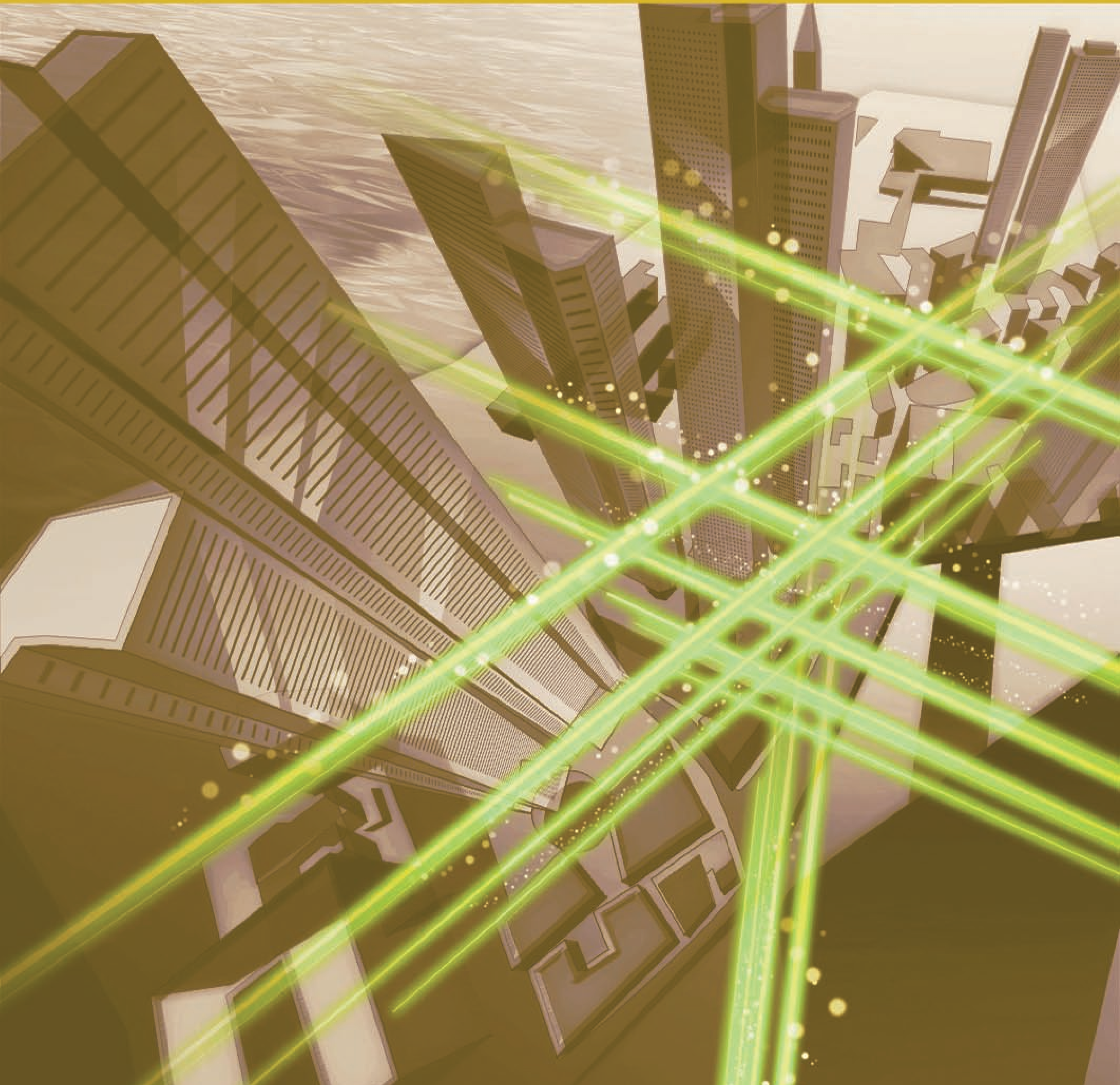
7
2014

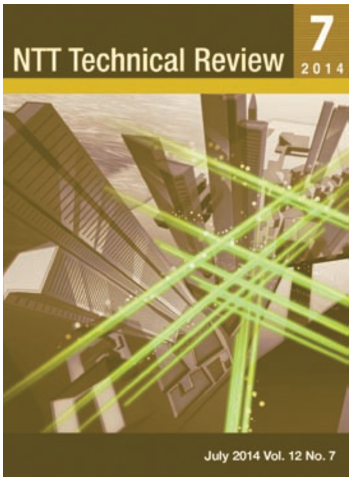
NTT Technical Review



July 2014 Vol. 12 No. 7

NTT Technical Review

July 2014 Vol. 12 No. 7



Feature Articles: Security Platform Technologies that Support Cloud Business

Regular Articles

Global Standardization Activities

New NTT Colleagues

External Awards/Papers Published in Technical Journals and Conference Proceedings

Security R&D Activities for Cloud Services

Toshiyuki Miyazawa, Yosuke Aragane, Yoshiaki Nakajima, and Hidetsugu Kobayashi

Abstract

The use of cloud services for handling economically and socially important information is increasing. In line with this trend, these services have become attractive targets for cyber attackers and have been exposed to more sophisticated cyber threats. Various efforts are underway at NTT to prevent these evolving cyber threats. In this article, we describe the activities of NTT Secure Platform Laboratories to provide safe and secure cloud services to our customers.

Keywords: security, cloud, R&D plan

1. Introduction

Cloud services, which provide storage and processing functions via the Internet, are becoming increasingly popular because of their economic advantages in reducing provisioning and operational costs as well as the convenience of being able to access them from various environments. As the use of smartphones to access the Internet has become more widespread, cloud services have accordingly provided more sophisticated and useful functions and have become an important infrastructure supporting our economy and society.

The incorporation of cloud services into the infrastructure means that cyber attackers have an appealing new target on the Internet. Additionally, cyber attacks are also a national-level threat that is expected to continue evolving at an accelerated pace. Therefore, implementing security countermeasures and security operations based on advanced research is important in order to protect customers' valuable information against evolving cyber threats and to provide safe and secure cloud services.

2. R&D at the NTT Secure Platform Laboratories

NTT Secure Platform Laboratories engages in research and development (R&D) based on leading-edge research on cryptography and malware analysis to contribute safer and more secure services provided by the NTT Group. Our basic R&D plan is to protect internal systems, the communication infrastructure, and enterprise solutions (**Fig. 1**). We are moving forward with R&D guided by a three-part vision: (1) coping with the most highly evolved attacks, (2) realizing safe and worry-free network use, and (3) creating new business through promoting secure use of information. We have targeted four R&D areas (**Fig. 2**) in order to achieve this R&D vision.

2.1 Information security platform

In the area consisting of the information security platform, we conduct leading-edge research on cryptography and develop security technologies that can protect systems and information from cyber attacks and internal fraud and also promote secure use of information. Typical technologies in this area include intelligent cryptosystems and secure computation. Secure computation technology and its evolved form, fully homomorphic encryption, are particularly suited for statistical processing, database processing, and similar types of computation while maintaining the secrecy of data stored in the cloud. The implementation of such techniques can promote not only the use of cloud services but also the creation of new business

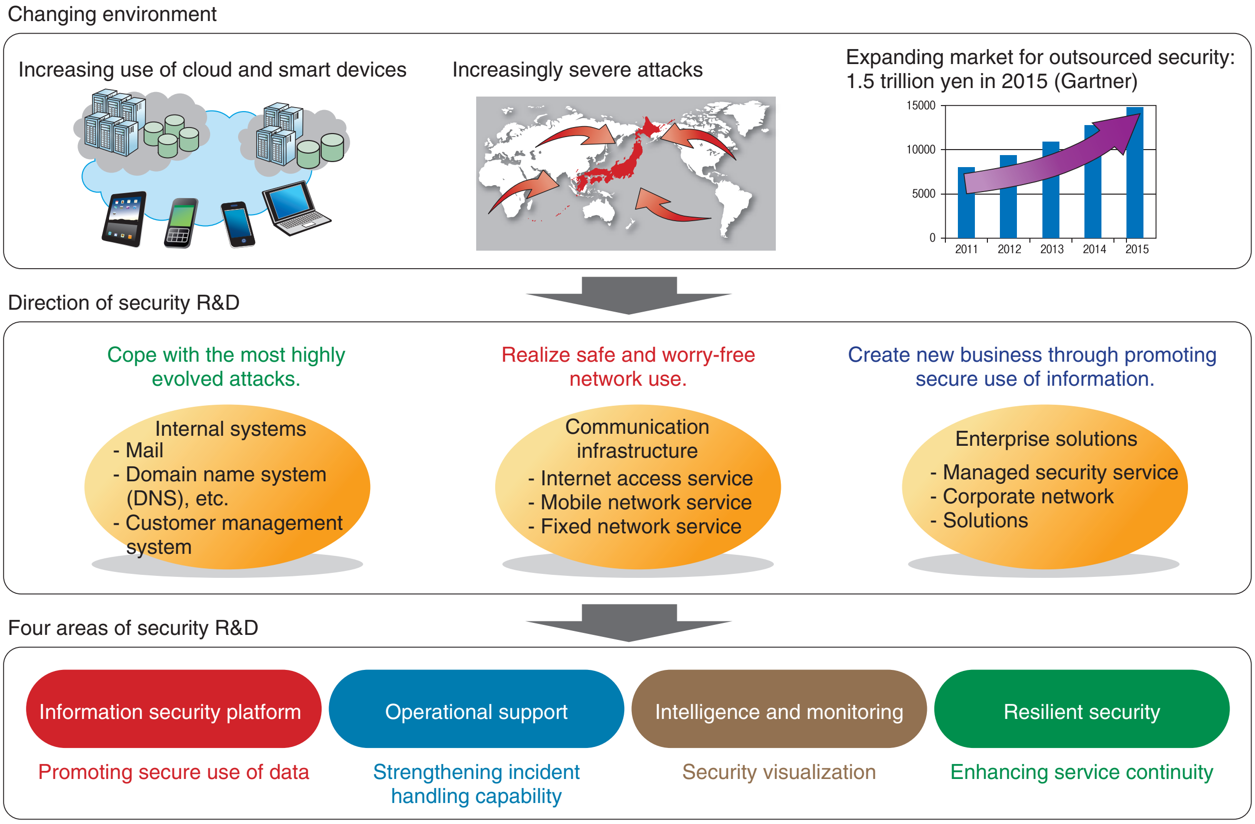

Changing environment
Increasing use of cloud and smart devices
Increasingly severe attacks
Expanding market for outsourced security: 1.5 trillion yen in 2015 (Gartner)
15000
10000
5000
0
2011
2012
2013
2014
2015
Direction of security R&D
Cope with the most highly evolved attacks.
Internal systems
- Mail
- Domain name system (DNS), etc.
- Customer management system
Realize safe and worry-free network use.
Communication infrastructure
- Internet access service
- Mobile network service
- Fixed network service
Create new business through promoting secure use of information.
Enterprise solutions
- Managed security service
- Corporate network
- Solutions
Four areas of security R&D
Information security platform
Promoting secure use of data
Operational support
Strengthening incident handling capability
Intelligence and monitoring
Security visualization
Resilient security
Enhancing service continuity

Fig. 1. Basic plan for security R&D.

that requires the use of sensitive data such as management data and personal information. The activities in this area are described in detail in the articles “R&D on Secure Computation Technology for Privacy Protection” [1] and “Fully Homomorphic Encryption over the Integers: From Theory to Practice” [2] in these Feature Articles. For information on other technologies we are working on, please see Fuji et al. [3].

2.2 Operational support

Our R&D in the area of operational support involves supporting security operations of NTT Group companies and improving the technology for such support. Preventing all cyber attacks is difficult because they are constantly evolving. NTT-CERT (NTT Computer Security Incident Response and Readiness Coordination Team), the CSIRT[*1] organization of the NTT Group, supports security operations in both pre-incident and post-incident measures in order to respond rapidly to cyber attacks on various systems such as the cloud service system, and to minimize the damage of those attacks. For more information on the work of NTT-CERT, refer to Tanemo et al. [4].

2.3 Intelligence and monitoring

The area consisting of intelligence and monitoring involves security visualization technologies that enable early detection of cyber attacks and provide an accurate understanding of the system status. In order to achieve early detection of cyber attacks, we research and develop technology for security log correlation analysis and malware analysis. We are also gathering information on malicious sites that infect and distribute malware and are providing such information as security intelligence to NTT Group companies. For more information on this work, please see Hariu et al. [5]. Security threats can also arise from internal fraud and operation errors, so it is important

[*1] CSIRT (Computer Security Incident Response Team): An organization responsible for incident response in the broad range of preventing cyber threats, detecting cyber attacks, and handling security incidents.

