ISSN 1345-3041

Mar.2017 / Vol.157

Mitsubishi Electric

ADVANCE

Communication Technology and IoT

MITSUBISHI ELECTRIC
Changes for the Better

Mar. 2017 / Vol. 157
Mitsubishi Electric
ADVANCE
Communication Technology and IoT

• Editorial Inquiries
Kiyoshi Sakai
Corporate Total Productivity Management
& Environmental Programs
Fax: +81-3-3218-2465

• Product Inquiries
Eiji Taniguchi
Planning & Administration Dept.
Corporate Research & Development
Fax: +81-3-3218-2188

Katsutoshi Shirai
Marketing & Planning Department
Communication Networks Center
Fax: +81-6-6495-6610

Mitsubishi Electric Advance is published on line quarterly (in March, June, September, and December) by Mitsubishi Electric Corporation.

CONTENTS

Technical Reports

Precis

Mitsubishi Electric Corporation is committed to creating a safe and convenient society by developing technology for smart devices and systems for factories, buildings, automobiles, and other parts of life, interconnected using communication and information technologies. This special issue features advanced technologies in the field of wired and wireless communications for high-speed, highly reliable large-volume data acquisition from numerous devices, and solutions that create new value based on such data.

Overview

Author: *Tetsuya Yokotani**

Full-scale Deployment of IoT

Several years have passed since the term “Internet of Things (IoT)” became widely used. During these years, the industrial revolution brought about by IoT, such as Germany’s Industrie 4.0 project, has attracted much attention. IoT devices, which are to be mainly used in factories, can help the manufacturing industry to progress. In addition, the IoT as social infrastructure is expected to penetrate social life and business, and to play a significant role in building smart cities and communities in the future.

The challenges for the prevalence of IoT include steady technological development for building information communication platforms, innovative thinking to create new applications, and interactions between these. Such challenges have already been considered worldwide in various forums, international standardization organizations and academic conferences, etc. In Japan, the Smart IoT Acceleration Forum was established in the fall of 2015 under the leadership of the government to be used by industry, academia, and government, beyond organizational boundaries. The forum has actively discussed ways to tackle these challenges.

In view of such trends toward the deployment of IoT, the feature articles in this issue propose technologies that can support IoT information communication platforms. Building such platforms requires large-capacity, highly reliable communication infrastructure, an area network with the capacity to handle an enormous number of devices, a cloud capable of handling distributed processing, security for the cloud and various devices, etc. The feature articles describe Mitsubishi Electric’s initiatives to make these things happen by using its cutting-edge technologies.

I hope that in the near future, packages of organically combined cutting-edge technologies will provide the foundation for smart cities and communities worldwide.

**Professor at Kanazawa Institute of Technology*

Radio Access Base Station Technology for the Fifth-Generation Mobile Communications System

Authors: *Naohito Tomoe** and *Akinori Taira***

1. Introduction

With the goal of expanding IMT (international mobile telecommunications) for 2020 and beyond, the fifth-generation mobile communications system (5G) is expected to support various usage scenarios including (1) enhanced mobile broadband, (2) ultra-reliable and low-latency communications, and (3) massive machine-type communications, all of which are described in Recommendation ITU-R M.2083 (IMT Vision).[1]

As technology that contributes to the enhanced mobile broadband usage scenario above, this article reports on the base station configuration and experimental results of a massive multiple-input multiple-output (MIMO) system being developed for 20 Gbps transmission, substantially exceeding the peak data rate of 3 Gbps specified for the fourth-generation mobile communications system (4G).

2. Massive MIMO

Massive MIMO is a beam forming technology that can compensate the propagation loss in high-frequency band, and also improve system capacity with high order spatial multiplexing using digital MIMO precoder.

NTT Docomo, Inc. and Mitsubishi Electric Corporation proposed a massive MIMO system using high SHF bands (6 to 30 GHz) in a research and development project on the fifth-generation mobile communications system – High Data Rate and Low-Power-Consumption Radio Access Technologies with Ultra Higher-Frequency-Band and Wider-Bandwidth Massive MIMO, which invited industry and academia to offer R&D themes as part of the Research and Development Project for the Expansion of Radio Spectrum Resources for FY 2015, led by the Ministry of Internal Affairs and Communications. The proposal was adopted.[2]

Figure 1 shows a block diagram of a massive MIMO system using hybrid BF that combines analog BF and digital precoder currently under development in the 28 GHz band. The antenna/RF front end consists of multiple subarrays. Each subarray forms analog beams by controlling the amplitude and phase of each element. This leads to high antenna gain, and enables simultaneous transmission of multiple streams using single frequency resource. On the other hand, since the side-lobes of analog beam generate inter beam interference, it is suppressed by digital precoding. In hybrid BF, the digital MIMO processing section performs precoding for each beam, not for each antenna element. Thus, computational complexity can be remarkably reduced.[3]

3. Fundamental experiments for a massive MIMO system

In order to establish massive MIMO technology in the 28 GHz band, we collaborated with NTT Docomo on fundamental experiments on a massive MIMO system using the 44 GHz band.[4][5] In these

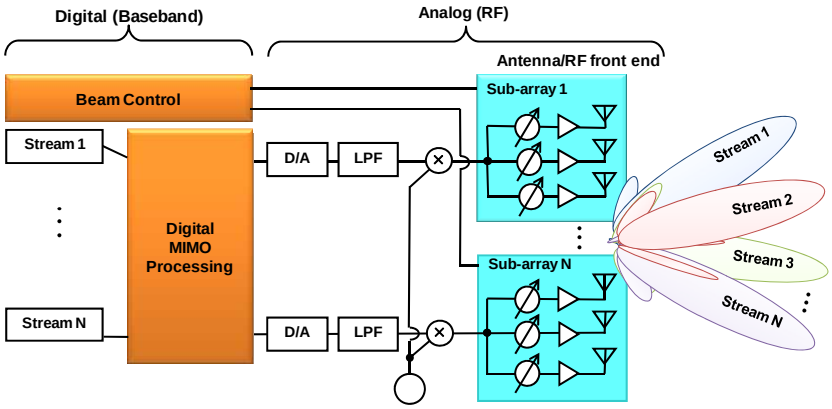


Fig. 1 Block diagram of a massive MIMO system with hybrid BF

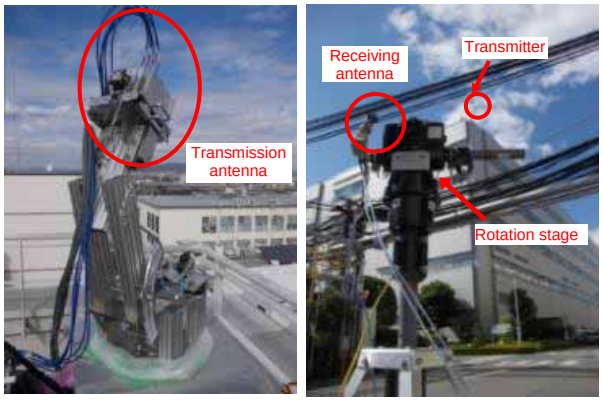
*Communication Networks Center **Information Technology R&D Center

experiments, we conducted a channel measurement in the EHF band (44 GHz) near the high SHF band in an open space condition evaluated the spectral efficiency of a massive MIMO base station considering interbeam interference of multibeam assignment, and clarified the feasibility of ultrahigh-speed transmission. Described below are the channel measurement results and computer simulation evaluations using channel models created from the measurement results.

Table 1 shows the major specifications. Figure 2 shows photographs of the transmitter and receiver used. The transmission antenna was a 48-element active phased array antenna (APAA) placed on the rooftop of a building 26 m in height. A broadband signal with a transmission frequency of 44 GHz and bandwidth of 100 MHz was radiated toward 25 areas while the beam direction was continuously switched. On the receiving side, using a horn antenna, the received signal strength indicator (RSSI) was measured with angle of arrival, while changing the elevation angle (30° to 160°; 0° for the direction directly under the antenna) and azimuth angle (0° to 360°).

Table 1 Major channel measurement parameters

Item	Specifications
Transmission antenna	48-element APAA (6 horizontal elements x 8 vertical elements) Gain: 17.2 dBi (half-width: 15°)
Frequency, bandwidth	44 GHz, 100 MHz
Transmitter location	Rooftop (height: 26 m)
Receiving antenna	Horn antenna Gain: 20.4 dBi (half-width: 20)
Receiver location	Measurement: 25 areas Location: Ground surface, rooftop (height: 11 m) Distance between the transmitter and receiver: 40 to 126 m



Transmitter side (APAA) Receiver side

Fig. 2 Experimental equipment

Figure 3 shows the measurement results obtained in two test areas on the rooftop and on a road. The horizontal axis represents the azimuth angle, and the vertical axis is the elevation angle. The color gradient expresses the received signal strength distribution when transmission beams were directed to the two areas. Since all areas were in line of sight environments, a direct path with strong signal intensity was observed in the transmitter direction. In addition, while some reflection paths were observed near the receiving points, their signal strength was clearly lower than that of the direct path, except for those reflected on a metal surface in the vicinity. In this experiment, we also measured the interference signal strength (side-lobe signal strength) distribution when transmission beams were directed to other test areas, in order to investigate the influence of interference between subarrays. It was found that in almost all areas, the direct path was dominant in the interference signal strength, while the reflected path components were very small.

Next, in order to evaluate the system throughput of the massive MIMO base station in this experimental environment, we used the measurement data to build a cluster channel model, shown in Fig. 4, and conducted a computer simulation. When building the channel model, we specified the propagation path between the transmitter and using the received signal strength and angle of arrival (AoA) at each measurement point, and also referring to the layout charts of the measurement locations, and then obtained the angle of departure and delay time. Considering the estimated reflection points as clusters made up of multiple scattered objects, we generated multipath fading.

Table 2 shows the major simulation parameters. A 16-subarray configuration was assumed at the base station side, and terminals equipped with a single nondirectional antenna were set at 16 areas. With the angular spread of each cluster set to 5°, 480 MHz bandwidth OFDM (orthogonal frequency division multiplexing) signal was transmitted. For multi-user MIMO involving 16 users, block diagonalization was performed. The difference in distance between the transmitter and receiver was treated as the difference in the SNR (signal-to-noise power ratio) to conduct the simulation.

