IoT Network Implemented with NFV

MATSUDA Naohisa, TAKAGI Kenki, HORIUCHI Sho, AOKI Hiroki, AKUTAGAWA Aiko

Abstract

Under the rapid expansion of the IoT (Internet of Things) market that is associated with the sharp increase in IoT traffic, telecom carriers must be capable of dealing with the traffic requirements that vary between systems and of providing economic and stable networks. As a result, telecom carriers that only expect the volume of the traditional smart phone network traffic may often encounter technical difficulties and cost problems in trying to meet the demands of IoT users. At NEC we believe that IoT dedicated networking is essential to overcome these difficulties. This paper introduces the convenience, service flexibility and economy that can be brought about by the use of IoT dedicated networks. The paper goes on to describe the innovative technologies that will support implementation, such as the NFV (Network Functions Virtualization), MEC (Mobile Edge Computing) and MANO (Management and Orchestration), together with examples of their usages.

Keywords

IoT (Internet of Things), network, NFV, SDN, MEC, MANO, edge computing

1. Introduction

IoT is attracting significant attention due to its capability of connecting various devices from the real world to the network. Starting with simple data collection and visualization, the IoT is now evolving continuously to include the remote control of devices and optimization of the systems in use. It is expected that this trend will lead to an increase in and diversification of the connected devices, as well as an expansion in the patterns of data usage.

In this paper, we set forth the issues affecting the mobile networks that result from the expansion of the IoT. We then introduce countermeasures proposed by NEC, in the form of the "IoT-dedicated network".

2. Issues Involved in the Expansion of IoT Network Usage

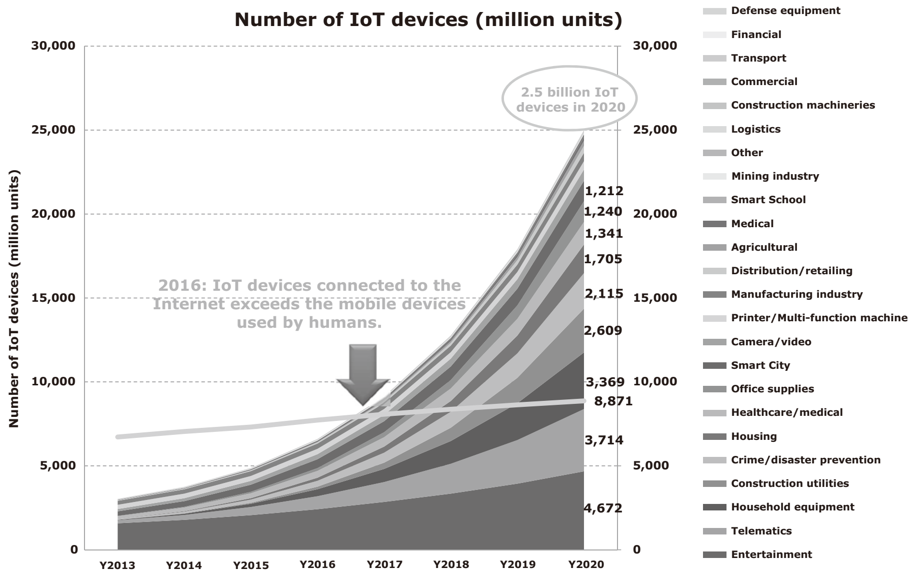
2.1 Increase in Traffic Amounts

In the pre-IoT world, networks were used mainly by humans and the number of connected devices was limited because of its dependency on the population size. Meanwhile, in the world of IoT, everything is connected to the network so that the potential of connection expands considerably.

Fig. 1 shows an estimation of the increase in the number of IoT devices. With about 5 billion units in 2015, the number of IoT devices is expected to multiply by about five times in the coming five years, or to be about 25 billion units in 2020. The growth in the number of IoT connected devices is expected to cause a rapid increase in the network traffic.

As will be described in section 2.2, the types of resources required by the smart phones and IoT devices differ due to the differences of their traffic properties. Consequently, if the equipment is extended under the presumption that smart phones occupy a large part of the traffic as before, those resources not required by the IoT would be extended unnecessarily. On the contrary, there would also be cases in which equipment extension following the properties of the IoT traffic would result in preparing excessive resources for the smart phone traffic management.

For example, it is known that the traffic of a sensor network composed of sensors including the Smart Me-



(Source: NEC (based on the forecast data of Gartner and GSMA))

Fig.1 Estimation of IoT devices.

ter used in the AMI contains a larger amount of control signals (hereinafter C-Plane) than the general user data signals (hereinafter U-Plane). If the network equipment for smart phones is extended to meet the traffic properties of such a sensor network, it is expected that the result would be optimum for the C-Plane but there would be significant excessive resources for the U-Plane.