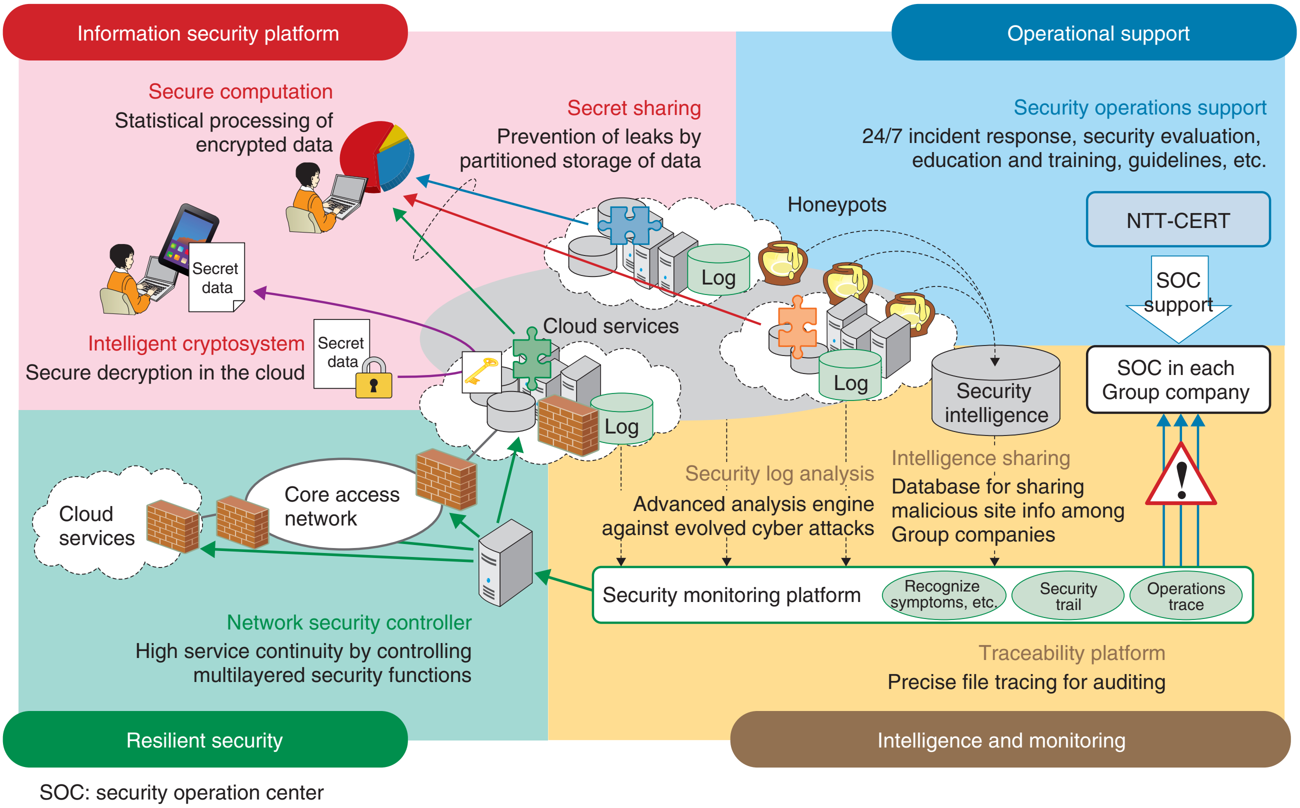

Information security platform
Operational support
Secure computation
Statistical processing of encrypted data
Secret sharing
Prevention of leaks by partitioned storage of data
Security operations support
24/7 incident response, security evaluation, education and training, guidelines, etc.
Honeypots
NTT-CERT
SOC support
Secret data
Log
Cloud services
Intelligent cryptosystem
Secure decryption in the cloud
Secret data
Log
Security intelligence
SOC in each Group company
Log
Intelligence sharing
Database for sharing malicious site info among Group companies
Security log analysis
Advanced analysis engine against evolved cyber attacks
Cloud services
Core access network
Security monitoring platform
Recognize symptoms, etc.
Security trail
Operations trace
Network security controller
High service continuity by controlling multilayered security functions
Traceability platform
Precise file tracing for auditing
Resilient security
Intelligence and monitoring
SOC: security operation center

Fig. 2 Security R&D overview.

to accurately comprehend the information flow within the system in order to maintain security. Visualizing the information flow is especially important with cloud services; such visualization makes it possible to strengthen the security of cloud services and to increase the sense of trust that customers have in cloud providers. In these Feature Articles, we introduce R&D on "The TRX Traceability Platform," which enables visualization of the information flow by collecting and linking various event logs from cloud services and other services [6].

2.4 Resilient security

Resilient security is a new area of R&D. A resilient function can avert a complete service shutdown and restore the service to a normal state, even when the service is affected by cyber attacks or natural disasters. To achieve cloud services with this resilient function, we are working on autonomous recovery technology that enables cooperation and control of virtual network technology and virtual appliance technology. The concept and component technologies of resilient security are described in the article "Resilient Security Technology for Rapid Recovery from Cyber Attacks" [7] in these Feature Articles.

3. Future study

Security is relevant to a very broad range of areas, and some of them are beyond the scope of our laboratories. In the four areas of our R&D described above, cooperation with global organizations is important. In particular, we cooperate closely with NTT I^3 (NTT Innovation Institute Inc.), an R&D facility in North America, by sharing the latest needs in the North American market and advanced technological knowledge in the cloud and security fields. We will proceed with security R&D to achieve our vision through cooperation with internal and external organizations.

References

[1] K. Chida, D. Ikarashi, T. Miyata, H. Takiguchi, and N. Kiribuchi, "R&D on Secure Computation Technology for Privacy Protection," NTT Technical Review, Vol. 12, No. 7, 2014.

https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201407fa4.html

[2] M. Tibouchi, "Fully Homomorphic Encryption over the Integers: From Theory to Practice," NTT Technical Review, Vol. 12, No. 7, 2014.
https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201407fa5.html

[3] H. Fuji, A. Fujioka, T. Kobayashi, K. Chida, F. Hoshino, T. Miyazawa, and K. Suzuki, "Cryptographic Techniques that Combine Data Protection and Ease of Utilization in the Cloud Computing Era," NTT Technical Review, Vol. 10, No. 10, 2012.
https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201210fa3.html

[4] F. Tanemo, I. Hayashi, M. Tanikawa, and T. Abe, "Tighter Security Operations to Help Provide Brands that are Safer and More Secure," NTT Technical Review, Vol. 10, No. 10, 2012.
https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201210fa4.html

[5] T. Hariu, M. Akiyama, K. Aoki, T. Yagi, M. Iwamura, and H. Kurakami, "Detection, Analysis, and Countermeasure Technologies for Cyber Attacks from Evolving Malware," NTT Technical Review, Vol. 10, No. 10, 2012.
https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201210fa2.html

[6] T. Motoda, T. Nagayoshi, J. Akiba, and K. Takeuchi, "The TRX Traceability Platform," NTT Technical Review, Vol. 12, No. 7, 2014.
https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201407fa2.html

[7] T. Koyama, K. Hato, H. Kitazume, and M. Nagafuchi, "Resilient Security Technology for Rapid Recovery from Cyber Attacks," NTT Technical Review, Vol. 12, No. 7, 2014.
https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201407fa3.html

Toshiyuki Miyazawa

Senior Research Engineer, Information Security Project, NTT Secure Platform Laboratories.

He received the B.E. and M.S. in mathematics from Waseda University, Tokyo, in 2000 and 2003, respectively. Since joining NTT Information Sharing Platform Laboratory in 2003, he has been engaged in R&D of information security, especially of public key cryptography and security protocols. From 2008 to 2011, he was with the IT Innovation Department at NTT EAST. He is a member of the Japan Society for Industrial and Applied Mathematics. He received the SCIS Paper Award from the Institute of Electronics, Information and Communication Engineers (IEICE) in 2007.

Yosuke Aragane

Senior Research Engineer, Planning Section, NTT Secure Platform Laboratories.

He received the M.S. and Ph.D. from Tokyo Institute of Technology, Tokyo, in 1997 and 2005 respectively. In 1997, he joined NTT Multimedia Network Laboratories, where he researched human factors and communication management methods in intelligent transportation systems (ITS). Since then, he has been involved in R&D focusing on ITS and security. From 2008 to 2011, he was with the IT Innovation Department at NTT EAST. He is a member of the Institute of Electrical and Electronics Engineers, the Association for Computing Machinery, IEICE, and the Information Processing Society of Japan (IPSJ). He was awarded the Best Paper Award from IPSJ in 2006 and has served as a committee member of major international conferences.

Yoshiaki Nakajima

Senior Research Engineer, Supervisor, Planning Section, NTT Secure Platform Laboratories.

He received the B.S. in information science and the M.S. in mathematical and computing science from Tokyo Institute of Technology, Tokyo, in 1995 and 1997, respectively. In 1997, he joined NTT Information and Communication Systems Laboratories, where he worked on R&D of information security. From 2009 to 2013, he was with the Security Strategy Section of the Technology Planning Department. He has been involved in R&D of information and communication platforms, security platforms, and other areas.

Hidetsugu Kobayashi

General Manager, Human Capital Management Group, NTT Research and Development Planning Department.

He received the B.E. from the University of Tokyo in 1987 and the M.S. in information networking from Carnegie Mellon University, USA, in 1991. Since joining NTT in April 1987, he has contributed to the development of a range of network security related products such as firewalls for IP-VPNs and authentication servers for the NGN. His research interests include network security and information networks. As of July 1, 2014, he moved from NTT Secure Platform Laboratories to NTT Research and Development Planning Department.

The TRX Traceability Platform

Toshihiro Motoda, Takeshi Nagayoshi, Junya Akiba, and Kaku Takeuchi

Abstract

TRX, which was developed by the NTT Secure Platform Laboratories, is a traceability platform for visualizing various events that occur in a system. A visualization function in the system makes it possible to track operations such as *copy* and *move* that are made to files and virtual machine images. This function provides easy and unprecedented understanding of the flow of information within an enterprise. It can be used for file life-cycle management in offices and license management of virtual server operating systems for cloud providers.

Keywords: visualization, log, traceability

1. Introduction

The concept of traceability as applied to farm products such as beef and other foods in the Japanese market is well known. It makes it possible to know when, where, and by whom cattle or another product was raised, and how the products were distributed. This gives consumers more information on the products available to them and allows them greater choice in what products to buy.

But can this concept be applied to information systems? When you create digital materials and send them to another person, how can you find out what subsequently happens to them, for example, how, where, and by whom they are later used and modified? Unease concerning information systems may arise when we are not sure how information is handled within the system because we have no way to visualize the situation [1]. Information traceability makes it possible to track and provide a visual view of how documents and other information are moved around and altered within an information system.

2. TRX traceability platform

The NTT Secure Platform Laboratories has been developing the TRX traceability platform as a step toward achieving information traceability. The role of TRX is illustrated in **Fig. 1**. The TRX traceability platform makes events visible when they occur in a system. These events include file operations, the creation of virtual servers in the cloud or another system, or web accesses that occur during the provision of services. This visualization is a matter of making connections in the relationships between events, and displaying in a visual or easily processed format information that cannot be understood simply by looking at individual events.

The functional elements of the TRX system and the flow of log information are illustrated in **Fig. 2**. Here, various events can be visualized. For example, a function for precisely visualizing file operations performed manually and a function for detecting the copying of virtual machine (VM) images[*1] using active trace technology are provided as basic functions. These functions are features of the TRX traceability platform and are described in more detail in the following subsections.

2.1 File operation visualization (file tracing)

(1) Highly precise logging of file operation events

The flow of log generation for file operation events in TRX is shown in **Fig. 3**. The file trace log-generating function on the user terminal monitors the file I/O

[*1] VM image: An electronic file that stores individual virtual server instances when virtualization technology is used to construct servers etc. Because it is an electronic file, it is easy to create, delete, or copy a virtual server.

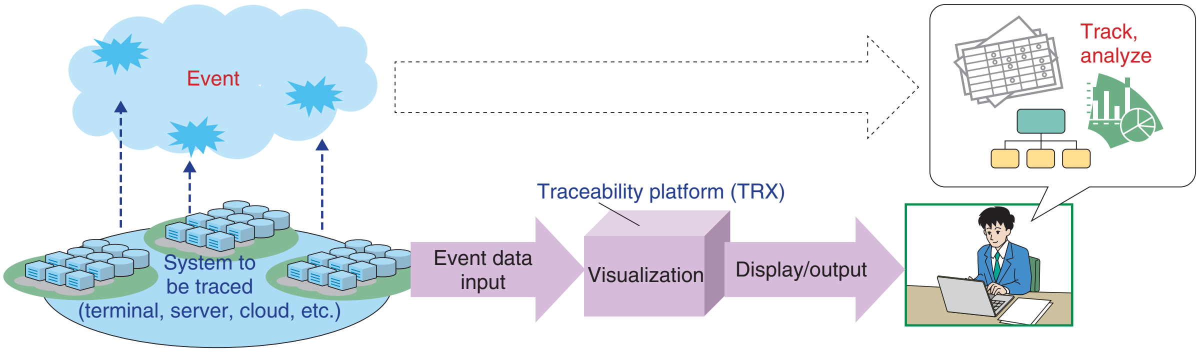

Event
Track, analyze
Traceability platform (TRX)
System to be traced (terminal, server, cloud, etc.)
Event data input
Visualization
Display/output

Fig. 1. TRX traceability platform.