Figure 5 shows the relationship between per-user transmission signal strength and system throughput. It is assumed that user terminals were placed in 16 areas that provided favorable conditions out of the 25 areas where the measurements were conducted. Since the distance from the transmitter varies depending on the measurement area, the average received signal strength varies. Figure 5 also shows the throughput broken down by area. As the per-user transmission signal strength increases, the receiver's SINR (signal-to-interference-plus-noise power ratio) increases. This leads to the selection of a higher-order modulation method/coding rate, resulting in high throughput. Figure 6 shows a simulation result as a panoramic view of the propagation experiment location, the positions of simultaneously communicating terminals, and each

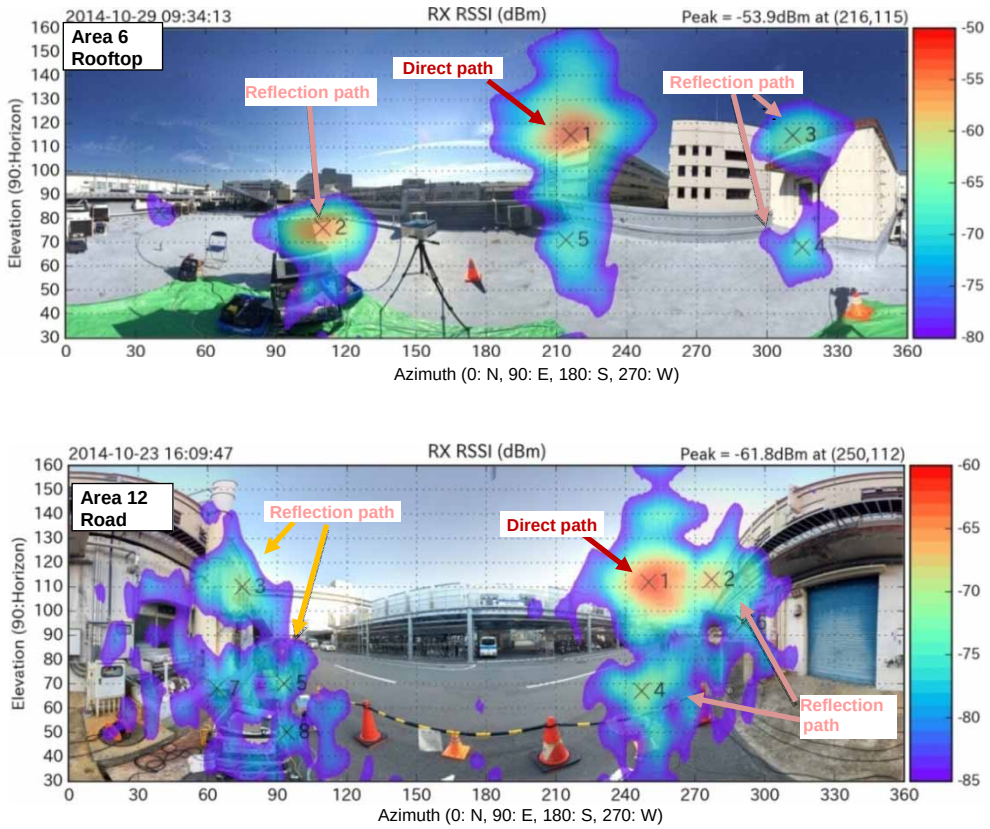


Fig. 3 Channel measurement results (RSSI and AoA)

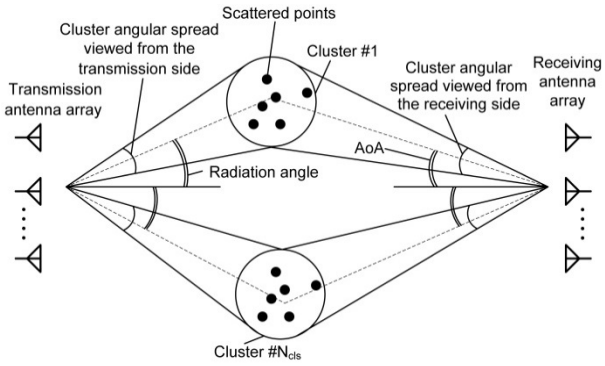


Fig. 4 Cluster-based MIMO channel model for computer simulation

Table 2 Simulation parameters

Item	Specifications
Transmission scheme	OFDM
Signal bandwidth	480 MHz
Modulation method	Adaptive modulation QPSK/16QAM/64QAM/256QAM
FEC	Turbo code (R=1/2, 2/3, 3/4)
TX subarray	2D planar array (48 elements)
Number of TX subarrays	16 (Element space: 10λ)
Number of users	16 users
RX antenna	Isotropic antenna x 1
RX NF	6 dB
Cluster angular spread	5° (TX, RX)
Precoding	Block diagonalization
Overhead	20%

terminal's throughput. It was found that the targeted 20 Gbps can be achieved with per-user transmission signal strength of 33 dBm, even when the terminals are distributed within an approx. 100 m radius.

4. Conclusion

In this article, we reported the base station configuration of a massive MIMO system being developed in pursuit of ultrafast transmission, and the results of fundamental experiments for the system. Going forward, we will continue to develop massive MIMO equipment to establish the technology for enhanced mobile broadband with high spectral efficiency as outlined above. We believe that the technology will contribute to solving the huge traffic demands and realizing various services and applications for 2020 and beyond.

This report includes part of the results of the research and development project on the fifth-generation mobile communications system commissioned by the Ministry of Internal Affairs and Communications. We sincerely thank the relevant parties.

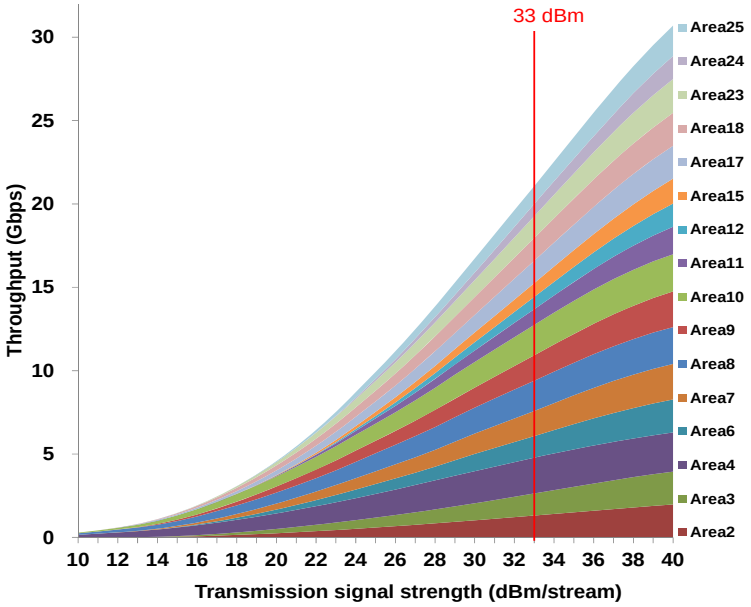
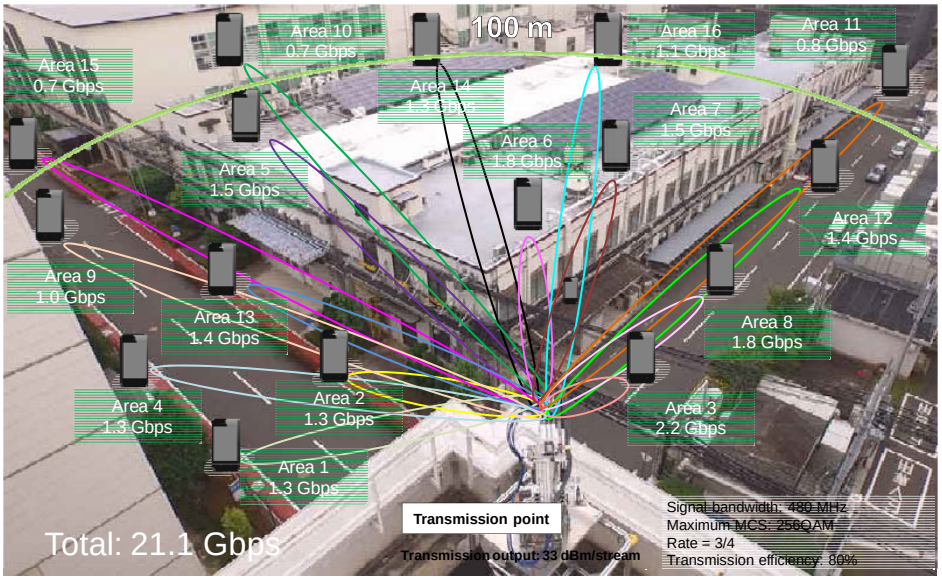


Fig. 5 Evaluation results of system throughput



Note: BF image in computer simulation using a channel model based on measurement result

Fig. 6 Experimental environment and simulation results for 16-user spatial multiplexing

References

(1) Recommendation ITU-R M.2083 (IMT Vision): Framework and overall objectives of the future development of IMT for 2020 and beyond (2015).
(2) Okumura, Y., et al.: 5G R&D Activities for High Data Rate and Low-Power-Consumption Radio Access Technologies with Higher-Frequency-Band and Wider-Bandwidth Massive MIMO, IEICE Technical Report, RCS2015-249 (2015).
(3) Okazaki, A., et al.: A Study on Next-Generation Wireless Access with Higher Frequency Bands," IEICE Technical Report, RCS2014-81 (2014).
(4) Okazaki, A., et al.: Multi-Beam Multiplexing MIMO Transmission and Evaluation by Outdoor Fundamental Experiment Trial at 44GHz Band, IEICE Technical Report, RCS2015-22 (2015).
(5) Taira, A., et al.: Evaluation of Multi-Beam Multiplexing Technologies for Massive MIMO System Based on the EHF-band Channel Measurement, 21st Asia-Pacific Conference on Communications (APCC), pp. 228-233 (2015).

Intelligent Hub Applicable to CC-Link IE Field Network

Authors: *Toshiyuki Nakayasu** and *Sachiko Taniguchi***

1. Introduction

Backed by the popularization of Ethernet,[1] which features high versatility and high speed at low cost, the demand for Ethernet-based industrial networks (N/Ws) has been growing. As industrial N/Ws require high-speed communication, precision time synchronization, enhanced reliability through redundancy of functions, etc., the demand for hubs with intelligent functions is expected to increase. Mitsubishi Electric Corporation has developed an Ethernet-based industrial N/W named CC-Link Industrial Ethernet (IE),[2] and has promoted this Ethernet-based industrial N/W through the CC-Link Partner Association of which the company is a board member.(1) As the next stage, the company developed an intelligent hub that can be applied to CC-Link IE.

This article describes the characteristics of the functions of this intelligent hub.

2. List of Requirements for Industrial N/Ws(2)

The requirements for industrial N/Ws are as follows (Fig. 1).

(1) Precision time synchronization

High-speed and high-precision synchronization control is required in communication among industrial devices for motion control system.

(2) Support of IP applications

Not only the use of applications specific to an industrial N/W, but also the use of IP applications such as FTP (File Transfer Protocol) and SNMP (Simple Network Management Protocol) is required.

(3) Enhanced redundancy/reliability

Enhanced redundancy/reliability is required in order to prevent the entire N/W from failing even if a failure occurs in a device or communication channel.

(4) Flexible wiring

It is necessary to flexibly arrange industrial devices by combining line, star, and ring network topologies.

3. Main Functions of the Intelligent Hub

Figure 2 shows the exterior view of the intelligent hub. Table 1 shows its major specifications.

This hub has a fixed delay transfer function for identifying a time synchronization frame for which precise synchronization control is needed, and performs cut-through forwarding with a certain time delay, thereby achieving precision time synchronization.

