routing protocols were created to control the expansion of routing tables and to provide a more structured view of the Internet by segregating routing domains into separate administrations, called ASs, which each have their own independent routing policies and unique IGPs.

Since each service provider of IoT would be willing to get the independent smart service and infrastructure based on autonomous operation as mentioned in previous section, ASoTs could share such definition and properties of ASs, and also show extended characteristics as shown in Fig. 1:

1) *an ASoT is a set of diverse devices (e.g., smart meters, sensors, tags, etc.) sharing not only the same routing policies but also the same service policies*;

2) *ASoTs operate unique IGPs and interconnect to each other as well as traditional ASs via an EGP*.

However, there could be one question why do we take into account this new concept, ASoTs, even if it is similar to traditional ASs? To better rephrase this question, what are the limitations of the traditional ASs for things networks?

First, heterogeneity of many types of devices, technologies, and services is one of the biggest characteristics of the future-driven IoT as M. Zorzi *et al.* have mentioned in [6] and Fig. 1 shows. Practically, ASs also allow competability of machines for routing as in interconnection between AS-1 and AS-2 in Fig. 1; however, they adopt the same global standards of IGPs and the EGP. On the other hand, devices and communication technologies of IoT do not follow global standards. For instance, in wireless sensor networks (WSNs), there have already been hung numbers of routing technologies proposed for highly various network environments and application requirements. Moreover, while ASs aim at the IP routing service only, ASoT should accommodate a wide range of intelligent services.

In addition, devices of IoT are able to configure an ad hoc network, in which all nodes fulfill both routers for data forwarding and hosts as users, in an ASoT. Of course, multiple wired/wireless devices having TCP/IP stacks can connect to a gateway operating as one border router running BGP (i.e., they configure one model of traditional ASs). Typically, however, in an ASoT a large number of devices adopting either IP, 6lowpan with IP addresses, or WSNs' protocols without IP addresses self-organize an ad hoc network with its own routing policies involving decision of IGPs. It means that ASoTs settle on IGPs developed for ad hoc networks (e.g., mobile ad hoc networks (MANETs) or WSNs) since legacy IGPs, such as RIP, OSPF, or IS-IS, have restriction of protocol operations (i.e., scalability problems) due to limited hop counts or calculation overhead [8].

The third limitation could be the configuration property of logical structures for IGP routing: static or dynamic. ASs build proactive routing topology with static elements (i.e., typical routers), whereas ASoTs should allow dynamic or reactive topology via static elements as well as mobile elements.

Finally, on the Internet interconnectivity between ASs (i.e., inter-domain routing through an EGP) relies on policy routing due to domain independency and privacy while IGPs aim at efficient routing such as building the shortest path tree among a set of routers. On this wise, inter-domain routing between ASoTs of the IoT environment would base on policy routing. It would be more important to connect and contract between an AS and an ASoT due to a service level agreement (SLA) of the ASoT into the AS. However, the current EGP (i.e., BGP) cannot support such connectivity.

B. Inter-domain Routing

On the Internet, routing is the process of selecting logical paths along which to send network traffic. This routing process directs packet forwarding toward destination addresses (i.e., the transit of logically addressed packets from their source toward their ultimate destination) through intermediate nodes. It could be dynamically fulfilled via routing protocols including IGPs or the BGP. In other words, since an IP address for the purpose of network management is divided into two logical parts (i.e., the network prefix and the host identifier or rest field), all hosts on a subnetwork have the same network prefix. ASs share their network prefixes each other by BGP, and then each AS configures network topology according to its own routing policies based on the prefixes information by combination of BGP and IGPs like RIP or OSPF [8].

In order to share network prefixes of ASs (i.e., inter-domain routing), BGP provides many attributes to support policy routing based on contracts between independent ASs' operators for connectivity to the Internet. Also, to build secure connection for the policy routing, BGP makes the TCP connection between each pair of ASs. As shown Fig. 1, there are various scenarios of configuration of BGP pairing, depending on how many exit points to outside ASs are desired and whether ASs should permit transit traffic.

In addition, BGP connections between border routers running both BGP and EGPs inside an AS are referred to as Internal BGP (IBGP), whereas BGP connections between routers in separate ASs are referred to as External BGP (EBGP). Routers that are running IBGP are called transit routers when they carry the transit traffic going through the AS. In other words, EBGP is used to provide network prefixes between ASs, but IBGP carries out sharing network prefixes from outside ASs between inside border routers of an AS.

When we include ASoTs in this inter-domain routing, there might be three big features in the inter-domain connectivity scenarios: 1) *AS-to-ASoT with IP*, 2) *AS-to-ASoT with non IP*, and 3) *ASoT-to-ASoT*.