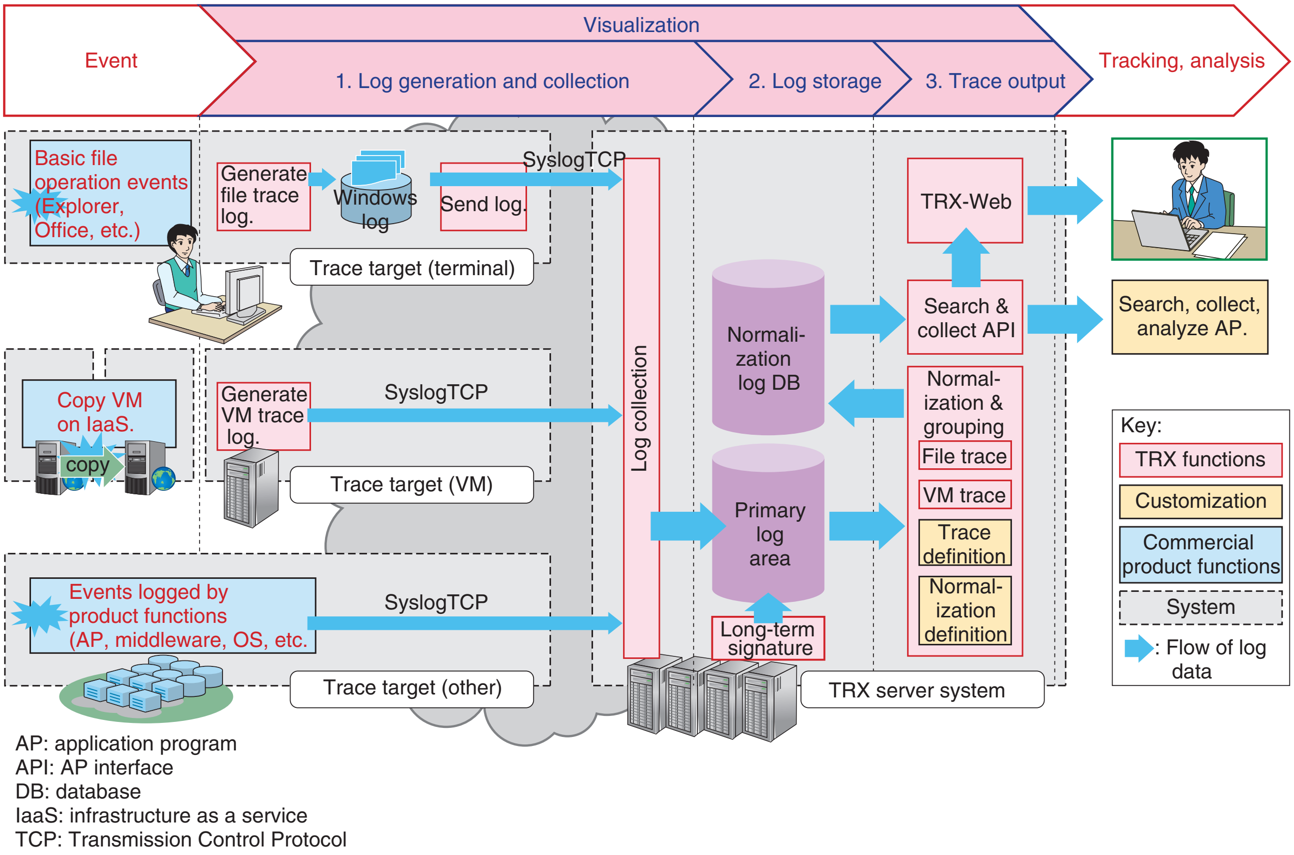
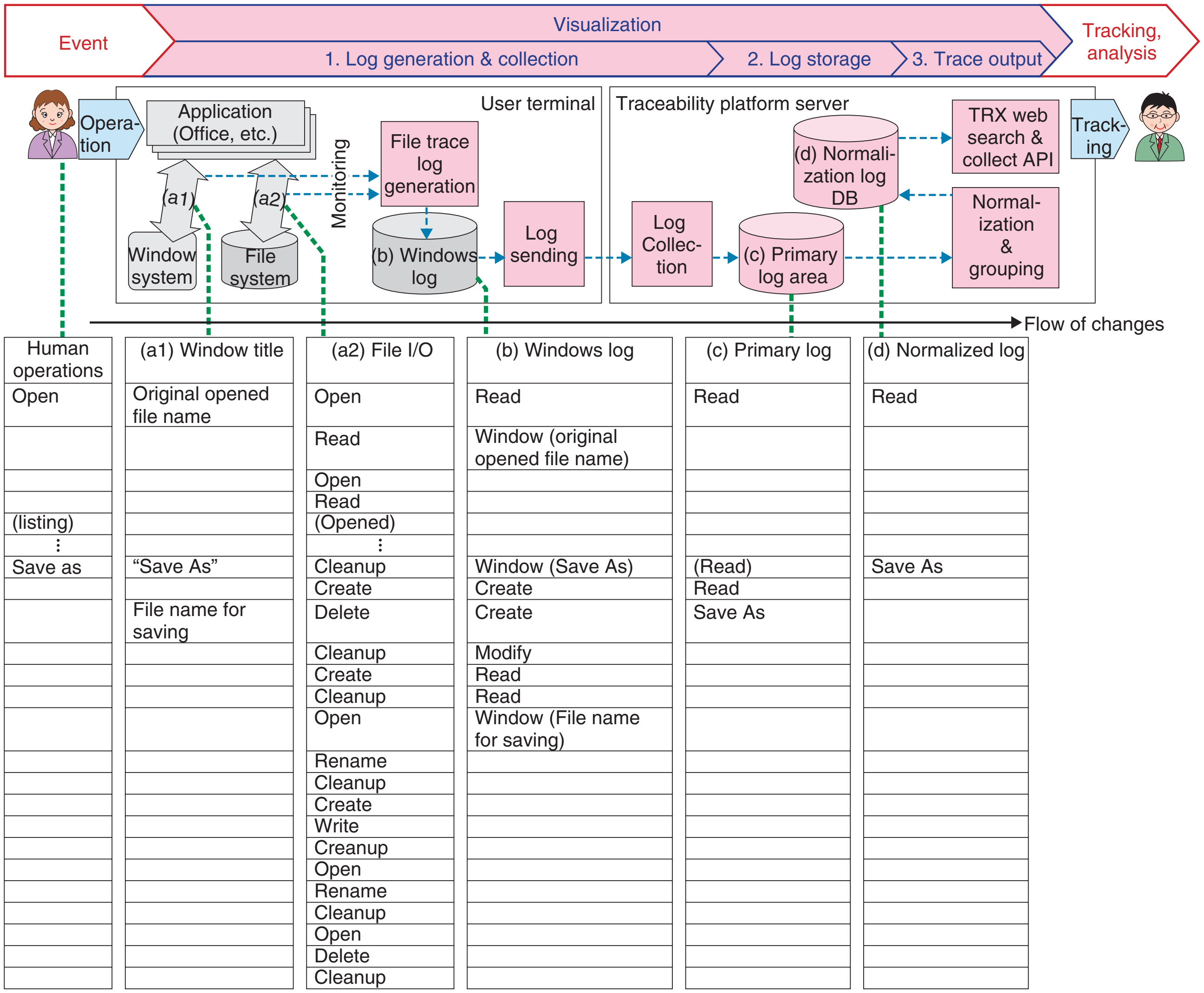


Fig. 2. Traceability platform functions and log data flow.

(input/output) and window events of an application running on a Windows terminal, including the virtual desktop (Fig. 3(a1) and (a2)). Although the monitored events are very primitive such as *open file*, *read data*, *write data*, and *delete* for file I/O, the various TRX functions abstract the events in multiple stages to produce a log that corresponds more or less one-to-one with the original events, which are operations performed by human operators.

The primitive events occur in huge quantities, for example, 10,000 file I/O events per second. A high level of expertise is necessary in order to accurately



Human operations	(a1) Window title	(a2) File I/O	(b) Windows log	(c) Primary log	(d) Normalized log
Open	Original opened file name	Open	Read	Read	Read
		Read	Window (original opened file name)		
		Open			
		Read			
(listing)		(Opened)			
⋮		⋮			
Save as	“Save As”	Cleanup	Window (Save As)	(Read)	Save As
		Create	Create	Read	
	File name for saving	Delete	Create	Save As	
		Cleanup	Modify		
		Create	Read		
		Cleanup	Read		
		Open	Window (File name for saving)		
		Rename			
		Cleanup			
		Create			
		Write			
		Creanup			
		Open			
		Rename			
		Cleanup			
		Open			
		Delete			
		Cleanup			

Fig. 3. Accurate logging of file operation events.

convert them to a log with the number of operations per second that corresponds to human operations. For the TRX platform, we devised a customized commercially available product[*2] so that logs with especially high accuracy can be generated for popular applications such as Microsoft Office and Adobe Acrobat.

(2) Grouping for file operation event visualization

The flow of grouping for event visualization is illustrated in **Fig. 4**. The logs for files derived by copying information from the same file are normalized and assigned to a single group so that they can be handled together. The normalized log for file operations contains the information listed below.

- File name before operation: The name of the file before the operation was performed[*3]
- Date and time: The time and date the operation was performed
- User ID (identification): A code to identify the user who performed the operation
- Terminal address: The address of the terminal on which the operation was performed
- Operation type: Types of operations include create, copy, rename, move, delete, etc.
- File name after operation: The name of the file after the operation was performed[*4]

[*2] A customized version of the Log Audit Tracker product for logging file operations; produced by the dit Company Limited.

[*3] For ‘create’ operations, no “file name before the operation” is included.

[*4] For ‘delete’ operations, no “file name after operation” is included.

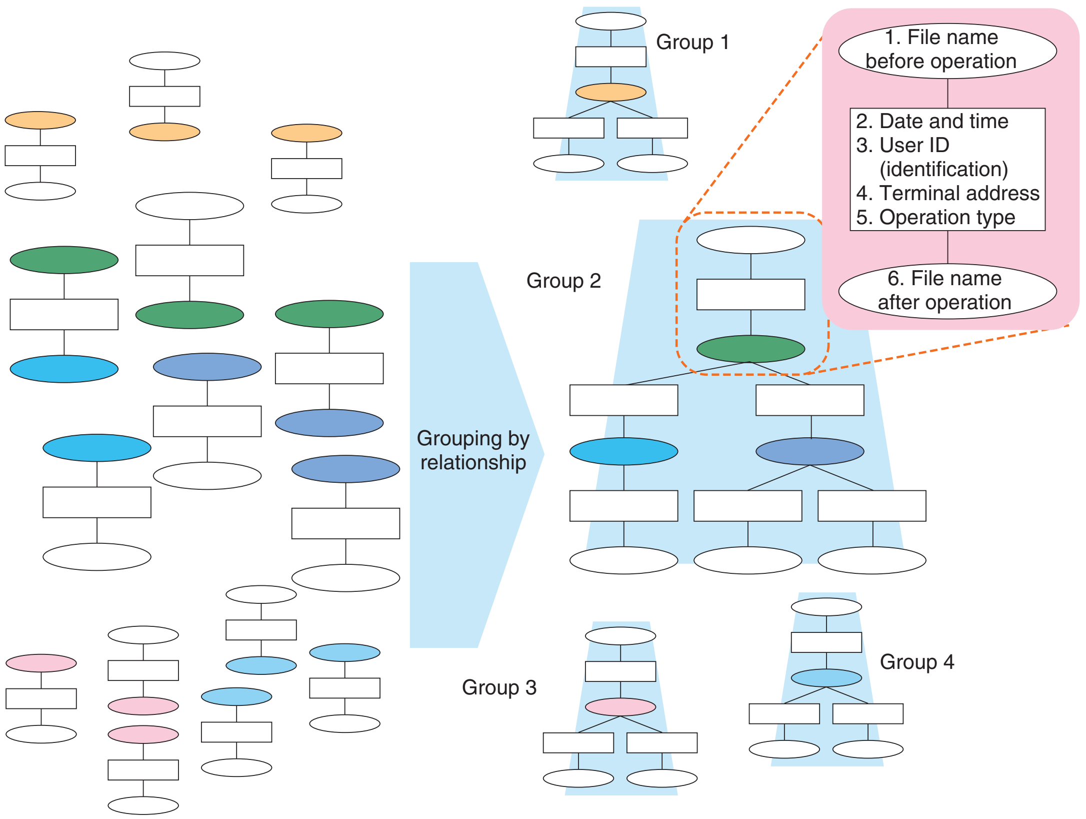


Fig. 4. Grouping for file operation event visualization.

In the grouping process of the normalized log, the names of the file before and after the operation are used. For example, if the file name before the operation for operation A is the same as the file name after the operation for operation B, then it is possible to relate the two operations as file operation events. Successively relating operations in this way makes it possible to manage files that have the same ancestor in the normalized log as a single group. This grouping can be processed at high speed by a proprietary algorithm that uses Hadoop Map Reduce [2]. Using groups constructed in this way makes it possible to search and display file operations at high speed.

(3) Scalability

File tracing in TRX uses a Hadoop distributed platform and is implemented with a scale-out-capable processing algorithm. The log storage can be scaled out from a single PostgreSQL relational database that can easily handle small-scale needs to HDFS (Hadoop Distributed File System) distributed processing by multiple units; HDFS processing is capable of conducting file tracing for offices with up to 100,000 employees.

2.2 Visualization of VM image copying (VM tracing)

In the past, a server was a fixed implementation in hardware, but the development of VM technology has changed the concept of a server to the form of a VM image file. This makes construction, addition, and copying of servers easy. Copying servers is advantageous, as it makes it easy to construct multiple servers when needed, such as for parallel processing tasks. However, there is also the disadvantage that license violations or information leaks may occur because the software license or critical information such as personal data that is included in the server image will also be copied. For these reasons, detecting the copying of servers has become a serious issue.