This hub adopts both the cut-through and

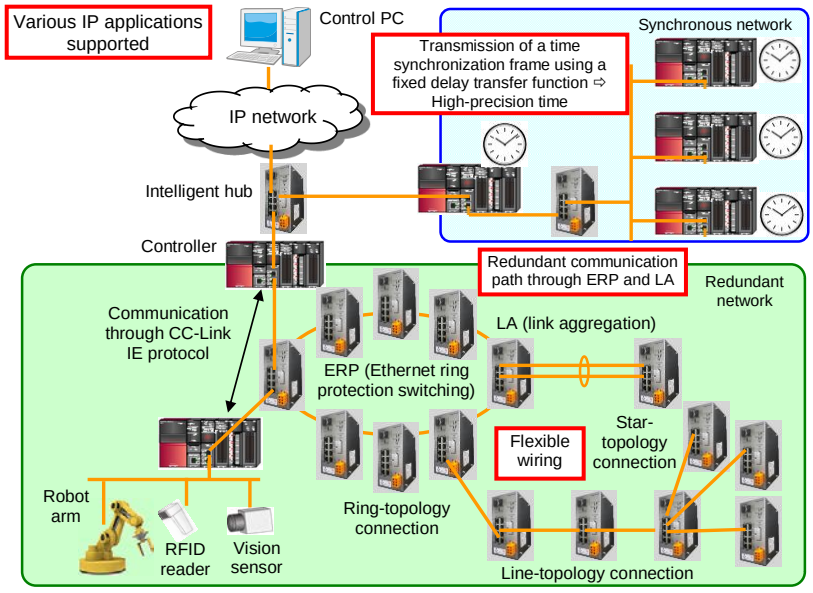


Fig. 1 Requirements for an industrial network

[1] Ethernet is a registered trademark owned by Fuji Xerox Co., Ltd.
[2] CC-Link is a registered trademark owned by CC-Link Partner Association.

*Communication Networks Center **Information Technology R&D Center

store-and-forward methods, allowing CC-Link IE and IP applications to be used in a network.

The device also includes redundancy functions of ERP (Ethernet Ring Protection Switching) and LA (link aggregation) in addition to a loop detection function for greater reliability.

Fig. 2 Exterior view of the intelligent hub

3.1 Fixed delay transfer function

Generally, hubs adopt the store-and-forward method, in which frames are stored and sent later in order of priority. In the store-and-forward method, the fluctuations of delay time ("delay fluctuations") become larger as the length of a frame to be transferred becomes longer. For this reason, in an industrial N/W that is configured with a star topology using a conventional hub, the delay fluctuations of time synchronization frames will be too large to perform precision synchronization control among CC-Link IE machines, which has posed a challenge.

Figure 3 shows the transfer method of the new intelligent hub. This hub identifies a time synchronization frame that requires punctuality ("high-priority frame"), and transfers it by cut-through forwarding with a fixed time delay needed for the transfer after a destination port is determined ("fixed delay transfer"). This reduces the delay time when transferring high-priority frames, and minimizes delay fluctuations.

On the other hand, frames for which punctuality is not required ("low-priority frames") are transferred using the store-and-forward method, as with the case of a conventional hub.

However, using these two types of transfer methods may cause a high-priority frame to be transmitted during the transmission of a low-priority frame. Furthermore, in some cases this device receives high-priority frames from several ports, causing coinciding multiple high-priority frame transmission processes to contend at a single port. This hinders contention control of the frame transmission. For this reason, modifications were made to suspend the transmission of low-priority frames and send high-priority frames, when frame transmission contention occurs between a high-priority frame and a low-priority frame; and to preferentially transfer a high-priority frame that should be transferred with a fixed delay, when frame transmission contention occurs between high-priority frames.

As a result, this hub has reduced the per-unit transfer delay time to about 1/4 of that of conventional hubs, and delay fluctuations to about 1/165. It ensures high speed, fixed delay transfer of high-priority frames for time synchronization, allowing precision synchronization control in star-topology N/Ws.

3.2 Redundancy function

In order to help users build highly reliable N/Ws,

Table 1 Major specifications of the intelligent hub

Item			Description
Transmission speed			10/100/1000 Mbps (full duplex)
Communication interface		Ethernet port (RJ-45)	8 ports
		Fiber-optic port (SFP)	2 ports (set on an exclusive basis to Ethernet ports)
Frame size (jumbo frames supported)			64 to 9,022 bytes (including VLAN)
Transfer method			Cut-through forwarding (fixed delay transfer) Store and forward
Number of MAC addresses learnable			Maximum 2,048
VLAN function		VLAN ID	0 to 4,095
Reliability and redundancy enhancement function	ERP	Number of ports that support ERP	2 ports
		ERP path switching time	Within 10 ms after failure occurs
	LA	Number of LA groups	4 groups (2 ports per group)
		LA path switching time	Within 1 s after failure occurs
	Loop detection	Loop detection frame method	Applicable to up to 8 VLAN IDs.
		CC-Link frame method	
Maintenance function		Log management	Operation logs, alarm logs
		Remote maintenance	Remote operation by Telnet, remote version upgrade, SNMP
		Others	Mirroring, initial settings and log storage using an SD card memory
Hardware specifications		Operation environment	0 to 60°C, 5 to 95% (no condensation)
		Rated input voltage	24 V DC (allowable voltage range 20.4 to 28.8 V DC)
		Rated input current	1.20 A
		External dimensions	147 (H) × 70 (W) × 122 (D) mm
		Mass	0.95 kg

RJ45: Registered Jack, SFP: Small Form Factor Pluggable, MAC: Media Access Control, VLAN: Virtual LAN, Telnet: Teletype network

the hub comes with a ring-topology N/W redundancy function, ITU-T G.8032 Ethernet Ring Protection (ERP).

Figure 4 shows an outline of the ERP operation when it is enabled. In ERP, one of the intelligent hubs configuring the ring is designated as an RPL (ring protection link) Owner, and frame loop is prevented by one of the RPL Owner ports blocking traffic on the ring link. If any failure occurs, the communication can be continued by blocking the ring link at the ports of the hubs in the part where the failure is detected, and at the same time opening the blocked RPL Owner's port to switch the blocked part on the ring.

The control frames of Ethernet OAM (ITU-T Y.1731) are used to check the connectivity between neighboring intelligent hubs in the ring, and to notify all intelligent hubs in the ring of the failure detection/recovery states. This hub has reduced the transmission cycle of Ethernet OAM connectivity check frames, which has been set at 3.33 ms or longer in G.8032 Recommendation, to 1 ms, to shorten the failure detection time.

As a result, in a N/W using 16 intelligent hubs, the switching time has been reduced to less than 5 ms (actually measured) when a failure occurs, which is 1/10 of the switching time of 50 ms set by G.8032 Recommendation for ERP.

3.3 Loop detection function

If a loop path is formed as a result of miswiring or other causes, broadcast traffic may spike on the loop path (a broadcast storm), possibly causing not only a communication problem but also a serious failure such as a system crash. To resolve this issue, this hub has a function to support a new loop detection frame method, in addition to the conventional function of detecting a loop from the flow rate of CC-Link frames sent from CC-Link IE devices. The loop detection frame method periodically sends a frame defined as that for detecting a loop ("loop detection frame"), and detects a loop upon receipt of the loop detection frame sent from the same hub that receives the frame.

The loop detection frame method uses the loop detection frame to detect a loop path and collect information on a port with the lowest priority in the loop path, and blocks only the port of the lowest priority. Furthermore, by setting the priority of the port that has been used for communication prior to the loop formation to a priority higher than that of the port newly added to the link, the communication path can be avoided from being switched between before and after the loop formation, thus avoiding CC-Link IE communication disconnection and network separation.

For the loop detection frame method, three types of port state are defined as shown in Table 2. A port that has been used in the communication prior to the loop formation is defined as being in the [operation] state; a port newly added to the link is the [main signal filtering] state; and a port blocked as a result of the detection of a loop is the [all frame filtering] state. The order of priority of these port states is defined as [operation] >

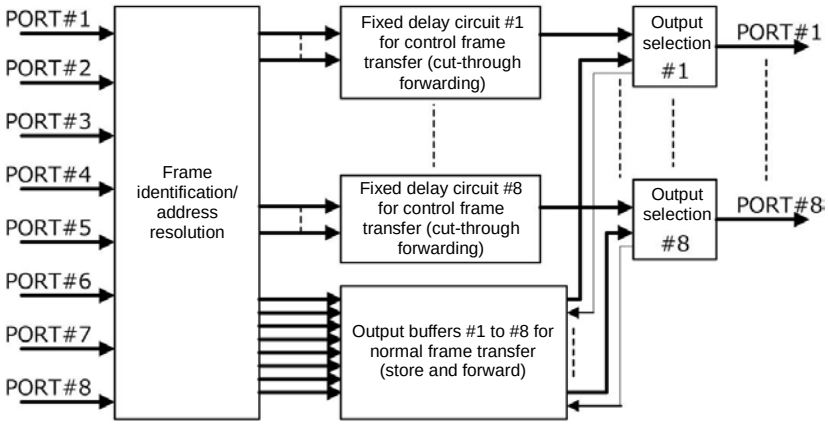
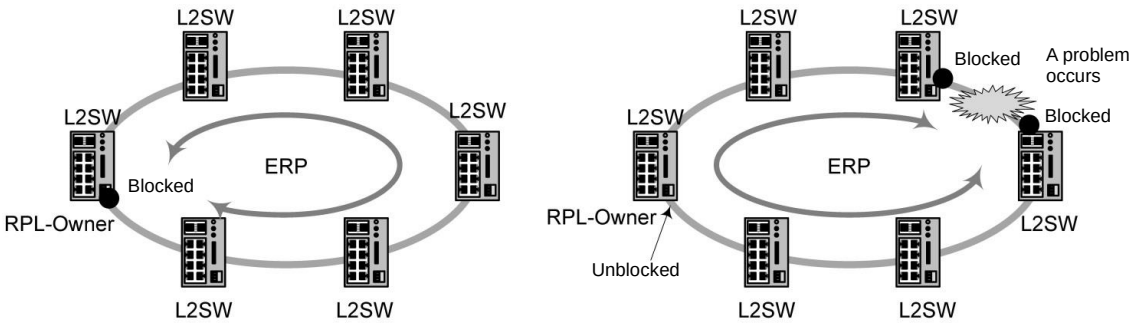


Fig. 3 Frame transfer method of the developed intelligent hub



(1) There is no problem (blocked at the RPL Owner) **(2) There is a problem (blocked at the fault-detection point)**

Fig. 4 Operation outline of Ethernet Ring Protection (ERP)

Table 2 Port state definition

Port state	Priority	Can the main signal be forwarded?	Loop detection frame	
			Can it be forwarded?	Can it be transmitted?
Operation	High	Yes	Yes	Yes
Main signal filtering	Medium	No	Yes	Yes
All frame filtering	Low	No	No	Yes

[main signal filtering] > [all frame filtering]. In the case of several hubs in an identical port state, a hub with smaller MAC address is given higher priority. In the case of ports of the same hub, a port with a smaller port number is given a higher priority in the hub.