As described above, extension of the existing smart phone oriented network equipment according to the increase in the IoT traffic has a potential of hyper-expansion in the CAPEX (CAPital EXpenditure) and OPEX (OPerating EXpenses).

2.2 Diversification of Traffic Requirements

(1) Diversification and technical progress of the traffic requirements

In the pre-IoT world where humans communicated with humans, the usage cases of networks were limited and traffic requirements such as the data quantity per device and the communication rate were fixed relatively. On the other hand, in the world of IoT where a large variety of devices are connected to the network, the traffic requirements are diversified considerably.

Table shows the general traffic requirements for each type of IoT service usage case.

For example, with the sensor network, the communication amount per device is low, so a high communication rate is not required, but the number of devices connected to the network is huge. The devices do not move about in the manner of the smart phones/cell phones. On the other hand, in the case of telematics such as in automated driving, the communication rate is required to be ultra-low latency as the devices keep on moving.

As seen here, in the world of IoT the forms of network usage are diversified. In addition, it is often difficult to meet traffic requirements that are in a mutually contradictory relationship.

Table Traffic requirements of each IoT service.

Use case	Connected devices	Data amount	Rate	Mobility
Sensor network	Very large	Very small	Low	No
Remote surveillance	Small	Large	High	No
Telematics	Large	Small	Very high	Yes
Digital signage	Small	Large	Low	No
Smart phones	Large	Medium	Medium	Yes

(2) Flexibility of required service specifications

Another issue posed by the differences in traffic requirements is the flexibility of service specifications, including the connection fee. **Fig. 2** shows a chart of connection fee asked for by each type of IoT usage case.

For example, the data amount per device is generally low in the sensor network so the quality of experience (QoE) of users, which is important with

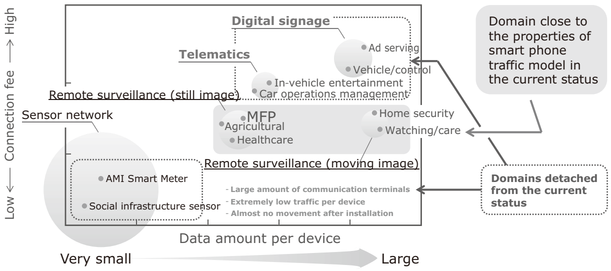


Fig.2 Chart of connection fee required for IoT services.

smart phones, is unnecessary. On the other hand, since a large number of devices in the sensor network need a communication function, the total connection fee would be enormous if a charge equivalent to the smart phone was billed for each device. In such a case, it would be difficult to maintain the service.

As seen in the above, if the IoT devices/applications are accommodated in an existing smart phone network, mismatching will occur between the required circuit service specifications and the connection fee, a situation that would not only hinder activation of the IoT but would also reduce the profitability of the telecom carriers.

3. Network Requirements in the IoT Age

In order to cope with the issues discussed so far, we at NEC believe that a network must provide the following capabilities.

(1) The capability of allowing equipment extensions according to the properties of the IoT traffic

The network should adopt an architecture suitable for the IoT that can optimize the network according to the properties of the IoT services and minimize the CAPEX/OPEX spent for equipment extensions, etc.

(2) The capability of dealing with diverse traffic requirements

To deal with diverse traffic requirements, the architecture should be flexible enough for enabling optimum deployment of network functions and resources according to usage cases and user status.

The network requirements for the IoT include the following.

- **Low-latency processing**
  The capability of responding to information and requests from terminals in the order of from 1 to 100 ms.
- **High traffic concentration (high speed, large capacity)**
  The capability of transmission and reception at high data rates with several terminals in a specific area (in case the traffic density in an area is increased locally).
- **Massive connections concentration**
  The capability of handling local increases in the connection density in a specific service area where multiple terminals are accommodated and of conducting data communications.
- **Peak traffic concentrations**
  The capability of dealing with peak traffic by preventing congestions and latency by means of dynamic modification of the network functions and resources.
- **Distributed processing**
  The capability of performing distributed processing by making use of core wireless and wireless access layers when the cloud processing of each service becomes excessive because a large number of terminals are accommodated over a broad area.

In addition, a network is also required to permit performance of the allocation of charge rates easily and to have customer management optimized for each IoT service; e.g., by assigning the bandwidth or separating the billing for each of the diverse traffic properties.

4. IoT-dedicated Networking with NFV

4.1 Concept of IoT-dedicated Network

We propose an IoT-dedicated network as the solution to the issues discussed above.