VM tracing is a function that detects the copying of a VM image and outputs a log when the virtual server boots up. This function embeds a notification mechanism called a *tracer* in the VM image and uses

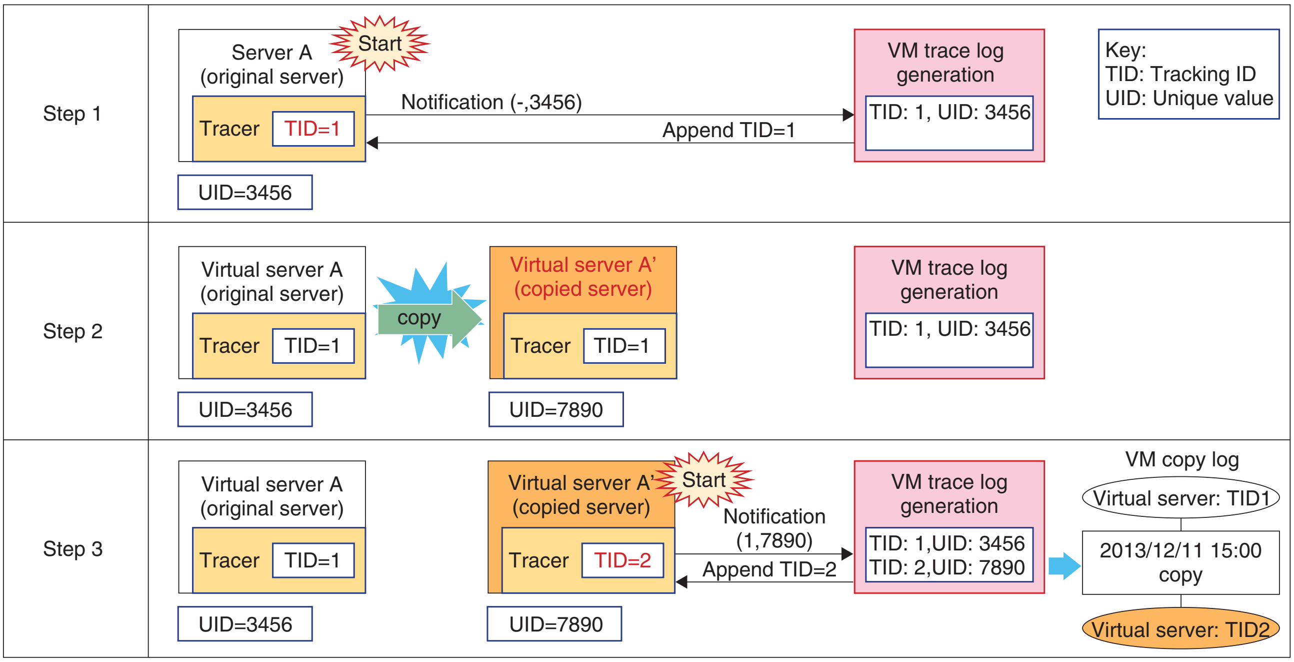


Fig. 5. VM trace log generation with active trace technology.

active trace technology to send a notification when the server boots up.

The mechanism of the VM trace log generator is illustrated in **Fig. 5**. In Step 1, the Unique Identification number (UID) 3456 is assigned to a virtual server instance when the instance is generated. Then the Tracking Identification number (TID) 1 is assigned and stored in the tracer when the virtual server is booted up. This pair of numbers is used for VM management. Consider the case in which virtual server A is copied, as in Step 2. When the copied server A' is booted up in Step 3, the notification contains TID=1 and UID=7890 (UID of server A'), but the VM trace log generator does not contain the pair of TID=1 and UID=7890; this means the VM image has been copied, and the event is logged. At the same time, a new TID=2 is assigned to the copied virtual server A'. In this way, VM image copying is detected and logged.

The remaining process of the generated log grouping is the same as for file tracing. This enables the VM image copy relationships to be tracked, and the grouping process enables the relationships to be visualized as a tree diagram. If VM images are restricted within a closed infrastructure-as-a-service (IaaS) provider system, tracking can also be done using the logs of hypervisors or other components. However, a function for uploading and downloading VM images makes it simple to move or copy images outside of the IaaS provider environment, which makes tracking difficult. Various products exist for protecting the data in a VM image, but they are ineffective when the entire VM image is copied. The VM tracing function of the TRX platform provides a post-incident method of tracking VM image copying, which has been a potential problem that may arise in the future.

3. Example of using visualization in the TRX platform

Examples of using the TRX traceability platform for file life-cycle management in an office and for virtual server operating system (OS) license management by a cloud provider are presented in **Table 1**.

3.1 File life-cycle management in an office

The need for strengthening internal control systems that pose a high risk of information leaks was described earlier. The TRX traceability platform can be used to manage the life cycle of files in a company. Installing an *agent* in the computers used by company personnel makes it possible to collect events related to company files, so that even in an environment where files are shared by multiple users, it is possible

Table 1. Example use of traceability platform.

	User (assumed)	Purpose	Effect
File life-cycle management in offices	- Company that has electronic files containing customer information or important internal information	- Strengthen internal control (electronic file management within the company)	- Confirm access and deletion of important information - Control information leaks - Rapidly respond to incidents
OS license management for virtual servers by cloud providers	- Cloud provider	- VM management - License management for OS etc.	- Easily confirm VM management in the cloud - Detect license violations for OS etc. - Control re-use of VMs that include royalty-bearing licenses

OS: operating system

to know when files are created, referenced, changed, copied, or deleted. It is also possible to retrace the path back to the original file, even when file names have been changed and the files have been moved between folders, or when derivative documents are created via common servers. This makes it easy to confirm that all files that contain erroneous information have been deleted and to find out whether important information has already been referenced by personnel.

3.2 Management of OS licenses in virtual servers by cloud providers

Cloud providers who rent out virtual servers to IaaS providers and other customers must properly manage the software licenses when the software included in the virtual servers is royalty-bearing software. Even when that is not the case, however, the software licenses may still require appropriate management.

Operations involving backup, redundancy, and the construction of test environments in the cloud provide many opportunities for copying VM images. It is also assumed that customers may download VM images enabling them to use services provided by other cloud providers. In such cases too, the VM tracing function described above can be used to ascertain that a VM image has been copied and booted up or that a problem concerning license management has occurred.

4. Future work

Introduction of the TRX traceability platform as a commercial product has begun. Specific points of improvement have come to light, and we are in the process of lowering the cost for a large-scale configuration, increasing the robustness of logging, and making improvements based on experience gained in operations.

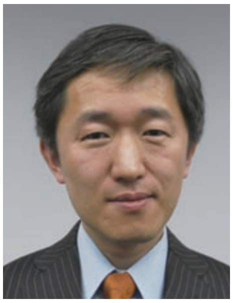
We intend to expand the range of tracing and are studying applications involving tracking of customer documents for which it is difficult to pre-install agents or other such mechanisms by applying the active trace technology that was developed for VM tracing to ordinary files [3].

References

[1] Ministry of Economy, Trade and Industry, Department of Commercial Information Policy, Office of Information Security Policy: “Information Security Management Guidelines for Use of Cloud Services,” METI Website, April 1, 2011 (in Japanese).
http://www.meti.go.jp/press/2011/04/20110401001/20110401001-2.pdf

[2] S. Nakahara and I. Tyou: “The Accountability of Cloud Services and Traceability Technology,” IEICE Technical Report, Vol. 112, No. 22, ICM2012–8, pp. 81–85, 2012.

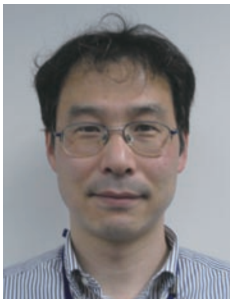
[3] I. Tyou, J. Akiba, T. Matsumura, and T. Motoda: “A Technology for Tracing General File Operations,” Proc. of CSS (Computer Security Symposium) 2013, pp. 832–839, Zhangjiajie, China.



Toshihiro Motoda

Senior Research Engineer, Supervisor, Security Management Promotion Project, NTT Secure Platform Laboratories.

He received the B.E. and M.E. in computer science and engineering from Toyohashi University of Technology, Aichi, in 1987 and 1989, respectively. He joined NTT Communications and Information Processing Laboratories in 1989 and studied end-user computing. He is currently studying an accountable security and traceability platform. He is a member of the Information Processing Society of Japan (IPSJ).



Junya Akiba

Senior Research Engineer, Supervisor, Security Management Promotion Project, NTT Secure Platform Laboratories.

He received the B.E. and M.E. in applied physics from Tohoku University, Miyagi, in 1990 and 1992, respectively. He joined NTT Switching Systems Laboratories in 1992 and studied advanced intelligent network systems. He is currently studying accountable security including audit and log management. He is a member of the Institute of Electronics, Information and Communication Engineers (IEICE) of Japan.

Takeshi Nagayoshi

Senior Research Engineer, Supervisor, Security Management Promotion Project, NTT Secure Platform Laboratories.

He received the B.E. and M.E. in electrical and electronics engineering from Sophia University, Tokyo, in 1990 and 1992, respectively. He joined NTT Information and Communication Systems Laboratories in 1992 and studied information security systems. He is currently responsible for developing the traceability platform.

Kaku Takeuchi

Research Engineer, Security Management Promotion Project, NTT Secure Platform Laboratories.

He received the B.E. and M.E. in computer science from Keio University, Tokyo, in 1992 and 1994 respectively. He joined NTT Software Laboratories in 1994 and was engaged in studying software engineering. He is a member of IPSJ.

Resilient Security Technology for Rapid Recovery from Cyber Attacks

Takaaki Koyama, Kunio Hato, Hideo Kitazume, and Mitsuhiro Nagafuchi

Abstract

Cyber attacks are a constant threat. In addition to taking the conventional—mainly defensive—countermeasures, it is important to do the utmost to control the effects of an attack once it has occurred in order to recover from those effects as rapidly as possible. In this article, we describe the concept of resilient security, present some use cases, and explain the technology that is used.

Keywords: network security, resilient security, security orchestration

1. Introduction

Public organizations and private enterprises have been subject to a barrage of cyber attacks in recent years. Those attacks cleverly work their way past conventional defensive measures in order to penetrate and exploit servers and network systems. Taking proactive security measures is a matter of course, but it is also important to assume there will be some damage from such attacks and to exert the utmost effort to control the damage and rapidly recover from the effects of an attack once it has been launched.

The development of computing resource virtualization has led to the study of network functions virtualisation* (NFV) and network software control. Virtual appliance products such as virtual switches and virtual firewalls are also beginning to appear in the actual market. These new technologies can be used to enable appropriate measures against attacks to be rapidly implemented on the network side by constructing flexible, reconfigurable networks.

In this article, we introduce the concept of resilient security, which is implemented with the technologies described above. We also present use cases and describe the virtual network and virtual appliance control technologies applied in those cases. Additionally, we discuss the work being done in our laboratories.

2. Objectives of resilient security

We are working to maintain service continuity in the event of unpredictable natural disasters or incidents involving security threats that evolve from year to year by autonomously implementing measures that have multiple layers and multiple aspects as virtual appliances. The objectives are to limit the scope of effects on services to the very minimum by controlling multiple devices at the appropriate points according to the type of attack and to provide clean pipe functions to isolate attacks and achieve rapid recovery.

One difficulty, though, is that the burden on operators to analyze and deal with sophisticated cyber attacks has been increasing rapidly. Reducing that burden is thus another aspect of our work, and we are developing recommendations for operators based on information we obtain about detected attacks and scenario-based autonomous control of multiple virtual appliances in order to implement measures that do not depend on the skill level of operators.

Also, even in cases where it cannot immediately be determined that an attack is in progress, it is still possible to secure the time needed for analysis by flexibly reinforcing virtual firewall resources and isolating the

* The British spelling used by the European Telecommunications Standards Institute

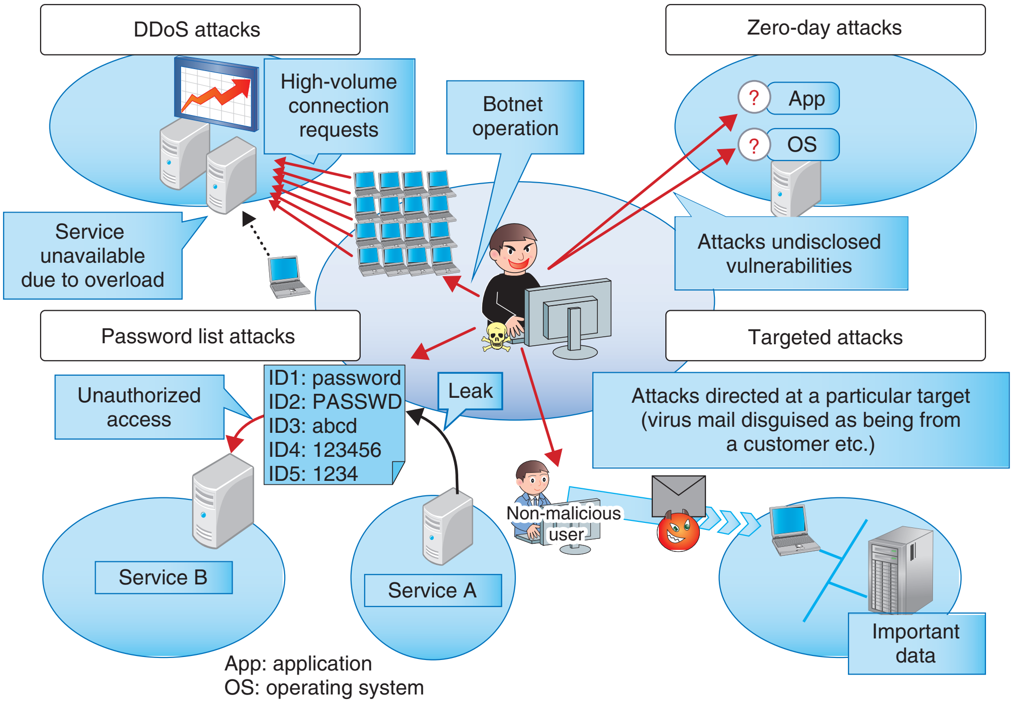


Fig. 1. Increasingly sophisticated cyber attacks.

attacked virtual machine (VM) to a quarantine network.

This application is also planned for network services, and to achieve this, the NTT Secure Platform Laboratories is also providing safe and secure platform technology to eliminate end-user concerns about the security of cloud or network services.