Specific examples are described below using Fig. 5. Of the MAC addresses of the three intelligent hubs, it is assumed that the MAC address of intelligent hub #2 is the largest.

(1) Before loop formation

Synchronous communication is in progress between CC-Link IE devices via the intelligent hubs. The ports on the communication path are in the [operation] state.

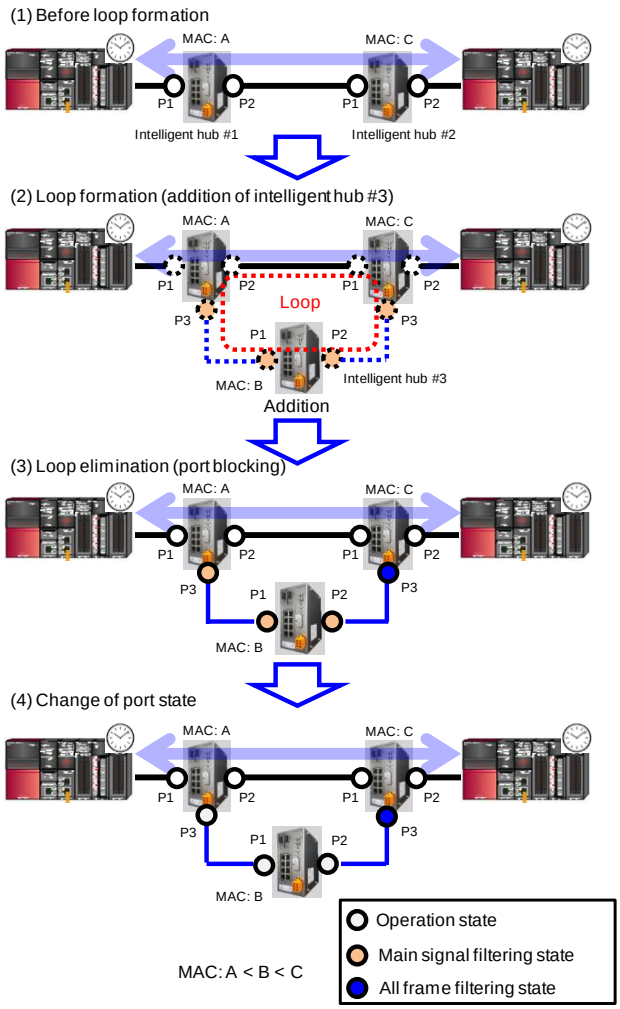


Fig. 5 Example of eliminating a loop path using the loop detection frame method

(2) Loop formation

When intelligent hub #3 is added, a port linked with the loop detection function enabled is switched to the [main signal filtering] state. All the intelligent hubs on the loop path detect a loop upon receipt of the loop detection frames transmitted by themselves. Stored in each loop detection frame are the state of the lowest-priority port and the MAC address of the intelligent hub that has the lowest-priority port ("lowest-priority port information").

(3) Elimination of the loop path by port blocking

The intelligent hub that detects a loop switches its own lowest-priority port (if any) to the [all frame filtering] state, based on the lowest-priority port information of the loop detection frame. In Fig. 5, P3 of intelligent hub #2, which has a port in the [main signal filtering] state with the lowest priority (i.e., the largest MAC address), is switched to the [all frame filtering] state.

(4) Change of the port state

Each intelligent hub switches the port state from the [main signal filtering] to [operation] by halting receiving the loop detection frame sent by itself for a certain period of time, as a result of (3) above.

The loop detection frame method makes it possible to avoid communication path switching before and after loop formation, by setting the port that has been used in communication prior to the loop formation to the [operation] state, and setting the newly linked port to the [main signal filtering] state. Furthermore, this method determines which port should be blocked based on the total time of transmission cycle of the loop detection frame (one second) plus the propagation delay time of the loop detection frame, thereby shortening the time taken to eliminate a loop.

4. Conclusion

This article has described the fixed delay transfer function, ERP, and loop detection function as the features of our new intelligent hub.

Going forward, we will strive to improve the environmental resistance and to extend the specifications, in addition to enhancing the functions of present models with a view to applying the intelligent hub functions to the next-generation industrial N/Ws. Thus, we will expand the use of our intelligent hubs even outside the field of industrial N/Ws, to capture a larger share of the intelligent hub market.

References

(1) Hisafumi, K.: CC-Link IE Field Network, Mitsubishi Denki Giho, 84, No. 3, 23-26 (2010)

(2) Tatsuhiko, N., et al.: Introduction to Industrial Ethernet, CQ Publishing Co., Ltd., 2009

88-Channel 8-Degree Optical Cross-Connect System

Authors: *Hajime Yamasaki** and *Yoshiaki Hamada**

1. Introduction

Wavelength division multiplexing (WDM) transmission systems for metro and core networks must allow for higher-capacity communications at higher speed with greater reliability. However, it is also necessary to reduce the ever-increasing capital expenditure/operating expenditure (CAPEX/OPEX) of networks, and to improve network efficiency. An optimal solution to such demand is a multi-degree optical cross-connect system, which allows for high-capacity WDM transmission and supports optical switching. To use this type of system in practice, both multi-degree technology and mesh network management technology are necessary. Using these technologies, Mitsubishi Electric Corporation recently developed a highly extensible 88-channel 8-degree optical cross-connect (OXC) system for metro and core networks.

2. Multi-degree Technology

Conventionally, the use of ring/linear topologies has been the mainstream for metro and core networks. When establishing communication channels in two or more directions, these topologies require the installation of multiple units of WDM equipment in one station building, which makes it harder to secure the requisite equipment space and power supply. Accordingly, there is a trend toward the use of a mesh topology using a multi-degree optical cross-connect system (Fig. 1).

Such multi-degree communication requires wavelength cross-connect technology, which allows the wavelength and direction settings to be remotely changed without affecting existing optical signals. Furthermore, for practical use, it is indispensable to use an ultra-long-haul, high-capacity transmission technology that allows for flexible telecommunication across any route.

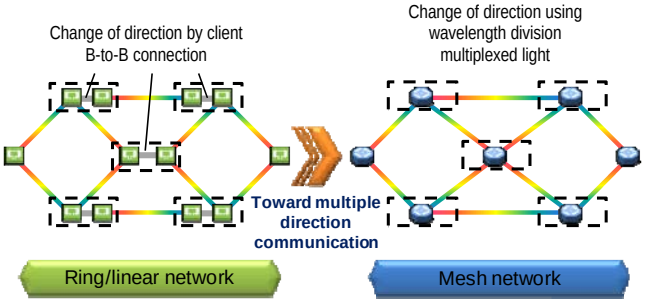


Fig. 1 Migration of the network topology

2.1 Wavelength cross-connect technology

The wavelength cross-connect technology switches to wavelengths in any direction and grouped wavelengths that are in different directions or that are multiplexed/demultiplexed at the station itself.

We have developed an economical wavelength cross-connect technology capable of adding/removing a channel in each direction, using a compact wavelength selective switch (WSS). Figures 2 and 3 show an exterior view and a functional schematic view of the equipment, respectively. The wavelength cross-connect technology is represented by the wavelength cross-connect (WXC) function part equipped with the above WSS. Mesh switching is enabled via multiple WXC function parts, each of which operates in a different direction and is connected using an optical fiber to the equipment inside it.

A configuration like this allows for remote switching of directions, without affecting the quality of signals in directions other than those involved in the switching. This contributes to flexible network building. The key device, the WSS, uses liquid crystal on silicon (LCoS) elements, which can also be used for future flexible-grid switches.

In addition to the wavelength cross-connect technology, we have developed the CDC (colorless, directionless, and contentionless) function, which enables a network to be built flexibly. Conventionally, fibers are reconfigured manually in order to switch the wavelength or direction each time a path is built. The CDC function allows all wavelengths and directions to be switched freely and remotely by simply connecting a fiber to a given port in advance. The MUX/DEMUX function

Fig. 2 Exterior view of the equipment

*Communication Networks Center

parts and MSW function part, which make the CDC function work, are configured to be functionally independent from each other, thereby enhancing the wavelength/directional independence. This configuration has made it possible to suppress physical wavelength interference to secure flexibility, and to prevent the signals affecting other directions when a wavelength/direction is added or removed, or when any failure occurs.

2.2 Ultra-long-haul and high-capacity transmission technology

In a mesh network, there exist multiple channels for an optical signal from its starting point to its end point. If the transmission performance is poor, 3R regeneration that involves photoelectric conversion is necessary, which lessens the advantage of a mesh network: flexible routing. In particular, when a 100 Gbps or faster signal is transmitted using WDM, there is an issue regarding compensation for the narrowing of an optical signal's bandwidth resulting from multistage relaying at OXC nodes on the route, as well as optical signal degradation as a result of a reduction in the optical signal-to-noise ratio (OSNR). We have developed spectral shaping technology for optical signals and forward error correction technology, enabling ultra-long-haul, high-capacity transmission to be put into practical use.

The spectral shaping technology was used to suppress the optical signal degradation caused by the narrowing of an optical signal's bandwidth. By applying pre-emphasis to the high-frequency components of the optical signal using an electrical filter within the transmitter, the spectral narrowing at an OXC node is compensated.[1] Figure 4 shows the difference in the transmission performance during multistage relay with and without compensation for the narrowing. The Q-penalty (Q is a signal quality parameter) was calculated with and without compensation for the narrowing when a DP-QPSK (dual polarization-quadrature shift keying) signal was transmitted through multiple relay stages at a transmission speed of 128 Gbps. The frequency interval of the OXC-node WSS passband was set to 50 GHz. Figure 4(a) shows the effect on the optical spectrum of the waveform. Figure 4(b) shows that as the number of OXC nodes that a signal passes increases, the effect of compensation for the narrowing becomes more evident. When the number of nodes involved is 10, the Q-penalty is expected to be improved by 0.5 dB or more.