The IoT-dedicated network is a network optimized for IoT services and separated from the traditional smart phone oriented networks. It builds the EPC (Evolved Packet Core) nodes, including the MME (Mobility Management Entity), P-GW (Packet data network Gateway) and S-GW (Serving Gateway) for each service. **Fig. 3** shows the concept of the IoT-dedicated network and **Fig. 4** shows an example of its configuration.

For example, when building a dedicated sensor network, it is possible to build a mobile network that is tuned optimally according to the C-Plane/U-Plane ratio proper to a sensor network in which a large number of devices are connected.

By building such a network on the same platform as an ordinary network by using the NFV function, it is possible to extend the equipment according to the proper-

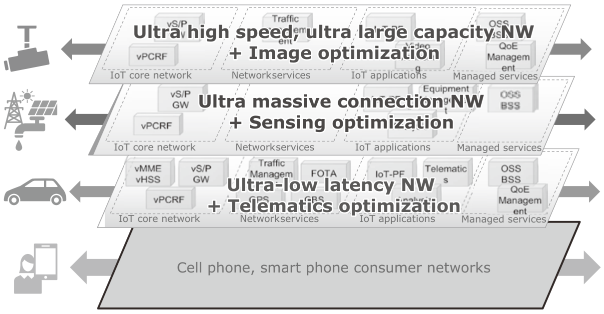


Fig.3 Concept of the IoT-dedicated network.

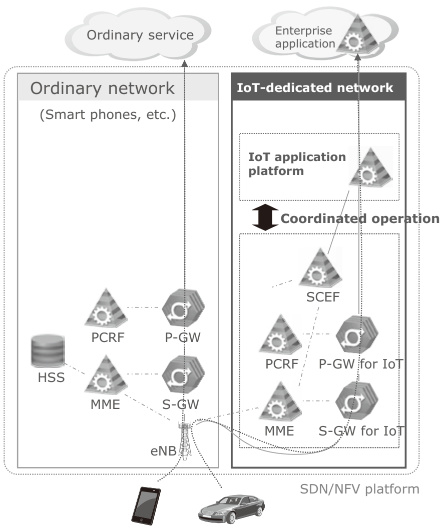


Fig.4 Example configuration of an IoT-dedicated network.

ties of IoT traffic with reduced CAPEX/OPEX.

Additionally, optimization of network services and resources using the MANO (Management and Orchestration) and use of low-latency processing using MEC (Mobile Edge Computing) enable the flexible handling of the diverse traffic requirements of the IoT.

In the following sections 4.2 to 4.4, we describe the technologies necessary for building an IoT-dedicated network.

4.2 NFV for Flexible Architecture

NFV is the technology that turns the network functions previously implemented using dedicated hardware into software, and runs it on a general-purpose server. The improvement in performance of general-purpose servers and the progress of server virtualization as seen with the hypervisor have made it possible to secure performance, scalability and reliability that is applicable even to carrier networks. By building a virtualized IoT-dedicated network utilizing NFV technology and by optimally deploying resources according to service requirements, it becomes possible to implement network infrastructures that are flexible, economical and optimized for the IoT.

4.3 MANO for Dynamic Configuration Changes

MANO is the orchestration function that operates and manages services and resources in an integrated manner in the NFV environment. When the virtualized IoT-dedicated networks are diffused, it becomes necessary to optimize the resource and function deployment of the entire network dynamically, as well as to introduce services quickly.

The use of MANO enables the dynamic processing of resource allocation to the core network as well as achieving flexible and quick configuration changes to the IoT-dedicated network according to the real-time traffic situation.

4.4 MEC

The MEC is the technology that performs the IT processing, which is usually done in the cloud of the Internet, at the edge of the mobile network and closer to the users (base stations, etc.). The use of MEC makes it possible to handle the service requirements that necessitate real-time processing or analysis of huge amounts of data without imposing too much burden on the core network and data center. For example, in the implementation of a mission-critical service that needs data transmission/reception at an ultra-low latency, such as for collision avoidance of automatically operated vehicles. Building the network by using MEC makes it possible to eliminate the effects of the transmission delay according to distance.

5. Applications to Usage Cases

5.1 Traffic Control

Fig. 5 shows an outline of a traffic control usage case. The network collects and analyzes big data (sensor information and images) from multiple IoT devices on the roads (vehicles, signal systems, etc.) Thereby predicting traffic situations such as collisions and congestions in real time provides notification via road-to-vehicle and inter-vehicle communications. This procedure enables traffic control for congestion easing, collision avoidance and coordinated driving.