3. Advanced cyber attacks

This section introduces typical examples of recent cyber attacks (**Fig. 1**) and gives an overview of those that are becoming difficult to prevent by pre-incident measures only.

3.1 DDoS attacks

A distributed denial of service (DDoS) attack targets a service that is open to the public and uses a botnet composed of a very large number of terminals to flood servers with connection requests, thus overloading the servers and interfering with the provision of the targeted service. This kind of attack is difficult to distinguish from ordinary user traffic when the connections are examined one at a time, so it is very difficult to recognize and block only the malicious communication.

3.2 Zero-day attacks

A zero-day attack exploits software vulnerabilities (security holes) that are unannounced and for which countermeasures have not been established. This type of attack generally targets unknown vulnerabilities, so the attack is launched before patches to remove the vulnerabilities are applied, making defense against such attacks very difficult.

3.3 Password list attacks

In this type of attack, a list of identifications (IDs) and passwords that was somehow leaked from one source is used to attack a completely different service by attempting an unauthorized log-in to another person's account. These attacks appear as individual log-in requests that are essentially no different from normal user use, and the ID and password combinations appear to be genuine, which makes it very difficult to distinguish the behavior as an attack and eliminate it.

3.4 Targeted attacks

This type of attack is characterized by the targeting of a particular company or organization for a particular purpose, such as theft or falsification of personal information or assets. Such attacks are designed for specific situations, so the methods are difficult to predict by looking at past attacks. They apply social engineering approaches that take advantage of human emotion and curiosity to create security vulnerabilities. It is therefore difficult to defend against this type of attack automatically with a security system.

4. Trends in virtual networks and virtual appliances

In this section, we introduce the virtual networks and virtual appliances that are used in current networks as technical elements of resilient security, which serves as an effective means of dealing with the different types of attacks described in the previous section. We also explain security orchestration functions for achieving resilient security.

4.1 Virtual networks

Virtual networks (NWs) are a virtual private network (VPN) technology for creating isolated networks for individual customers as an Internet Protocol (IP) network that is constructed within a cloud system and extends to the customer's premises. IP networks can be constructed for both on-demand and high-volume use. Three types of systems are used: tagged VLAN (virtual local area network), OpenFlow-based hop-by-hop systems, and tunneling-based overlay systems [1].

Also, working in coordination with a cloud management system makes it possible to change network settings automatically for live migration of VMs. If a VM is moved to a different hypervisor, the customer's IP network can be moved to a different physical network without terminating the session, and isolation is also possible. In 2012, the OpenStack open source software (OSS) cloud management system also began providing virtual NW construction and other such operations [2].

4.2 Virtual appliances

A virtual appliance can provide network functions that have previously been provided by dedicated hardware such as routers, firewalls (FWs), and load balancers (LBs) as software implementations in a virtual environment. These functions constitute the set of functions needed to construct an enterprise intranet, and virtual appliances were developed to meet the need to use those functions with a virtual network. Research has been done recently on appliances running in dedicated virtual environments as dedicated network equipment for which functions can be freely combined and replaced. Standardization under the general name of NFV is also in progress. Virtual appliances that provide an intrusion detection system, web application firewall, and other such security functions in addition to an FW and LB have also been developed. In 2013, Linux network namespace settings for the OpenStack OSS virtual router, virtual FW, and virtual LB became available, and the number of virtual appliance products that can be controlled with OpenStack is increasing.

4.3 Distributed virtual appliances

The standard specifications for routers and FWs specify one operating unit, with others serving as spares. This prevents the distribution of virtual appliances and makes it difficult to distribute the virtual appliance load or completely separate communication paths that pass through virtual appliance input/output interfaces in units of IP addresses and end-to-end connections. Techniques for a distributed arrangement of multiple virtual appliances and route changing in a flow unit at layer 4 are therefore required. In regard to the distributed arrangement of virtual appliances, companies such as VMware, vArmour Networks, and others are making progress in implementing configurations of their own products in which multiple appliances connected in a dedicated virtual network work cooperatively to reduce the processing load. Rerouting techniques include those that use conventional switches and those that use advanced switches. Conventional switches can be used in three ways: using a routing protocol and directly rewriting the routing table to change the routing destination; using address conversion techniques and a DNS (domain name system) server to change the destination IP address; and rewriting the media access control (MAC) address table to change the destination MAC address without changing the IP address. When advanced switching functions are used, switching can be done according to IP packet header data such as the TCP (transmission control protocol) or UDP (user datagram protocol) port number in addition to the IP address [3]. The built-in switch of the hypervisor or the OpenFlow switch can be used, and implementation using ordinary OpenFlow switches, etc., as well as VMware NSX or the OSS Linux OpenvSwitch is also possible.

4.4 Security orchestration functions

Currently, the NTT Secure Platform Laboratories is developing ways to implement resilient security using virtual NWs and virtual appliances as well as distributed virtual appliances. Specifically, security orchestration functions have been configured that can work in cooperation with various devices to collect information and define device control scenarios. The security orchestration system functions together with multiple types of virtual appliances located on networks and systems and with server and network device logs to detect indications of cyber attacks and the damage they have caused. Even though the zero-day attacks, password list attacks, targeted attacks, and other attacks described in section 3 are themselves difficult to detect, it is not impossible to discover proof of damage that corresponds to the purposes of attacks, such as the altering of data or information leaks. Using virtual appliances as security sensors enables the placement and number of units to be changed dynamically for efficient detection. Detected cyber attacks are automatically classified as those for which countermeasures are possible and those for which countermeasures are not possible. Even for the attacks for which an automated response is not possible, automatic generation and notification of response recommendations that guide the decisions of the operator is possible. That function is implemented by arranging the appropriate virtual appliances at the right places in the system in order to control servers and network equipment. When the existing configuration is inadequate, virtual appliances are automatically added, and control is performed to move traffic to the virtual NW, thus preventing major harm, blocking the attack, and strengthening the system. Even when it is difficult to directly block an attack, such as with a DDoS attack, if the system can be strengthened and services continued by automatically adding resources such as virtual appliances in response to the attack, then the attack can be withstood, and the purpose of the attack can be defeated.

5. Resilient security engine through security orchestration

The resilient security engine being developed by the NTT Secure Platform Laboratories is intended for implementation as a security orchestration system for coping with cyber attacks. As the first step, we are currently developing a security orchestration system for protecting normal communication with VMs against DDoS attacks on a datacenter (DC) on which cloud services are running and for minimizing the harm to the DC and the VM under attack. The operation of the system is illustrated in **Fig. 2**. There are functions for recommendations to deal with three cases: 1) a DDoS attack on the DC or FW set up for each customer IP network will prompt a recommendation to the operator to use external network equipment to block the attack; 2) an attack that can be clearly determined to be on a VM will prompt a recommendation to the operator to block the attack with a virtual FW or external network equipment; and 3) discovery of communication that is suspected to be an attack on a VM will prompt a recommendation to reinforce the virtual FW resources, migrate to a different DC, or block the attack by a virtual FW or external network equipment. The first of these three cases is a matter of maintaining continuity of the network service, the second involves preventing an attack on a VM, and the third involves implementing a response when a gray zone is determined. Defense against a DDoS attack is described here, but the functions for the second and third cases described above are being designed for application to various types of attacks, with a view to applying them to targeted and other attacks.

The three internal functions are for logging, analysis and identification of an attack, and appliance setup. Functions are provided for analysis and determination according to scenarios for which conditions are set within the resilient security engine using flow data, attack detection data, and data collected by security sensors for judging suspected attacks, and for making recommendations to the security operator in the cases of automatic virtual FW setup and blocking with external network equipment. Naturally, the security operator is informed even when the setting is for the reinforcement of virtual FW resources or migration to another DC; the setting for manual blocking for the virtual FW can be performed later based on the security operator’s decision. We are moving forward with development in which we describe the operation for the three cases described above as scenarios. Customization is possible according to the individual operation conditions and descriptions.

6. Future development

We are currently developing virtual FW control technology for dealing with DDoS attacks. When this development is completed, we plan to conduct trials to evaluate its effectiveness. We also plan to expand the extraction of control scenarios from actual operation sites and extend the types of virtual appliances in order to cope with complex, advanced, and sustained attacks.

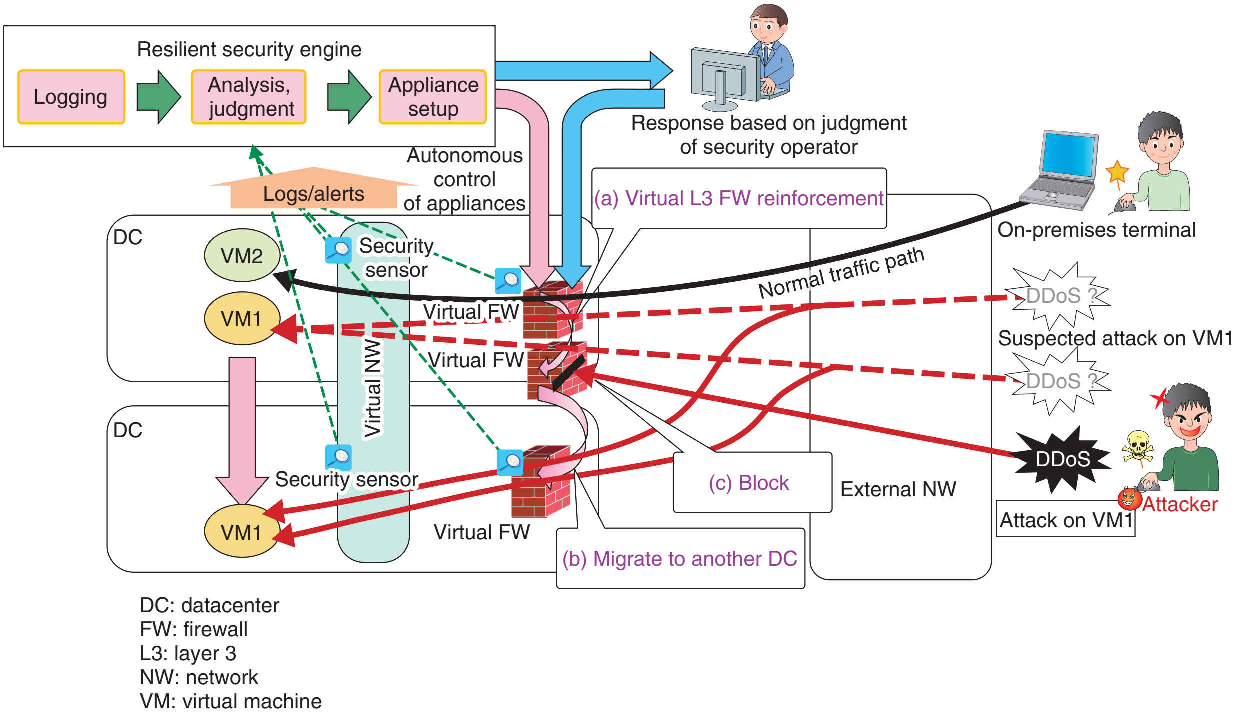


Fig. 2. Resilient security engine.

References

[1] H. Kitazume, T. Koyama, Y. Tajima, T. Kishi, and T. Inoue, "Network Virtualization Technology for Cloud Services," NTT Technical Review, Vol. 9, No. 12, 2011.
https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201112fa4.html

[2] S. Mizuno, H. Sakai, D. Yokozeki, K. Iida, and T. Koyama, "IaaS Platform Using OpenStack and OpenFlow Overlay Technology," NTT Technical Review, Vol. 10, No. 12, 2012.
https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201212fa1.html

[3] T. Koyama, T. Kishi, T. Inoue, Y. Nagafuchi, and H. Kitazume, "Report on the Effects of Multiple Active Virtual Routers and Virtual L3 FW," IEICE Technical Report, Vol. 113, No. 303, IN2013-89, pp. 13–18, 2013.

Takaaki Koyama

Senior Research Engineer, Network Security Project, NTT Secure Platform Laboratories.

He received the B.A. and M.M.G. in media and governance from Keio University, Tokyo, in 1994 and 1996, respectively. He joined NTT Software Laboratories in 1996 and has been studying software CALs (client access licenses). Since 1999, he has been studying a type of IP-VPN technology called GMN-CL, and developing network equipment. His recent research interests are enterprise cloud network systems and security orchestration systems. He is a member of the Information Processing Society of Japan.

Kunio Hato

Senior Manager, Network Services, NTT Communications Corporation.

He received the B.E. and M.E. in information processing from Tokyo Institute of Technology in 1997 and 1999, respectively. Since joining NTT in 1999, he has been engaged in researching and developing IP VPNs, Wide Area Ethernet, network security systems and intercloud computing systems. He is a member of the Institute of Electronics, Information and Communication Engineers (IEICE).

Hideo Kitazume

Senior Research Engineer, Supervisor, Network Security Project, NTT Secure Platform Laboratories.

He received the B.E and M.E. in computer science from Gunma University in 1987 and 1989, respectively. He joined NTT in 1989 and engaged in researching and developing ATM-LAN systems, studying ATM traffic control, and developing a global networking service platform. From 1998 to 2010, he was involved in the development, design, and operation of IP-VPN services at NTT EAST. He is currently researching and developing network security orchestration technologies based on network virtualization. He is a member of IEICE and the Operations Research Society of Japan.

Mitsuhiro Nagafuchi

Manager, Produce Section (Security), Research and Development Planning Department.

He received the B.A. in mechanical information science and technology from Kyushu Institute of Technology in 1997. He joined NTT in 1997. He was with the Corporate Sales Department of NTT WEST from 1999 to 2013.