We also used the error correction technology with a view to receiving optical signals at a low OSNR. We developed a soft-decision, low-density parity-check code using a multi-spatial combination method. This code is combined with a hard-decision code to form a concatenated forward error correction (FEC) system which achieves high correction performance with a coding gain of 12 dB.[2]

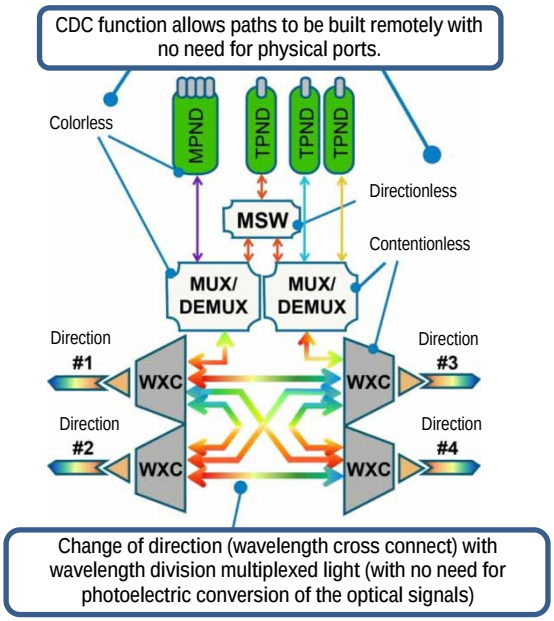
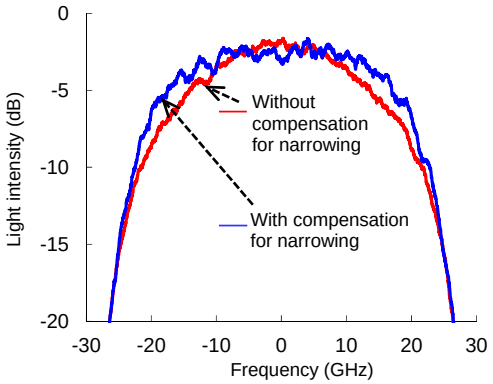
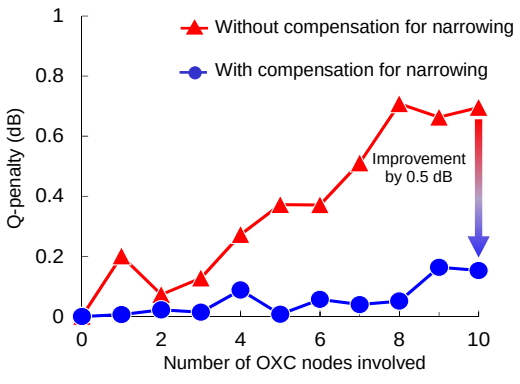


Fig. 3 Wavelength cross-connect configuration



(a) Optical spectrum of the waveform



(b) Q-penalty

Fig. 4 Transmission performance when transmitting a signal through multiple OXC nodes

3. Mesh Network Management Technology

In a conventional ring topology, reliability is ensured by a redundant architecture to provide 1+1 protection. Furthermore, a network management system (NMS), which monitors and controls a network including the equipment, etc., has been a suitable distributed monitoring system for networks that are each independent rings. On the other hand, in a mesh topology in which multiple routes can be configured, services can continue to be provided without a break even if multiple problems occur in the network by using multi-route redundancy. As seamless connections make networks more complex, however, a layer management technique is becoming important to ease the burden of maintenance work.

3.1 Multi-route redundancy

By combining the wavelength restoration technology for sharing backup route resources with the 1+1 protection technology, we have introduced multi-route redundancy to balance reliability and economy.

3.1.1 Wavelength restoration technology

The multi-route redundancy technology supports advance reservation of wavelength resources for restoration as part of the wavelength restoration functions. In the case of advance reservation restoration, a bypass route and bypass wavelength are registered in the NMS in advance for the optical path on the current route. When a failure occurs, the backup optical path is activated on the registered bypass route, and the failed route is switched to the backup path. Thus, by registering optical paths on multiple backup routes for the optical path on the current route, signals can be restored even when there are multiple concurrent problems. In addition, the wavelength restoration function that reserves wavelength resources for restoration signals the failure of the optical path on the route in use, and sets up a reserve optical path. This allows for resource sharing on backup routes for the optical paths on multiple routes in current use, thus improving the efficiency of wavelength resource usage.

3.1.2 3-route protection technology

In addition, we have effected 3-route protection by combining 1+1 protection with advance reservation wavelength restoration. Figure 5 shows a route diagram for 3-route optical path protection. For each optical path on the route in current use and each optical path on the backup route for 1+1 protection, multiple bypass routes are registered in advance in the NMS. If a problem occurs in the optical path on the route in current use or the optical path on the backup route, the 1+1 protection automatically switches the failed optical path. The wavelength restoration function then sets up a preregistered bypass route as a new backup-route optical path. This makes it possible to constantly maintain 1+1 protection even when multiple failures occur concurrently.

3.2 Layer management technology

In a ring network, the NMS monitors each ring as an independent network in a distributed manner. In a mesh network, on the other hand, there is no connection gap within a network, which requires seamless monitoring even when the number of devices in the network increases. Given this, we have divided the NMS into two functional parts: the main server in charge of network management and the sub-server in charge of device management. Figure 6 shows the NMS server configuration. This configuration allows the number of sub-servers to be increased as the number of devices in the network increases. As a result, seamless network management can be performed by the main server, achieving large-scale monitoring in a mesh network.

Moreover, as management networks become more complex, it is vital to reduce the operators' workload. We launched the development of an NMS client pursuing the concept of a user-friendly GUI (graphical user interface), which enables intuitive operation of the network by the operators. The equipment in a network and the optical paths passing through the network can be centrally controlled on the network management screen, which is one of the main displays. This centralized operation has been implemented by making

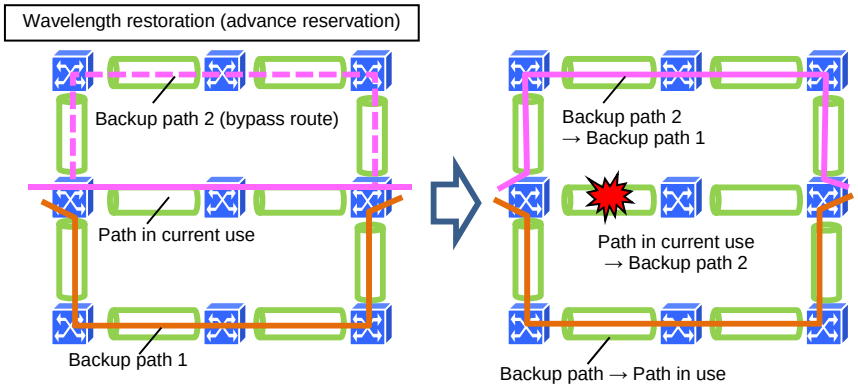


Fig. 5 Overview of the 3-route protection

the NMS perform not only network management but also equipment control handled for it by an EMS (equipment management system).

4. Future Technologies

In order to achieve high-speed, high-capacity transmission at speeds of 400 Gbps or 1 Tbps, we are developing a signal transmission technique using DP-16QAM modulation and multi-subcarrier transmission technology.(3) In addition, we are pursuing an OXC system with higher efficiency to enable a network to accommodate a larger number of routes. This system comes with a path computation element (PCE)(4) function that can derive the optimum combination of modulation format and wavelength grid, and can calculate the optimum optical paths taking the required bandwidths and transmission distances into consideration.

In the future, we will improve the management interface to higher-order devices to achieve integrated monitoring and control of transport network layers including integration packs that use orchestrator functions. Furthermore, discussions are underway on subjects such as online PCE functions to make optimal failure recovery possible over multiple layers of layer-integrated networks, transport SDN usage cases, and interconnection.(5)

5. Conclusion

In this article, we have described the technologies we have developed for wavelength cross-connect and ultra-long-haul, high-capacity transmission to put multi-degree technology into practice for 88-channel 8-degree OXC systems, as well as those for the multi-route redundancy and layer management that constitute the mesh network management technology. It is our hope that these technologies will improve the speed, capacity, and reliability of current metro and core networks, and help reduce CAPEX/OPEX.

The results on which the development described here are based in part derived from the following projects commissioned by the National Institute of Information and Communications Technology (NICT): Research and Development on Photonic Transparent Transmission Technologies (λ-Reach Project), and Research and Development on Optical Frequency/Phase Control Optical Relay Transmission Technologies.

References

(1) Sano H., et al.: A Study of Non-Nyquist LPF for Subcarrier Multiplexed Transmission in ROADM Systems, the Institute of Electronics, Information and Communication Engineers (IEICE), Society Conference, B-10-48, 2015.
(2) Sugihara, K., et al.: MSSC-LDPC: Multiple-Structured Spatially-Coupled type LDPC, OFC/NFOEC 2013, OM2B.4, 2013.
(3) Noguchi Y., et al.: A Study of Spectral Shaping for Subcarrier-Multiplexed DP-16QAM Signals, 29th OCS Symposium, P-8, 2015.
(4) Horiuchi E., et al.: Network Control, Operations and Management for Photonic Networks, IEICE Technical Report, Vol. 111, No. 475, PN2011-92, pp. 61-66, 2012.
(5) Mitsubishi Electric News Release, The World's First Success in Nationwide Flow/Path Setting in Interconnected Multiple Different Optical Transport Networks with Multi-SDN Controllers, http://www.mitsubishielectric.co.jp/news/2015/0420.pdf, 2015.

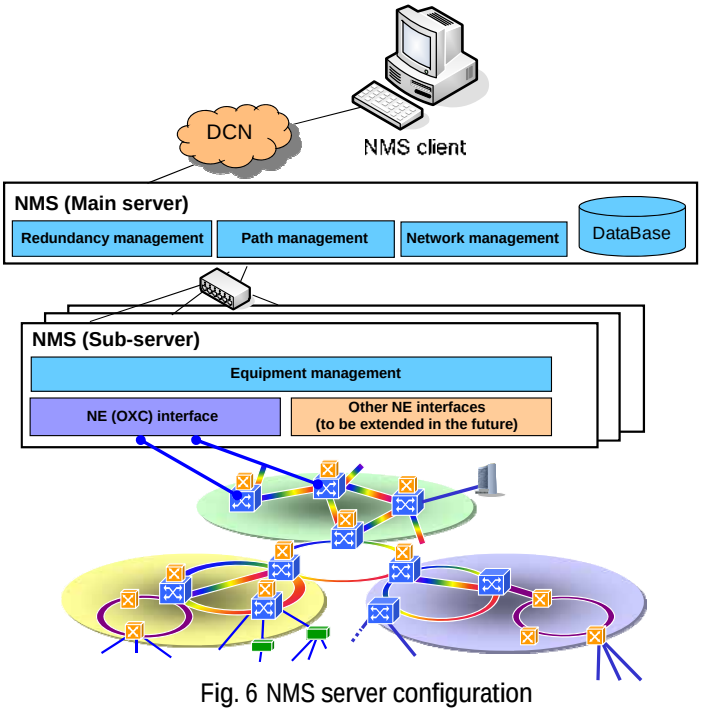


Fig. 6 NMS server configuration

Architecture of DIAPLANET – An IoT Platform

Authors: *Takayuki Tamura** and *Masahiro Ito***

1. Introduction

Since April 2015, Mitsubishi Electric Corporation has provided its DIAPLANET smart managed cloud services as a common platform to improve the efficiency of development and operation of IoT (Internet of Things) systems. This article describes the architecture of DIAPLANET, in terms of the functions for connecting various devices and managing various device data.

2. Configuration of the IoT Platform

An IoT system, which connects various things to a network and establishes remote monitoring and remote management, requires a broad range of functions including data acquisition and data transmission/receiving through gateways (GWs) and in the cloud. In addition to application servers with general middleware for web applications, the DIAPLANET platform as a service (PaaS) provides a machine-to-machine (M2M) server with IoT platform functions required to connect devices and GWs, thereby improving the efficiency of IoT system development. Figure 1 shows a schematic view of an IoT system based on the DIAPLANET PaaS.