This usage case is required to reduce the latency in road-to-vehicle and inter-vehicle communications to

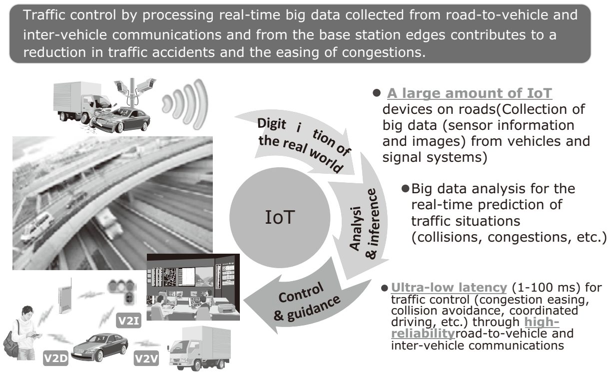


Fig.5 Traffic control.

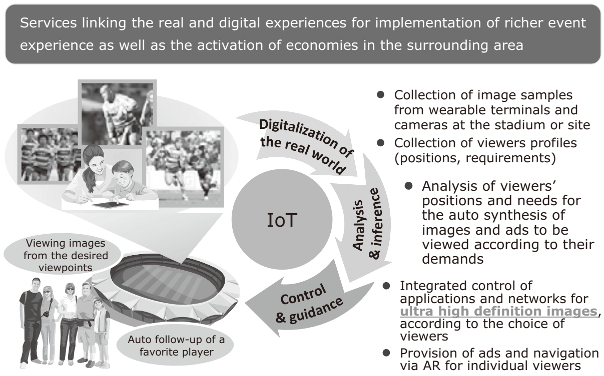


Fig. 6 Real-time image distribution to meet the demands of viewers.

between 1 and 100 ms. Particularly, in the mission-critical services such as in collision avoidance, the required latency should be achieved with a reliability close to 100%. It is also required to provide the vehicles moving at ultra high speeds with a highly reliable means of communication for connecting them with millions of IoT devices on the road. Nevertheless, with the traditional mobile network, the long data transmission distance between the IoT devices and the cloud system provides service results that produce propagation latency according to the distance. This leads potentially to latency in the road-to-vehicle and inter-vehicle communications being unable to be reduced to the range between 1 and 100 ms. In addition, optimization is also required to provide highly reliable communications for vehicles moving at ultrahigh speeds.

It is only after the IoT-dedicated network using the NFV is tuned optimally to meet the low latency and high reliability requirements specific to the traffic control and is built using the MEC that the service requirements for the low latency and high reliability can be fulfilled perfectly.

5.2 Real-time Image Distribution for a Stadium Audience

Fig. 6 shows an example of real-time image distributions according to the wishes of viewers as a usage case of IoT-based entertainment. When the 4K movie streaming of ultra high definition became popular, a viewer of a soccer game, for example, could automatically track the performance of a favorite player or refer to the related statistical information using the image attribution information. In the stadium, it is also possible to collect image samples from cameras and wearable terminals at the site, generate images from viewpoints according to the demands of spectators (viewers) and distribute them selectively. The spectators (viewers) can also find facilities in the stadium using the navigation service or receive ads matching their demands.

This usage case requires accommodation of huge communication traffic from multiple viewers, particularly for a large-scale event. To provide the individual viewers with ads and navigation with AR (Augmented Reality), it is also required to analyze the viewers' positions and demands and to distribute contents to them in real time (about 100 ms).

However, an ordinary mobile network may be unable to provide high-quality services due to congestion particularly when a large number of connections and a large amount of communication traffic is produced in a specific area. The IoT-dedicated network using NFV can tune the network functions and resources dynamically according to the traffic requirements for multiple connections and large capacities, and can meet the service requirements under such conditions.

6. Conclusion

In the above, we introduced the IoT-dedicated network as a network technology for supporting communications in the age in which the IoT is becoming more popular.

The technology introduced here can meet the diverse traffic requirements of the IoT and build a communication network that is safe, secure and economic.

At NEC, we believe that this solution can lead to improve the social value of the networks that support IoT and we are determined to pursue further social ideals based on applying the present technology.

Authors' Profiles

MATSUDA Naohisa
Manager
Carrier Services Division

TAKAGI Kenki
Manager
Carrier Services Division

HORIUCHI Sho
Assistant Manager
Carrier Services Division

AOKI Hiroki
Assistant Manager
Carrier Services Division

AKUTAGAWA Aiko
Assistant Manager
Carrier Services Division

The details about this paper can be seen at the following.

Related URL:

For Telecom Operators
http://www.nec.com/en/global/solutions/nsp/index.html

Information about the NEC Technical Journal

Thank you for reading the paper.
If you are interested in the NEC Technical Journal, you can also read other papers on our website.

Link to NEC Technical Journal website

Japanese | English

Vol.10 No.3 Special Issue on Telecom Carrier Solutions for New Value Creation

Vol.10 No.3
July 2016

Special Issue TOP