R&D on Secure Computation Technology for Privacy Protection

Koji Chida, Dai Ikarashi, Teruko Miyata, Hiroyoshi Takiguchi, and Naoto Kiribuchi

Abstract

Demand is growing for a means of securely processing highly confidential data on the cloud. To meet this demand, the NTT Secure Platform Laboratories has developed practical, fast, multi-party secure computation technology that provides both confidentiality and usability. This article presents some background issues concerning this technology and explains efforts to develop the basic mechanism into a commercial product.

Keywords: secure computation, cloud security, personal data

1. Introduction

Innovation in information and communication technology is making it possible to collect and analyze large amounts of diverse data, and there are increasingly high expectations for value creation by using big data. In particular, various efforts have been made recently to enable secondary use of personal data for the development of society and industry. The term *personal data* is not limited to the data defined by the Personal Information Protection Law, but is used in the broader sense of all information that concerns individuals [1]. Businesses that handle personal data are responsible for giving sufficient consideration to the privacy of the individuals who provide that information and for taking appropriate security management measures. Article 20 of the Personal Information Protection Law, Measures for Security Management, states that "Businesses that handle personal data must prevent the leaking, loss, or damage of that personal data and devise other appropriate measures for managing the security of personal data." In general, obtaining the *consent of the person* in respect to the purposes for using personal data is different from taking measures required by the Measures for Security Management. Leakage of personal data after the business obtains consent is an issue of responsibility, and such leakages reduce the public's trust.

The problem, then, is what security management measures are necessary and appropriate for the secondary use of personal data. Consider, for example, the situation in which individuals and businesses provide personal data to cloud providers, the cloud providers process the personal data for provision to secondary users, and the secondary users use the results of that processing (**Fig. 1**). In this case, the processing results consist of analysis results or anonymized personal data. The cloud provider is required to take security management measures for the obtained personal data and also for the processing results provided to the secondary user. In particular, the suppliers of the personal data cannot directly manage or control the personal data supplied to the cloud provider, and therefore, they probably worry about the possible leakage or unintended use of that data. This concern about security is cited as the most important factor in decisions to refrain from using cloud services. The concept known as *secure computation* has been attracting attention as a technological solution for security management that solves that problem by preventing the leakage or misuse of personal data and by maintaining privacy. In the remainder of this article, we present an overview of technology related to secure computation and describe the work being done at the NTT Secure Platform Laboratories.

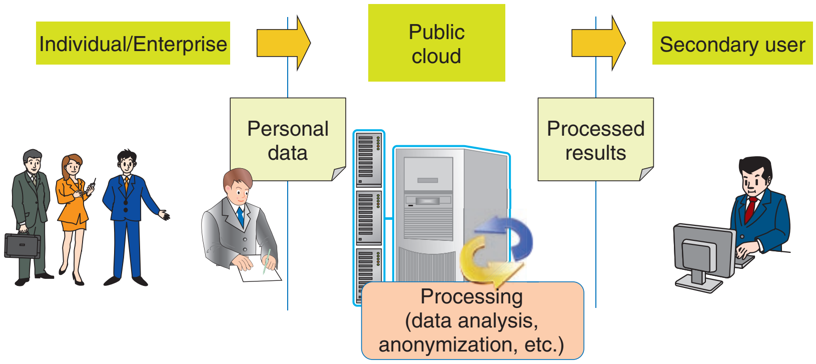


Fig. 1. Example process of secondary use of personal data.

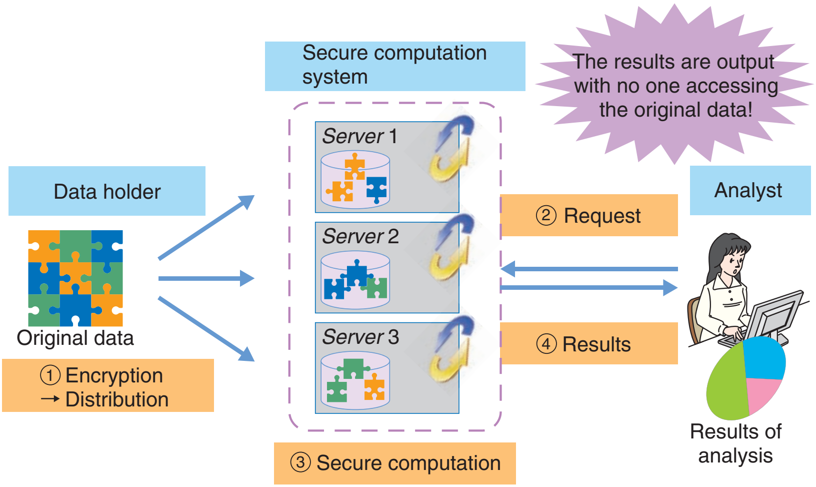

Secure computation system
The results are output with no one accessing the original data!
Server 1
Server 2
Server 3
Data holder
Original data
① Encryption → Distribution
Analyst
② Request
④ Results
Results of analysis
③ Secure computation

Fig. 2. Basic system model of secure computation.

2. Secure computation

Secure computation technology allows statistical processing and other kinds of data processing to be performed on data that remains in a secure form. One security measure used when information is entrusted to the cloud is data encryption. When the data processing is also done in the cloud, the processing is not usually performed with the data in the encrypted state, so the data must be decrypted in the cloud, which creates a risk of data leakage.

Secure computation is a technology that reduces that risk. A secure computation system is illustrated schematically in **Fig. 2**. First, the possessor of the data to be used in statistical processing or another form of processing sends the anonymized data to a secure computation system. Next, the analyzing party that wants to do the processing sends a request for analysis to the secure computation system. The secure computation system then performs the processing on the data that is still in the anonymized form and sends only the results to the party that requested the analysis. The special feature of secure computation is that the data is never decrypted, and the requesting party never receives anything other than the analysis results.

The secure computation technology that is currently under development is implemented by the interworking of multiple computers (secure computation servers) that communicate with each other. The input data is first anonymized with a secret-sharing algorithm and then distributed among the secure computation servers. The secure computation servers perform the processing while exchanging the

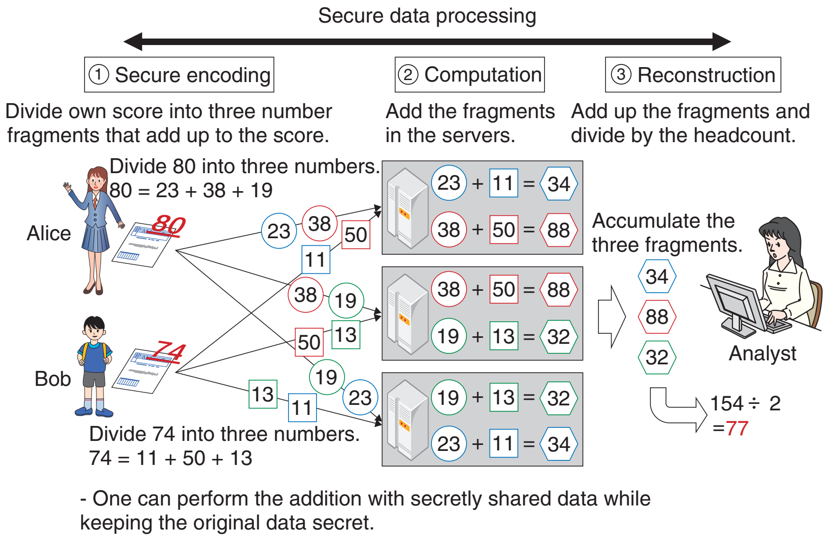

Secure data processing
① Secure encoding
② Computation
③ Reconstruction
Divide own score into three number fragments that add up to the score.
Add the fragments in the servers.
Add up the fragments and divide by the headcount.
Divide 80 into three numbers.
80 = 23 + 38 + 19
Alice
80
23
38
50
11
38
19
50
13
Bob
74
19
13
11
23
Divide 74 into three numbers.
74 = 11 + 50 + 13
23 + 11 = 34
38 + 50 = 88
38 + 50 = 88
19 + 13 = 32
19 + 13 = 32
23 + 11 = 34
Accumulate the three fragments.
34
88
32
Analyst
154 ÷ 2
=77
- One can perform the addition with secretly shared data while keeping the original data secret.

Fig. 3. Simple example of secure computation processing.

anonymized data among themselves. The simplest example of secure computation processing is illustrated in **Fig. 3**.

In Fig. 3, person A (Alice) and person B (Bob) have test scores. We want to obtain the average score for these two people without anyone learning what the individual test scores are. To obtain that result, the two test scores are first processed by implementing secret distribution. Specifically, each score is split into three numbers whose sums are the original scores. Those three distributed numbers are sent to secure computation servers, which then add up the received data. Finally, the resulting numbers are summed, and the sum is divided by the number of persons (two in this case) to obtain the ultimate result, which is the average test score for the two people (77 in this example). The numerical values used within the secure computation servers are unrelated to the original test scores, so the privacy of person A and person B is preserved.

The method depicted in Fig. 3 can only be used to obtain an average value. In 1982, however, A. C. Yao proposed a method that enables secure computation for any type of processing [2], although it was impractical for processing very large amounts of data. Research to improve efficiency has continued since that time, however. Research on secure computation began over ten years ago at the NTT Secure Platform Laboratories, and we achieved the world's fastest processing in 2005 [3]. Good compatibility between secure computation and statistical processing has also been discovered in recent years, and experiments that verify practical performance have been conducted [4].

3. Overview of the Trust-SC secure computation platform

Trust-SC is the first on-line statistical analysis system that was developed applying secure computation technology for commercial use. NTT Secure Platform Laboratories keeps striving to be a world leader in research on secure computation technology, and this on-line service makes it possible to analyze data and obtain results of statistical analysis without reconstructing any master data.

An overview of the Trust-SC platform is presented in **Fig. 4**. The main features are explained in the following subsections.

3.1 Fast processing and variety of statistical functions with combination of *R* functions

The statistical functions provided by the Trust-SC secure computation platform are listed in **Table 1**. The first group of functions includes basic statistical functions (maximum, minimum, median, mean, and distribution), the second group consists of applied statistical functions such as table operations and a t-test function, and the functions in the third group are related to database processing operations (search and shuffle). Most all-purpose statistical functions can be covered by combining Trust-SC and "R" statistical

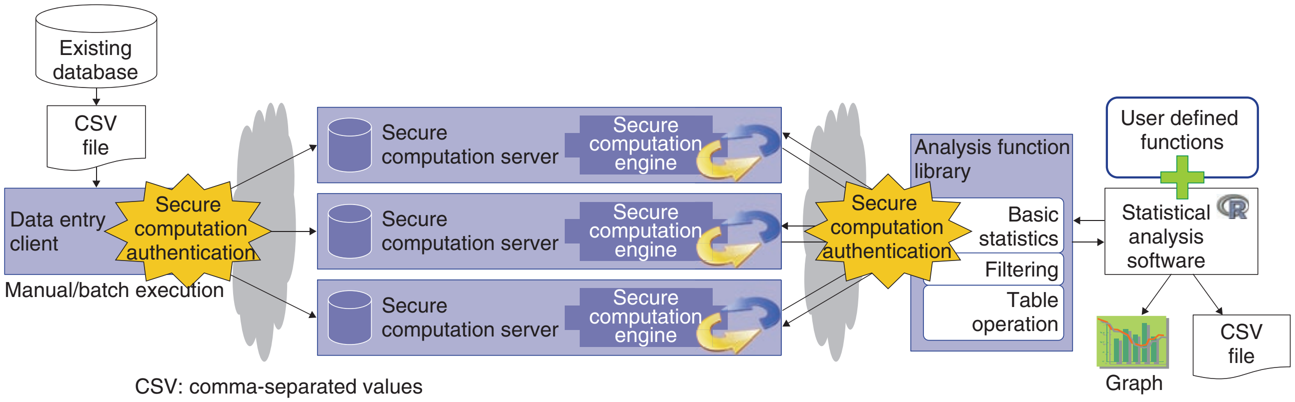

Existing database
CSV file
Data entry client
Manual/batch execution
Secure computation authentication
Secure computation server
Secure computation engine
Secure computation server
Secure computation engine
Secure computation server
Secure computation engine
Secure computation authentication
Analysis function library
Basic statistics
Filtering
Table operation
User defined functions
Statistical analysis software
R
Graph
CSV file
CSV: comma-separated values

Fig. 4. Trust-SC secure computation platform.

Table 1. Statistical functions provided by Trust-SC.

Type	Function
Basic statistical functions	Maximum Minimum Median Mean Distribution
Applied statistical functions	Table operations t-test Kaplan-Meier estimator
Additional functions	Item count Item filter Shuffle

functions. Furthermore, the performance of the Trust-SC functions has the possibility of achieving the world's fastest speed class while still keeping data in an anonymized form.

This performance was largely possible thanks to NTT's research on a secure computation algorithm. The Trust-SC platform does not require any special personal computer (PC) power; it can be installed and perform those functions at high speed on ordinary PC servers (e.g., a four-core CPU (central processor unit) and 32 GB of RAM (random access memory)).

3.2 Statistical analysis with R

The Trust SC is operable with the R language, a major statistical computing and graphics OSS (open source software) tool that is used extensively in various fields, including medicine, finance, and the environment (**Fig. 5**). The statistical analysis functions supplied by the Trust-SC platform are all implemented as R function libraries. By using R, the basic statistical functions listed in Table 1 can be combined to define other required R functions. Also, the many R library functions can be used to output results in various formats such as graphs and files.