As a basic function for server applications in the cloud to use device data, the M2M server receives data from a GW/edge device and stores it in the database (data accumulation function). The default settings for the database are as a "Not only SQL (NoSQL)" database. The database is further used as a relational database and file server depending on the application requirements. NoSQL can support key-based distribution of data over multiple servers, and can handle an increased data volume by adding servers to scale up.

The M2M server also provides a function to send a request from a server application to GW/edge devices (control messaging function), as explained in detail later. When the number of GW/edge devices and user terminals to be connected increases, the situation is dealt with by adding M2M servers and application servers to scale up. This may cause the M2M server connected to GW/edge devices and the application

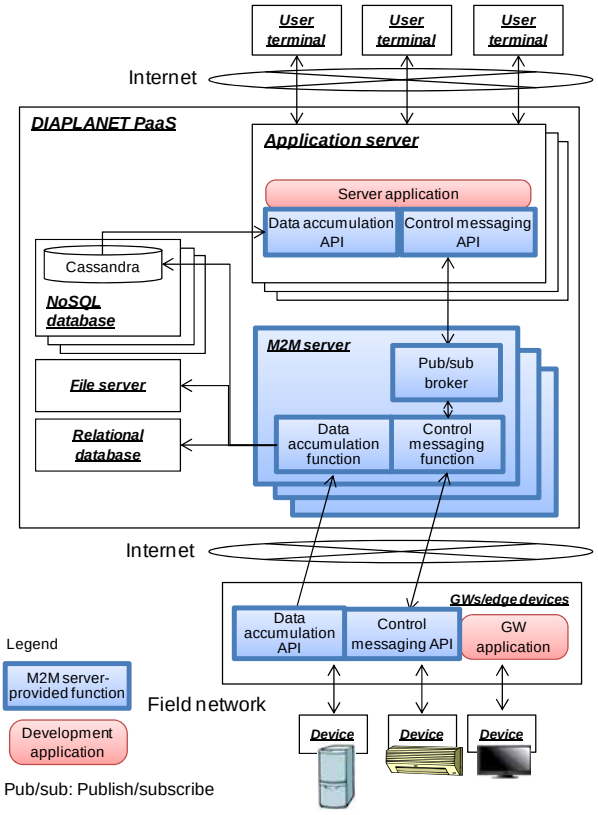


Fig. 1 Overview of IoT system based on DIAPLANET PaaS

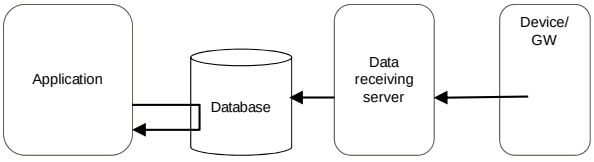
*Information Technology R&D Center **Information Systems & Network Service Division

server connected to user terminals to differ each time the number of servers is increased. This problem is addressed by relaying between the M2M servers and application servers via a pub/sub broker to process communications based on topic names instead of the IP addresses of these servers.

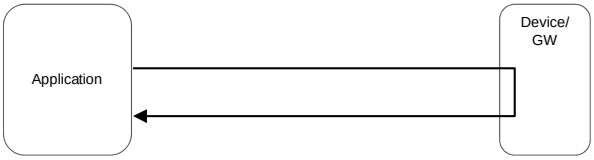
3. Abstraction of Message Exchange Patterns

For exchanging messages between a device and an application to acquire device data, two types of patterns as shown in Fig. 2 can be used. The data accumulation function of the M2M server is based on the notification type pattern in Fig. 2(a) in which a device/GW acts as a client. With this function, the environment in which the device/GW is installed can be safely connected to the Internet via an NAT (network address translation) router or other device.

On the other hand, in the request-response type pattern shown in Fig. 2(b), which is seen in applications for monitoring/managing devices in a local network, a device/GW acts as a server. When using an application of this type as-is in the cloud, it is vital to employ a virtual private network (VPN) for the server function of the device/GW to be accessed without exposing it on the Internet.



(a) Notification type (device/GW = client)



(b) Request-response type (device/GW = server)

Fig. 2 Message exchange patterns for device data acquisition

The control messaging application program interface (API) provided by the M2M server supplies the server application with the request-response type message exchange pattern, with a device/GW acting as a client. This allows a request-response type application to migrate to the cloud without a VPN or significant modification to the application. Figure 3 shows a block diagram that indicates the detailed implementation of the request-response type message exchange pattern using the control messaging API of the M2M server. First, a request ("msg") is sent through pub/sub communication from the cloud to the GW via a pub/sub broker at the M2M server. Next, the response ("res") is returned through pub/sub communication from the GW to the cloud. The topic used when sending the request is the ID ("devA") of the destination GW/edge device. The topic used when returning the response is the value ("resTopic") generated by the cloud-side API that is sent together with the request.

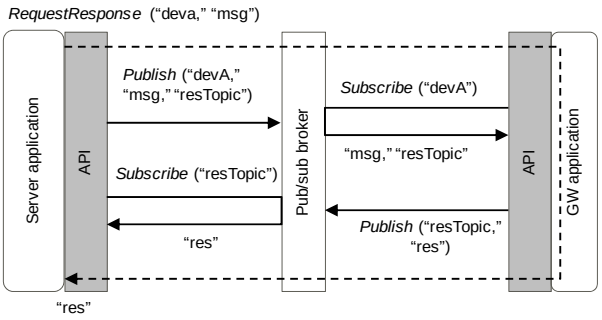


Fig. 3 Implementation of the request-response pattern in the control messaging API

4. Sophistication of Data Utilization

An IoT platform is essential not only for improving the efficiency of IoT system development, but also for implementing a solution for wider use of devices and applications across existing business areas. The challenge is the differences in the data representation between data generated by a device and that expected by an application.

Such differences include those concerning the semantics of a value, in addition to those in the encoding format such as XML and binary. For example, in the case of temperature representation, depending on whether the unit system is Celsius and Fahrenheit, a different value corresponds to the same physical quantity. Some data requires calibration (engineering value conversion) in order to obtain the original physical quantity from a read value, as with the case of the raw data of A/D conversion results. Information needed to interpret such values is often given offline as the specifications of a device/sensor or as the installation requirements. If the interpretation of such values is fixed by a server application, it will be difficult to apply the interpretation to devices of the same type with different specifications or installation requirements.

The NoSQL database of the M2M server uses a data lake method,[1] which accumulates various raw data. It stores the name of the data type, device/sensor ID, and time stamp together with the values in the given format. By referring to the name of the data type and device/sensor ID, the server application can appropriately interpret the values, allowing for integrated processing of various device data. (See Fig. 4.)

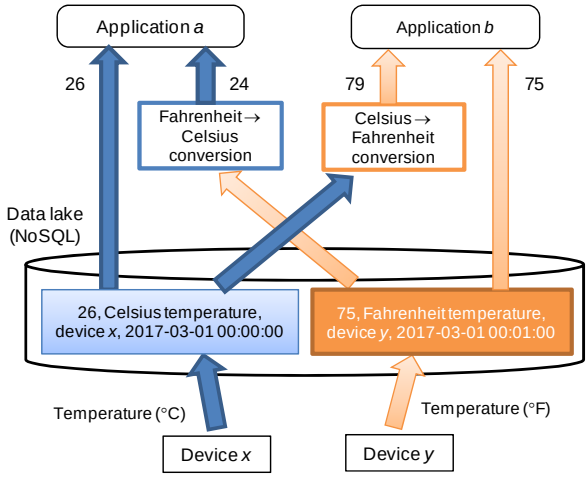


Fig. 4 Semantics conversion of device data

The logic used to interpret device data only needs to be prepared for each device or typical data representation, and is preferably provided as a library for common use from server applications. In the future, we will enhance the middleware functions to perform device data conversion in order to encourage more sophisticated data utilization.

Reference

(1) Dixon J.: Pentaho, Hadoop, and Data Lakes, https://jamesdixon.wordpress.com/2010/10/14/pentaho-hadoop-and-data-lakes/, browsed by the authors on 11/1/2016.

Information Security Technologies in the Age of the Internet of Things (IoT)

Author: *Takeshi Yoneda**

Along with recent advances in the IoT, there are increasing risks of leakage of confidential information and disruption of critical infrastructure caused by network cyberattacks. This article outlines the approach of the Japanese government and the initiatives of Mitsubishi Electric Corporation in terms of cybersecurity, which is vital to safety in the age of the IoT.

1. Approach of the Japanese Government

The *Cybersecurity Strategy*(1) endorsed by the Cabinet on September 4, 2015 emphasizes the necessity to ensure the security of IoT systems in order to boost economic development. The strategy also stresses the need to ensure the security of critical infrastructure for a safe and reassuring society.

The strategy sets forth the following measures to help achieve these goals: (1) Efficiently and speedily sharing cyberattack information between the government and private sector, setting up organizations responsible for cyberattack detection/prevention, and facilitating cooperation among organizations; (2) establishing security standards and guidelines for the development and operation processes of equipment/systems, and promoting compliance with these standards and guidelines; and (3) establishing a public system to objectively evaluate and certify the security of equipment/systems and organizations through third-party authentication. In addition to such security enhancement from the standpoint of organizations, development/operation processes, and public system, the work on core technologies such as encryption and cyberattack detection/prevention technologies is also reinforced to enhance the security of R&D.

2. Initiatives of Mitsubishi Electric Corporation

We have set up an internal computer security incident response team (CSIRT), which serves as a common contact point for cyberattack information in the company, and have also participated in organizations including the Nippon CSIRT Association for the purpose of fostering information sharing and other cooperation systems between the government CSIRTs and private-sector CSIRTs. These are part of our initiatives toward the building of security organizations jointly by the government and private sector. We have also joined the Control System Security Center (CSSC) where we are researching and studying security evaluation/authentication methods and development/operation security guidelines based on IEC 62443, which is a series of standards with the necessary adaptability for control system security.

For technological differentiation, we are working on R&D in anticipation of future IoT needs in the areas of data security, network security, and equipment security.

3. Data Security – Searchable Encryption

3.1 Development background

In the age of the IoT, added value is expected from big data processing through which personal and device information is acquired and stored in the cloud for analysis. However, this information is highly confidential and requires encryption for storage in the cloud. Conventionally, when searching for encrypted information, it must first be decrypted in the cloud, creating a risk of leakage in the process (Fig. 1). We have therefore developed an encryption technology called “searchable encryption” that allows for searches in the cloud without decryption. As a result, confidential information can be kept concealed and utilized at the same time.

3.2 Mechanism of searchable encryption

For the searchable encryption to work, calculation is necessary to determine if the encrypted search request matches the encrypted data registered in the cloud. In 2010, the mechanism for this calculation was completed using the inner-product predicate encryption(2) that we jointly developed with NTT.