Firstly, an AS would be connected to an ASoT in which IP is working for intra-domain routing. Even if ASoTs adopt IP, they can follow different configuration models. For example, merely as an common AS, there are some border router(s), and every device connects with them. In this case, ASoTs are attached to ASs via BGP. On the other hand, an ASoT organizes an ad hoc network of devices adopting IP or 6lowpan. It aims at providing any point connection from ASs. So, via any device, data of smart services and applications can be requested and delivered. However, it bring other challenges. For any point connection, every device is able to run BGP so that there would be a huge number of TCP sessions for EBGP and IBGP. That is, this ASoT would be multi-homed to ASs with a large number of points by edge point nodes of the ASoT; moreover, to share network prefixes from outside, all the devices make IBGP connection based on TCP. Also, there might be many issues to cooperate and combine BGP with diverse new IGPs of MANETs.

Secondly, an ASoT, relying on one of a number of data-centric routing mechanisms or location-based routing mechanisms developed for wireless sensor networks (WSNs), is able to be connected to an AS based on IP routing. This inter-domain connectivity between different types of domains (i.e., IP-to-non IP interconnectivity) brings many new challenges. Because gateways, called sinks, in WSNs are commonly multiple, they should have methods to share network prefixes by EBGP and IBGP. Also, sinks can be selected dynamically so that all or edge point devices adopt BGP. Namely, there are the same problems about the scale of TCP sessions mentioned in the previous paragraph as well as for IBGP network prefixes should be shared by non-IP routing. In addition, all sinks should be able to understand all queries received by IP for all smart services, and then they should translate or reform them to packets suitable for non-IP routing. Finally, BGP would be altered or extended to support more various types of inter-domain connection and diverse services in high heterogeneous device environments.

Thirdly, different types of ASoTs can be connected each other since an ASoT could cooperate with the other ASoT for integrated smart services. For this, even if an ASoT does not take IP for routing, for connection to the Internet to become an element of IoT it should allocate at least one device running BGP and understanding all queries for all services.

IV. Conclusion

In this article, we explicitly classify and explain the ultimate requirements, called 6A connectivity, of the Internet of Things (IoT) paradigm European project cluster for IoT (CERP-IoT) has brought up. Then, for the requirements, we address a novel component of the Internet of Things (IoT), named an autonomous system of things (ASoT). The ASoT is able to accommodate many phases of IoT interoperability property. In addition, ASoT's interoperability to either other ASoTs or traditional autonomous systems (ASs) brings up new challenges on inter-domain routing because they show a wide variety of features regarding interconnectivity. We summarize the challenges for future-driven studies in terms of IoT routing architecture.

References

[1] ITU Internet Reports, "The Internet of Things," Nov. 2005.

[2] J.P. Conti, "The Internet of Thing," *IET Communications Engineer*, Vol. 4, No. 6, Dec.-Jan. 2006, pp. 20 - 25.

[3] J. Gubbi *et al.*, "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions," *Elsevier Future Generation Computer Systems*, Vol. 29, No. 7, Sep. 2013, pp. 1645-1660

[4] O. Vermesan *et al.*, "The Internet of Things - Strategic Research Roadmap," Cluster of European Research Projects on the Internet of Things (CERP-IoT), Retrieved Apr. 2011.

[5] J. Zhen *et al.*, "Guest Editorial: The Internet of Things," *IEEE Communications Magazin*, Vol. 49, No. 11, Nov. 2011, pp. 30–31.

[6] M. Zorzi *et al.*, "From Today's INTRAnet of Things to a Future INTERnet of Things: a Wireless- and Mobility-related View," *IEEE Wireless Communication*, Vol. 17, No. 6, Dec. 2010, pp. 44–51.

[7] N. Bui *et al.*, "The Internet of Energy: a Web-enabled Smart Grid System," *IEEE Network*, Vol. 26, No. 4, Jul. 2012, pp. 39–45.

[8] S. Halabi and D. McPherson, *Internet Routing Architectures*, 2nd Censitioin, Cisco Press, 2000.

[9] Hedrick, L. Charles, "Routing Information Protocol," IETF: The Internet Engineering Taskforce RFC 1058, 1988.

[10] J. Moy, "Open Shortest Path First (OSPF)," IETF: The Internet Engineering Taskforce RFC 2328, 1998.

[11] ISO, "Intermediate System to Intermediate System Routing Information Exchange Protocol for use in Conjunction with the Protocol for Providing the Connectionless-mode Network Service (ISO 8473)," ISO/IEC 10589:2002, Second Edition.

[12] Y. Rekhter and L. Tony, "A border gateway protocol 4 (BGP-4)," IETF: The Internet Engineering Taskforce RFC 1654, 1995.