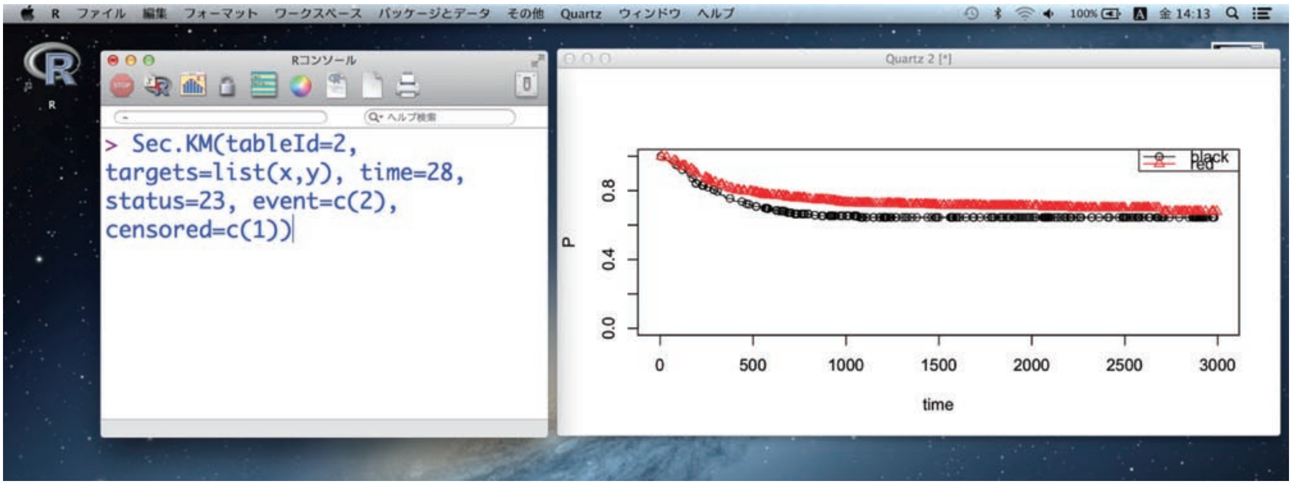
3.3 Secure computation authentication

This system prevents leaking of the original data even if a single secure computation server is breached. A security policy of this kind, however, requires that the user perform authentication with a different password for each secure computation server. The secure computation authentication process uses a proprietary method that achieves both usability and security. The user uses a single password for authentication, but the passwords stored in the servers are managed in secret-sharing encryption form, and password verification is performed with secure computation. Even in the event that one secure computation server is invaded, only a single item of secret-sharing data can be leaked, and it is not possible for someone to obtain the data needed to pose as the user.

4. Future development

Research on secure computation was previously only theoretical, but practical research has suddenly accelerated with the demand for security management in the secondary use of personal data, and practical goals have been established. The NTT Secure Platform Laboratories has developed the world's first commercial-level secure computation system and confirmed the ability of the system to carry out data analysis processing on a data scale of 100,000 items in a practical amount of time.

Our future tasks include developing the system so



```
> Sec.KM(tableId=2,
targets=list(x,y), time=28,
status=23, event=c(2),
censored=c(1))
```

Fig. 5. Results of executing a Kaplan-Meier estimator with R.

that it is capable of handling data on a larger scale for use in big data applications, and adopting a social scientific approach to research that supports relevant laws in order to give users a greater sense of security.

References

[1] IT Strategic Headquarters, Personal Data Study Group (in Japanese).
http://www.kantei.go.jp/jp/singi/it2/pd/index.html

[2] A. C. Yao, “Protocols for Secure Computations (Extended Abstract),” Proc. of 23rd Annual Symposium on Foundations of Computer Science (FOCS 1982), pp. 160–164.

[3] NTT press release, “World’s Fastest Secure Circuit Evaluation Algorithm Enabling Arbitrary Operation on Encrypted Data,” published on October 25, 2005.
http://www.ntt.co.jp/news/news05e/0510/051025.html

[4] NTT press release, “World’s First Verification of Secure computation Technology Applied to Medical Statistical Processing,” published on February 14, 2012 (in Japanese).
http://www.ntt.co.jp/news2012/1202/120214a.html

Koji Chida

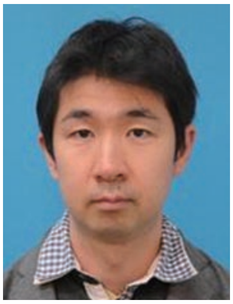
Senior Research Engineer, Information Security Project, NTT Secure Platform Laboratories.

He received the B.S. and M.S. from Waseda University, Tokyo, in 1998 and 2000, respectively. Since 2000, he has been engaged in research on cryptography and privacy enhancing technologies at NTT. He received the Dr. Eng. degree from Waseda University in 2006. He is a member of the Information Processing Society of Japan (IPSJ). He was awarded the IPSJ Best Paper Award in 2012.

Hiroyoshi Takiguchi

Research Engineer, Security Management & Operations Project, NTT Secure Platform Laboratories.

He received the B.S. and M.S. in human-environment studies from Kyushu University, Fukuoka, in 2000 and 2002, respectively. He joined NTT laboratories in 2003. His current fields of interests are protection technology of privacy and identity management.



Dai Ikarashi

Researcher, Information Security Project, NTT Secure Platform Laboratories.

He received the B.S. and M.S. from The University of Tokyo in 2005 and 2008, respectively. Since 2008, he has been engaged in research on cryptography and information security at NTT. He is a member of the IPSJ.

Naoto Kiribuchi

Security Management & Operation Project, NTT Secure Platform Laboratories.

He received the B.E. and M.E. in informatics from the University of Electro-Communications, Tokyo, in 2010 and 2012, respectively. He joined NTT laboratories in 2012. His current fields of interests are cryptography and information security.

Teruko Miyata

Senior Research Engineer, Security Management & Operations Project, NTT Secure Platform Laboratories.

She received the B.S. and M.S. in mathematical science from Ochanomizu University, Tokyo, in 1991 and 1993, respectively. She joined NTT laboratories in 1993. Her current fields of interests are protection technology of privacy and identity management.

Fully Homomorphic Encryption over the Integers: From Theory to Practice

Mehdi Tibouchi

Abstract

Fully homomorphic encryption is a groundbreaking cryptographic technique that allows the processing of data in encrypted form and is likely to have major applications in cloud security. However, significant efficiency improvements are needed before we can hope to put it to practical use. We, at the NTT Secure Platform Laboratories, have made multiple theoretical and practical advances in the area of fully homomorphic encryption over the integers, which is a particular type of fully homomorphic encryption, and have obtained the world's fastest implementation of it to date as a result.

Keywords: security, cryptography, cloud computing

1. Fully homomorphic encryption

In recent years, we have been entrusting more and more of our electronic data to the cloud, including e-mail, internal company documents, and personal information. Protecting the privacy and confidentiality of that data is a major challenge for today's security researchers and practitioners. A 2013 study by the Cloud Security Alliance revealed a worrying increase in the number of major data breach incidents in which cloud data was leaked as a result of negligence, malware, or insider attacks [1]. Cryptographers have proposed several possible approaches to addressing the problem of cloud security without compromising on functionality. One of the most promising approaches is fully homomorphic encryption, which has garnered a lot of attention in recent years.

Encrypting data before sending it to the cloud is a simple way of guaranteeing confidentiality. Parties who do not own the decryption key, including malicious hackers and the cloud server operators themselves, cannot learn anything about the data that was encrypted. Therefore, that data remains safe even in the case of a breach. However, if one uses traditional encryption, it also becomes impossible for the cloud operators to carry out any kind of processing of that data (even searching it, for example), as they would have to decrypt it first. This defeats the purpose of most applications of cloud computing. Fortunately, fully homomorphic encryption eliminates that limitation. Data encrypted with fully homomorphic encryption enjoys essentially the same security guarantees as with traditional encryption, but it becomes possible to carry out arbitrary computations on it without decrypting it first. The result of those computations remains in encrypted form, and can thus only be recovered by the owner of the decryption key. That unique property makes it possible to build a wide range of highly secure cloud services.

2. Potential applications

The most direct application of fully homomorphic encryption is probably *outsourced computation* (**Fig. 1**). Consider a scenario in which a client has some sensitive data to process but lacks the required expertise or sufficient computational power; as a result, they want to commission a cloud service to carry out the processing, but without revealing this sensitive data in plaintext form. Fully homomorphic encryption offers a simple solution to that problem; the client simply sends the data to the cloud server in encrypted form, and the server processes the data without decrypting it using the property of fully homomorphic encryption (this computation on encrypted data is called

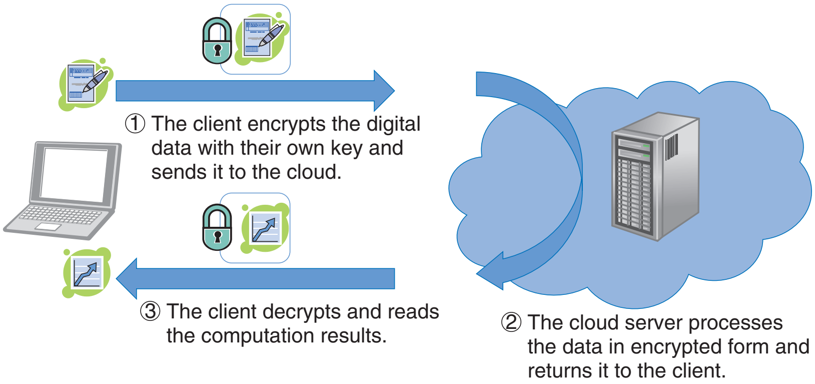

① The client encrypts the digital data with their own key and sends it to the cloud.
② The cloud server processes the data in encrypted form and returns it to the client.
③ The client decrypts and reads the computation results.

Fig 1. Outsourced computation based on fully homomorphic encryption.

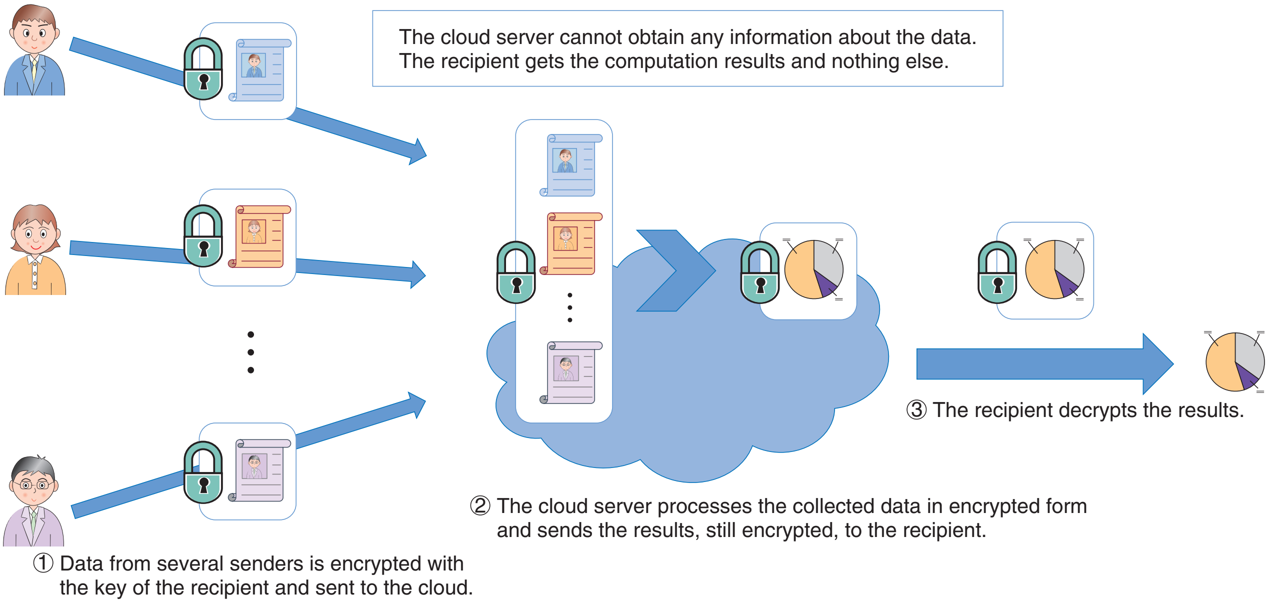

The cloud server cannot obtain any information about the data.
The recipient gets the computation results and nothing else.
① Data from several senders is encrypted with the key of the recipient and sent to the cloud.
② The cloud server processes the collected data in encrypted form and sends the results, still encrypted, to the recipient.
③ The recipient decrypts the results.

Fig. 2. Anonymous data processing with fully homomorphic encryption.

homomorphic evaluation of the corresponding function). Finally, the client receives the encrypted output from the server and decrypts it with his key, obtaining the result of the processing without having revealed any information about the sensitive data. For example, cloud services already exist that perform backtesting of stock market trading strategies, but professional traders are unlikely to rely on them for fear of revealing highly valuable strategies. With fully homomorphic encryption, however, it is possible to provide a backtesting cloud service to traders while ensuring that their valuable techniques will remain safe from prying eyes (even those of the cloud operators themselves!). Similarly, one can imagine cloud services that provide DNA (deoxyribonucleic acid) analysis for medical institutions and law enforcement authorities while maintaining the confidentiality of DNA samples, or services that perform mechanical structural analysis for the aerospace or construction industries without asking clients to compromise the secrecy of their designs.