In the inner-product predicate encryption, function *f* is capable of calculating an inner product from two vectors without decrypting them. Then, if the vectors are orthogonal to each other (if the inner product is zero), the function returns a zero. If they are not

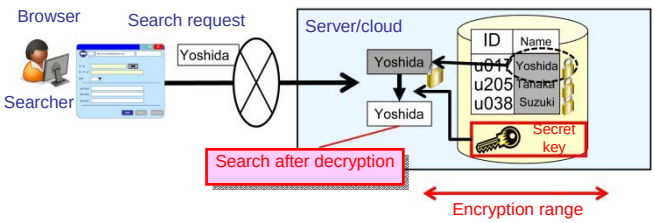


Fig. 1 Conventional search method for encrypted data

*Information Technology R&D Center

orthogonal, the function returns a random number. To be more precise, as shown in Fig. 2, the inner product between a vector encrypted (E) with a public key (pk) and another vector encrypted (E) with a secret key (sk) is calculated; if these vectors before encryption are orthogonal to each other, the product is zero; and if they are not, the result is a random number.

$E_{pk}(\vec{a})$: Public key encryption of $\vec{a}$

$E_{sk}(\vec{b})$: Secret key encryption of $\vec{b}$

$$E_{pk}(\vec{a})\cdot E_{sk}(\vec{b}) = f(\vec{a}\cdot\vec{b}) = \begin{cases} 0 & When\ \vec{a}\cdot\vec{b} = 0 \\ Random\ number & When\ \vec{a}\cdot\vec{b} \neq 0 \end{cases}$$

Fig. 2 Determination of vector orthogonality using inner-product predicate encryption

We have developed a method for encoding a search item and search keyword to vectors, in order to apply the vector orthogonality determination for inner-product predicate encryption to the searchable encryption. More precisely, a search item and search keyword are encoded as a pair of vectors that will be orthogonal to each other (the inner product becomes zero) when the search item matches the search keyword. Figure 3 shows a vector encoding example in which the search item and search keyword use the data "Yoshida."

Searched item $\vec{a} = (Yoshida, 1)$

Search keyword $\vec{b} = (-1, Yoshida)$ $(\vec{a}\cdot\vec{b} = Yoshida * -1 + 1 * Yoshida = 0)$

Fig. 3 Vector encoding of a search item and search keyword

With this vector encoding, the server determines the orthogonality of a pair of vectors without decrypting the encrypted search item and encrypted search keyword. A result of zero indicates that the search item and search keyword match each other (Fig. 4).

The searchable encryption described above allows the cloud to determine if the encrypted search request matches the encrypted search item registered in the server without decrypting them, eliminating the risk of information leakage. We also upgraded this technology to searchable encryption with partial matching,[3] which makes it possible to search for a keyword in a document without decryption. In February 2016, we created the world's first platform software for this technology.[4]

3.3 Future initiatives

Our technology for searchable encryption with partial matching has expanded the scope of application for searchable encryption, from structured data such as equipment operation logs and network communication logs to unstructured data such as office documents and medical documents. Going forward, we will work on optimizing this technology for each application field.

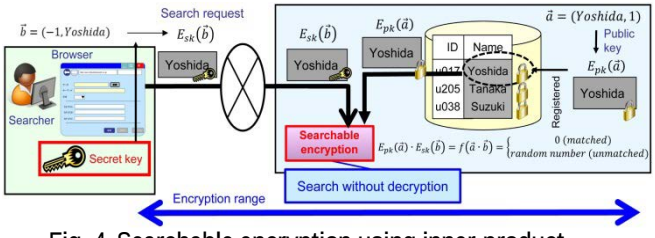


Fig. 4 Searchable encryption using inner-product predicate encryption

4. Network Security – Attack Detection Technology

4.1 Development background

Large-scale information leakages that recently occurred at corporations and national/local governments were caused by cyberattacks using computer viruses sent via email attachments or by planting unauthorized pages on websites. Since 300 million new types of computer viruses are created each year, it has become difficult to find new ones using virus detection methods that check a virus against those already known.[5]

In response, we have developed a method for detecting attacks based on the attacker's method of using viruses instead of focusing on individual viruses. With our analysis results showing that there are about 50 tactics to use computer viruses, the focus on such attacker's tactics led to an efficient attack detection method.[6]

4.2 Mechanism of attack detection based on the tactics

Virus activities in a cyberattack involve the following steps: (1) Infection of the target terminal; (2) Receiving the hacker's instructions; (3) Scanning of the infected terminal; and (4) Unauthorized acquisition of access rights to a wider attack range. For instance, in the step for scanning the infected terminal, what to steal and how to steal it are determined using a number of attack tactics such as searching for documents stored in the infected terminal, checking for communication routes, and checking for security measures taken.

We classified tactics common to attacks using computer viruses into about 50 different patterns, and developed analysis rules to detect the occurrence of each pattern from logs. The number of attack tactics increases by about a dozen per year. Additional analysis rules can be created when a new attack tactic is uncovered.

Upon the detection of activities of an authorized user that resemble those seen in an attacker tactic, it is necessary to determine that such activities do not constitute an attack. For this reason, we have developed a correlation analysis method in which a cyberattack scenario made up of a series of multiple attack tactics is defined to check whether the attack tactics occur along the scenarios. This method allows an authorized user's activities that resemble an attacker tactic to be distinguished from a cyberattack (Fig. 5).

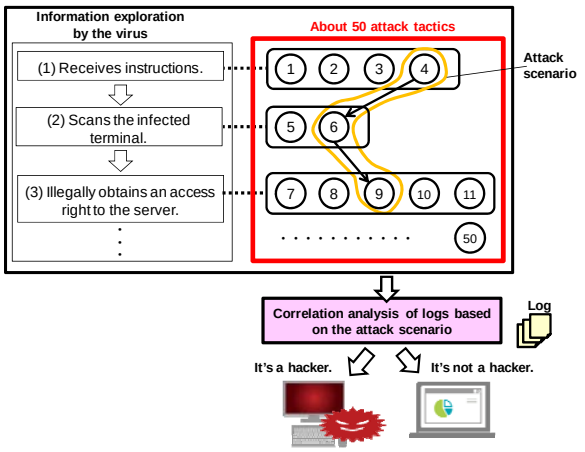


Fig. 5 Cyberattack detection based on attack scenario

4.3 Future initiatives

The technology described above was developed targeting attacks on information systems. For IoT systems as well, attackers are likely to use tactics common to similar scenarios in a limited manner. Therefore, we will research and analyze tactics used in attacks on equipment in order to extend the application of this technology to attacks on IoT systems.

5. Equipment Security – LSI Fingerprinting

5.1 Development background

The age of the IoT has gained momentum. All kinds of devices, not only information communication devices such as personal computers and smartphones, are being connected to each other via the Internet. While this provides greater convenience, it is necessary to take measures against security risks such as malicious program update and impersonation. Traditionally, risks have been in the cyber society such as unauthorized bank transfers. However, in the age of the IoT in which all kinds of systems and devices are connected, risks can be in the real space such as endangering human life.

Generally, the operation of an electronic device is controlled by programs installed on a large-scale integrated circuit (LSI). If these programs are altered, all devices connected to the network will be at risk. Our efforts to solve these problems resulted in the development of LSI fingerprinting.[7][8]

5.2 Mechanism of LSI fingerprinting

An electronic device is equipped with operation control programs and LSIs including a CPU responsible for executing these programs. Each LSI has its own voltage increase pattern called a transient glitch, even when the LSIs use the same type of circuit or have the same output. Using such properties, a unique ID for each LSI that is equivalent to an LSI fingerprint is created.

There are two requirements for keeping confidential information safe in an LSI. One is to ensure that information will not be leaked even if the LSI is disassembled and analyzed. Conventionally, ID information is encrypted before being stored in nonvolatile memory (a storage cell that can retain data without power supply). This makes it possible to view and steal the information in the memory by disassembling and analyzing. The LSI fingerprinting technology allows the unique ID to be visible only when the LSI is in operation, and no confidential information can be seen even if it is disassembled. The other requirement is to ensure that confidential information cannot be reproduced even if the circuit is copied. The difference in glitches is the result of unexpected individual differences. This means that a copied circuit cannot have the same ID of the original circuit. Thus, this technology fulfils the two safety requirements, as proven by the fact that the ID is invisible and not reproducible (Fig. 6).

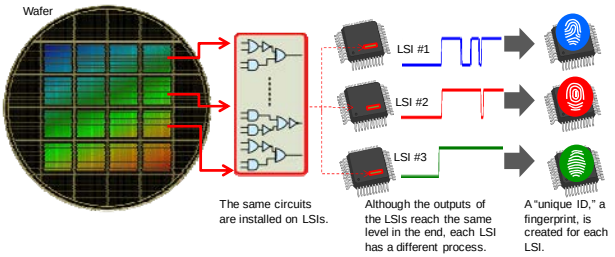


Fig. 6 Mechanism of LSI fingerprinting

5.3 Future initiatives

The creation of such a high-security unique ID for each electronic device makes it possible to protect the secret keys and authentication keys of the device from attacks. This allows strict protection of programs and prevention of equipment spoofing, contributing to the safety and reliability of devices in the age of the IoT.

References

(1) http://www.nisc.go.jp/active/kihon/pdf/cs-senryaku-c.pdf
(2) Okamoto, T., et al.: Fully Secure Functional Encryption with General Relations from the Decisional Linear Assumption, CRYPTO (2010).
(3) Kawai, Y., et al.: Efficient Partial Keyword Search on Encrypted Data, CANS (2015).
(4) http://www.mitsubishielectric.co.jp/ news/2016/0204.html
(5) Symantec Corporation, Internet Security Threat Report 2015
(6) http://www.mitsubishielectric.co.jp/news/2016/0217-f_zoom_01.html
(7) Suzuki D., et al.: The Glitch PUF: A New Delay-PUF Architecture Exploiting Glitch Shapes, CHES (2010).
(8) http://www.mitsubishielectric.co.jp/news/2015/0205.pdf

EMS Solutions in Overseas Markets

Authors: *Daisuke Takita** and *Takanori Kyoya**

In developing countries in Asia, companies need to reduce energy consumption to resolve a number of operational problems. Mitsubishi Electric Corporation has proposed an energy management system (EMS) that supports energy saving through visualizing energy consumption. This unique EMS provides a solution that can be readily customized by utilizing wireless and application technologies to help customers locate problems through experimental trials. With this system, we are pursuing new business opportunities and stronger competitiveness in our field.

1. Introduction

In rapidly growing China and ASEAN countries, the need to reduce energy consumption is increasing in view of electricity shortages, as well as to reduce costs, comply with environmental restrictions, and deal with other operational issues. In these emerging nations, we have proposed our EMS tailored to the legal restrictions, needs, and use conditions unique to each country, as a solution to support energy saving mainly through a feature for visualizing energy consumption; we also conduct experimental trials for customers to check the energy saving effects and obtain data. This EMS solution is characterized by the combination of simple installation, expandability through autonomous routing technology, and visualization applications. This allows the system to be customized quickly at low cost; it is easy to commence an experimental trial or to change the configuration based on the test results.

2. EMS for Overseas Markets

To reduce energy consumption, the most important part is understanding and analyzing the current situation.[1] We have developed a system that is easy to introduce and that allows the current status of energy use to be ascertained and analyzed. For this system, we have conducted experimental trials under various conditions, with the main purpose of acquiring data and knowledge to working with customers and eventually increasing the collaboration areas in the future.

3. Components

3.1 Wireless network technologies

Table 1 shows the wireless network communication protocol stack of this system. It consists of functions that allow low power consumption and communication range expansion, suitable for machine-to-machine (M2M) communication.[2]

Table 1 Network protocol stack

Layer		Protocol
Physical layer		IEEE 802.15.4g[4]
	Physical medium	In accordance with laws and regulations of the country
	Communication speed	100 kbps
Data link layer		IEEE 802.15.4[3]
	Media access control	CSMA/CA
Network layer		Original protocol
	Routing control	Original RPL[6]-based protocol
Application layer		Original protocol

IEEE 802.15.4[3] is a wireless communication standard that defines a protocol such that the power consumption of a device can be easily reduced. In addition, the physical layer uses the IEEE 802.15.4g[4] standard, which defines the specifications for the use of sub-GHz bands supplementing the provisions of IEEE 802.15.4. Sub-GHz bands have excellent radio reachability and diffraction characteristics. Compared with 2.4 GHz bands and others, sub-GHz bands characteristically have lower radio-frequency interference. For the EMS system, we used the wireless module[5] (Fig. 1) developed for use in Japan that was modified to comply with the laws and regulations of individual countries. Equipped with a routing protocol based on RPL,[6] the system allows for multihop wireless communication in which multiple redundant routes can be used. This makes it possible to reduce management costs by increasing the data acquisition range using the multihop communication, preventing network failure using the redundant route setting function, etc. Figure 2 shows a network constructed based on RPL.

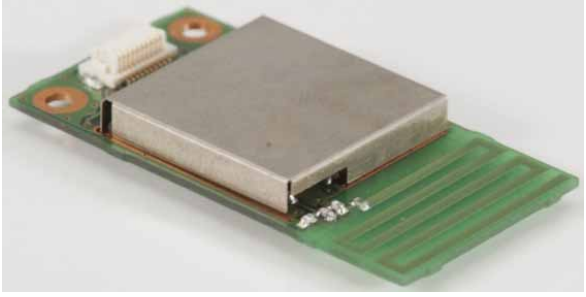


Fig. 1 Wireless module

*Information Technology R&D Center

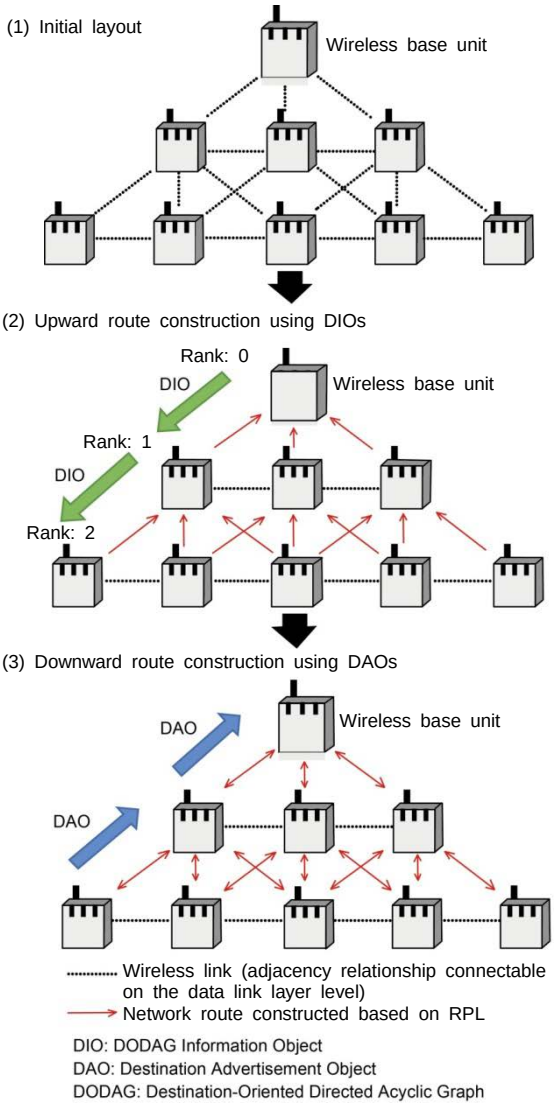


Fig. 2 RPL example

3.2 Applications

The basic function required of an application used in the EMS solution is accurate "visualization" of data on the status of power consumption and other management items. By clarifying activities that hinder energy consumption reduction, it is easier to devise a specific energy saving measure. For example, at a manufacturing plant, the potential reduction in power consumption during nonproduction hours and the power consumption of heat-generating manufacturing equipment that increases the air conditioning load can be ascertained for control. Effective ways to reduce power consumption include measures such as leveling the power consumption, shifting the operation hours, and improving the energy consumption efficiency by intensive operation. However, it is necessary to take into account factors not directly involved in energy saving, such as productivity, impact on cost/quality, and coordination with personnel plans.

3.3 Support tools

The design, installation and maintenance of a wireless system involves operations to determine the location for installing wireless units in consideration of the radio wave reachable distance and noise environment, to check and monitor the communication state after installation, detect abnormalities, recover from failure, etc. To allow users with no special knowledge on wireless communication to carry out these operations, we have developed various support tools with intuitive user interfaces. As examples, the installation support tool useful for determining where to install a wireless unit and the wireless network monitoring tool for visualizing the connection state are shown in Fig. 3 and Fig. 4, respectively.

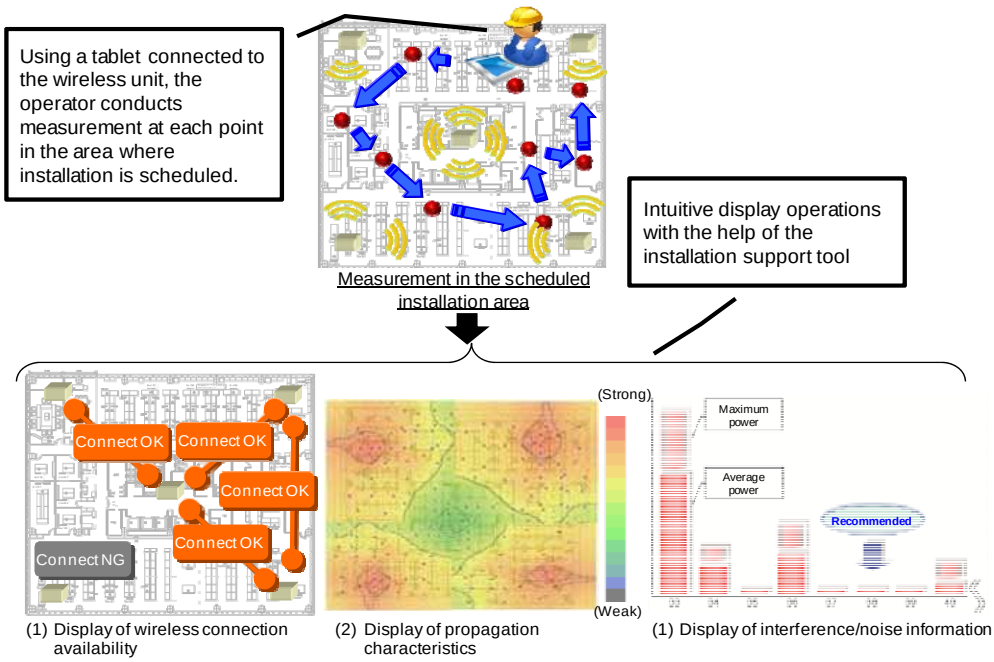


Fig. 3 Installation support tools

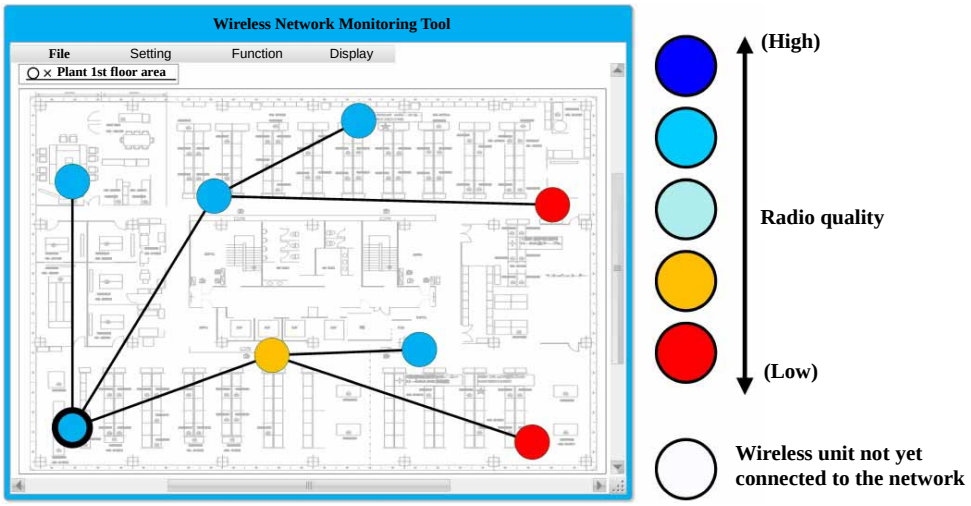


Fig. 4 Wireless network monitoring tool

4. Experimental Trials Overseas

Using the technologies described above, we have been conducting experimental trials in each country where the EMS solution is introduced. Table 2 lists the trials that are currently underway. The results of past experimental trials have revealed that the advantages of this system which offers speedy identification of requirements and test operation are well suited to the needs of individual countries.

Table 2 Experimental trials in progress

Experimental trial	Purpose
Plant (China)	Investigation of wireless propagation (inside the plant) Reduction of operating cost
Building (China)	Investigation of wireless propagation (inside the building) Demonstration
Commercial facilities (China)	Improvement of air conditioning efficiency
Building (Singapore)	Investigation of actual power consumption in a tropical region

5. Conclusion

This article described an EMS solution that can be customized quickly at low cost by applying wireless technology, using a combination of multiple visualization tools, and experimental trials conducted overseas. Going forward, utilizing data and knowledge gained from the experimental trials, we will continue to clarify the key problems faced by various customers in different regions and propose more effective solutions, with the aim of creating new business opportunities and strengthening our competitiveness in this field.

References

(1) Mitsubishi Electric Energy-Saving Support Website: http://www.mitsubishielectric.co.jp/shoene/
(2) Fujie, R., et al.: Wireless and network technology to support M2M, IEICE General Conference BT-3-1 (2013).
(3) IEEE Std 802.15.4
(4) IEEE Std 802.15.4g
(5) Technologies for Sensor Network with Specified Low Power Radio, Mitsubishi Denki Giho, 89, No. 1, 7 (2015).
(6) T. Winter, et al. RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks, IETF RFC6550.

MITSUBISHI ELECTRIC CORPORATION