Another application of fully homomorphic encryption is *anonymous data processing* (**Fig. 2**). This kind of scenario involves multiple users sending some sensitive data to a cloud server, where it is aggregated, stripped of identifying information, and analyzed, typically to extract some statistical information, which is then delivered to the final recipient. The security requirement is that the cloud server must learn nothing about the content of users' data, and the recipient must obtain only the anonymized results of the statistical analysis, and in particular, no information on individual users. This can also be achieved using fully homomorphic encryption; the users first use a fully homomorphic encryption scheme to encrypt their own data under the recipient's public key and send it to the cloud server. The data collected on the server is then processed in encrypted form using homomorphic evaluation. The result of this processing is the anonymized statistical information, also in encrypted form. That output is then sent to the recipient, who finally decrypts it. Possible applications of such a protocol include secure electronic voting, where individual voters encrypt their ballots with the public key of the organizer of the vote and then send them to a tallying server. The server uses homomorphic evaluation to carry out validity checks on encrypted ballots and to compute the encrypted tally, which is then sent to the organizer, who finally decrypts that aggregate result without learning individual votes. Secure auctions and statistical analysis of medical data are other possible uses.

There are also examples of cloud services for which fully homomorphic encryption is not well suited. One is encrypted search on a database. The reason for this is that the server cannot obtain any information on the content of the search query, so homomorphic evaluation of the search operation requires processing the entire database from beginning to end, rather than just a small portion of it, making the whole operation very computationally costly. A secure web search service based on fully homomorphic encryption, for example, would be prohibitively impractical. Similarly, spam filtering of encrypted e-mail and other services that require the cloud server itself to obtain the result of processing encrypted information cannot be implemented using homomorphic encryption. In the case of spam filtering, for example, processing e-mail using homomorphic evaluation would yield a list of messages detected as spam in encrypted form, making it impossible for the server itself to delete them without asking the client to decrypt that list first, a rather inconvenient process.

Despite such limitations, though, fully homomorphic encryption is undoubtedly a very promising technology for cloud security—if only it can be made efficient enough for practical applications. At the NTT Secure Platform Laboratories, we are hard at work trying to achieve this goal.

3. Fully homomorphic encryption over the integers

The concept of fully homomorphic encryption itself was proposed in the late 1970s, but constructing an actual fully homomorphic encryption scheme remained an open problem for a long time; in fact, many cryptographers believed that it was impossible. In 2009, however, Craig Gentry of Stanford University disproved this widely held belief by describing the first fully homomorphic encryption scheme. The following year, he also proposed, together with van Dijk, Halevi, and Vaikuntanathan, a conceptually simpler construction of fully homomorphic encryption, based entirely on integer arithmetic. These results were major theoretical breakthroughs, but the proposed schemes were both extremely inefficient; thus, the problem of fully homomorphic encryption, while solved in theory, remained open as far as practical implementations were concerned.

Here is a succinct, somewhat simplified description of the original fully homomorphic encryption scheme over the integers of van Dijk et al. An important observation is that to obtain a secure fully homomorphic scheme that supports the encryption of arbitrary messages and the homomorphic evaluation of arbitrary functions on ciphertexts, it is in fact sufficient to construct a scheme to encrypt single-bit messages (either 0 or 1) and evaluate an arbitrary number of XOR and AND logic gates on encryptions of those bits. Indeed, data of any length can be represented as a bit string, and arbitrary functions on such a bit string can be represented as Boolean circuits (consisting of XOR (exclusive OR) and AND gates) on the corresponding bits. By encrypting each bit of the bit string independently and applying the homomorphic evaluation of the XOR and AND gates of the Boolean circuits, we obtain the required fully homomorphic functionality.

In fully homomorphic encryption over the integers, the secret key is a relatively large odd integer p (of about 600 digits, say). Given several multiples $q_i p$ of p, it is easy to recover p by computing the greatest common divisor (GCD). However, recovering p from many *approximate multiples* of the form $q_i p + e_i$ (where e_i is a relatively small 20- to 30-digit *noise* value) is believed to be a hard problem. In fact, if q_i is a large enough random integer (a few million digits),

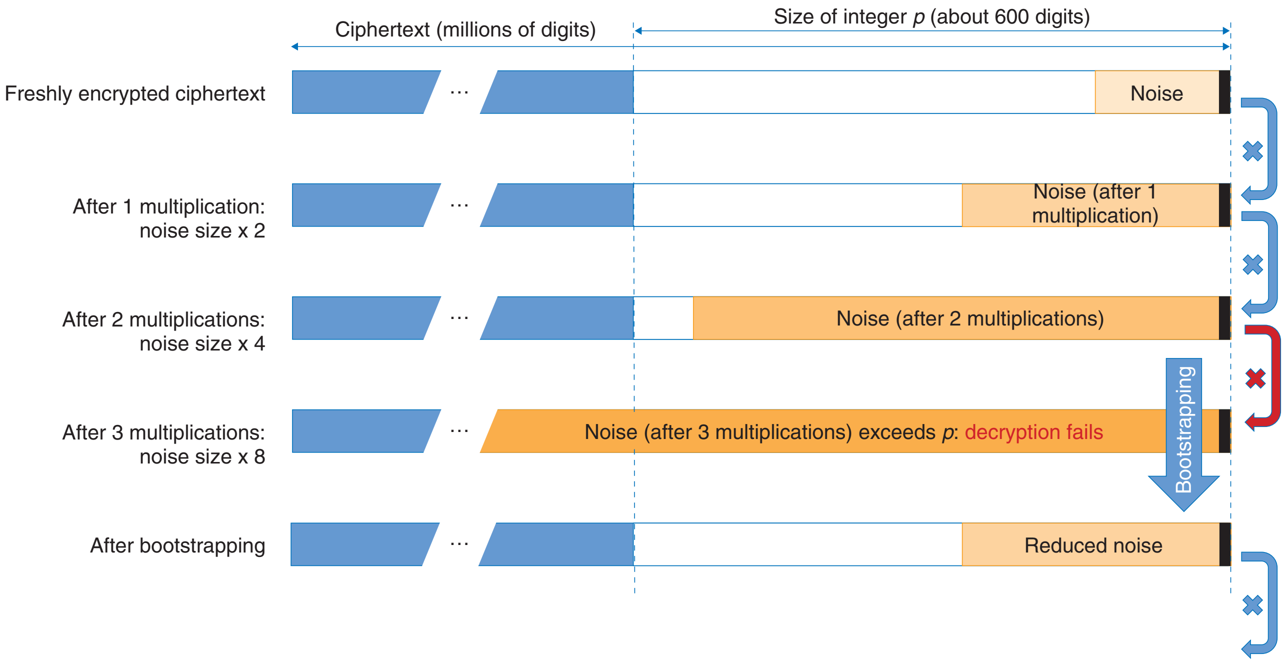

Ciphertext (millions of digits)
Size of integer p (about 600 digits)
Freshly encrypted ciphertext
Noise
After 1 multiplication: noise size x 2
Noise (after 1 multiplication)
After 2 multiplications: noise size x 4
Noise (after 2 multiplications)
After 3 multiplications: noise size x 8
Noise (after 3 multiplications) exceeds p: decryption fails
Bootstrapping
After bootstrapping
Reduced noise

Fig 3. Bootstrapping for fully homomorphic encryption.

the approximate multiple $q_ip + e_i$ is indistinguishable from a random integer of the same size in the view of an attacker who does not know p. As a result, one can encrypt a one-bit message m (0 or 1) by adding to it a large, random multiple $q\,p$ of p (of a few million digits) as well as some *even* random noise $2r$ (of 20 to 30 digits). To an attacker who does not know the secret key p, the resulting ciphertext $c = q\,p + 2r + m$ is then indistinguishable from a random integer of the same size, as discussed above, regardless of whether m is 0 or 1; hence, attackers cannot learn anything about m from the ciphertext c. On the contrary, the legitimate owner of the secret key p can decrypt the ciphertext c by computing the Euclidean division by p and checking the parity of the remainder $2r + m$: it is even if m is 0 and odd if m is 1. Thus, we have described a secure (secret-key) encryption scheme.

Moreover, this encryption scheme supports the homomorphic evaluation of XOR and AND gates. Indeed, consider two single-bit messages m_1 and m_2 and corresponding ciphertexts c_1 and c_2. We claim that the sum $c_1 + c_2$ is an encryption of m_1 XOR m_2. Indeed, $c_1 + c_2 = (q_1 + q_2)p + 2(r_1 + r_2) + (m_1 + m_2)$, and its remainder in the Euclidean division by p is $2(r_1 + r_2) + (m_1 + m_2)$. If $m_1 = m_2$, this is an even number, and hence, $c_1 + c_2$ decrypts to 0. Similarly, if $m_1 \neq m_2$, this is an odd number, and $c_1 + c_2$ decrypts to 1, as required. We can check in much the same way that the product $c_1\,c_2 = (q_1q_2p + 2q_1r_2 + q_1m_2 + 2q_2r_1 + q_2r_1)p + 2(2r_1r_2 + r_1m_2 + r_2m_1) + m_1m_2$ is a valid encryption of m_1 AND m_2.

Unfortunately, the scheme described above is not quite a fully homomorphic encryption scheme yet; it only satisfies the weaker property of being ‘somewhat homomorphic’. The problem is that whenever a homomorphic XOR and especially AND operation is carried out, that noise value within the ciphertext grows (its size roughly doubles with each AND gate). If too many such homomorphic operations are carried out, at some point the noise value becomes larger than p, at which point it becomes impossible to ensure correct decryption anymore (**Fig. 3**). Therefore, the scheme we just described does not support the homomorphic evaluation of arbitrary functions, but only of those functions which, when represented as a Boolean circuit, consist of only a limited number of successive levels of AND gates (hence the name *somewhat* homomorphic encryption). To overcome this problem and enable the homomorphic evaluation of arbitrary functions, it is necessary to devise a procedure to reduce the noise within a ciphertext to some extent. One of the key insights of Gentry’s work is a technique called *bootstrapping* for exactly that purpose. Applying that technique after each AND gate makes it possible to evaluate arbitrary Boolean circuits, and hence, to obtain proper fully homomorphic encryption.

However, the resulting scheme is very inefficient. Even if we consider the somewhat homomorphic scheme, we see that a ciphertext of several million digits is needed to encrypt a single bit; in other words, ciphertexts are millions of times larger than the corresponding plaintexts, and homomorphic operations corresponding to simple XOR and AND gates involve arithmetic on huge integers, requiring both a large amount of memory and lengthy computations. Using bootstrapping to turn the scheme into a fully homomorphic one further reduces the efficiency by a considerable extent. Consequently, something has to be done to approach practical levels of efficiency.

4. Contributions of NTT

Obtaining more practical constructions of fully homomorphic encryption over the integers is one of our research topics at the NTT Secure Platform Laboratories. We face three main challenges that hold back the performance of fully homomorphic encryption over the integers. The first one is ciphertext expansion; as described above, ciphertexts consist of millions of digits for every single message bit. The second one is the overhead of homomorphic evaluation; evaluating an operation as simple as a bitwise AND requires carrying out exact arithmetic on huge integers, which is slow. This problem is further compounded by bootstrapping, which makes each homomorphic operation considerably costlier. The third bottleneck is the size of the public key and of public parameters. So far, we have described a secret key encryption scheme, but many applications such as anonymous data processing require public key encryption. The conversion from secret key to public key for a fully homomorphic scheme can be done in a relatively straightforward manner (it is sufficient to publish a large number of encryptions of 0), but this results in a prohibitively large public key. Moreover, the bootstrapping method requires publishing very large public parameters for homomorphic evaluation, even for secret key schemes.

Until 2012, we mainly tackled the first and third of those problems, and by introducing novel techniques to compress public keys and ciphertexts, as well as a nonlinear optimization of the encryption algorithm, we were able to obtain major efficiency improvements. Public keys and parameters, in particular, went from a size so large that they would barely fit in an entire datacenter, as in the original construction by van Dijk et al., down to only a few megabytes. This increased the speed considerably, as less data had to be processed for homomorphic evaluation, enabling us to obtain a proof of concept implementation executable in reasonable time on an ordinary computer [2].

In 2013, we proposed yet another fully homomorphic encryption scheme over the integers offering dramatic improvements to both ciphertext expansion and homomorphic evaluation overhead at the same time [3]. The key idea was to pack multiple message bits $m_1, \ldots, m_n$ into a single ciphertext in such a way that all of these bits could be processed in parallel during homomorphic evaluation (**Fig. 4**). To do so, we use several odd numbers $p_1, \ldots, p_\mathrm{n}$ as the secret key, and we encrypt the multi-bit message $(m_1, \ldots, m_\mathrm{n})$ as an integer c obtained as a multiple of the product $p_1 \ldots p_\mathrm{n}$ plus some noise chosen in such a way that the remainder of the Euclidean division of c by p_i is of the form $2r_i + m_i$. The Chinese remainder theorem ensures that we can compute such a c, and that the sum and product of two of these ciphertexts respectively encrypt the bitwise XOR and AND of the corresponding multi-bit messages. Putting these many message bits together in a single ciphertext and processing them homomorphically in parallel yield the expected efficiency improvements in terms of ciphertext expansion and homomorphic evaluation complexity. More recently, we proposed a further major improvement by adapting to fully homomorphic encryption over the integers a technique, originally conceived for a different type of schemes, to avoid the use of the expensive bootstrapping method when evaluating arbitrary functions homomorphically [4]. With that technique, homomorphic AND operations only increase the size of ciphertext noise by a small fixed amount instead of doubling it every time. As a result, with a suitable choice of parameters, it becomes possible to evaluate any given Boolean circuit homomorphically and still ensure that the noise size does not exceed the limit of correct decryption, making bootstrapping unnecessary. The new results from 2013 alone enabled us to improve the speed of fully homomorphic encryption of integers by about two orders of magnitude, and to obtain the world's fastest homomorphic evaluation of the AES (Advanced Encryption Standard) block cipher in about 20 seconds per block on a standard personal computer with no compromise on security. This level of performance already makes homomorphic processing of small amounts of data practical and enables us to envision

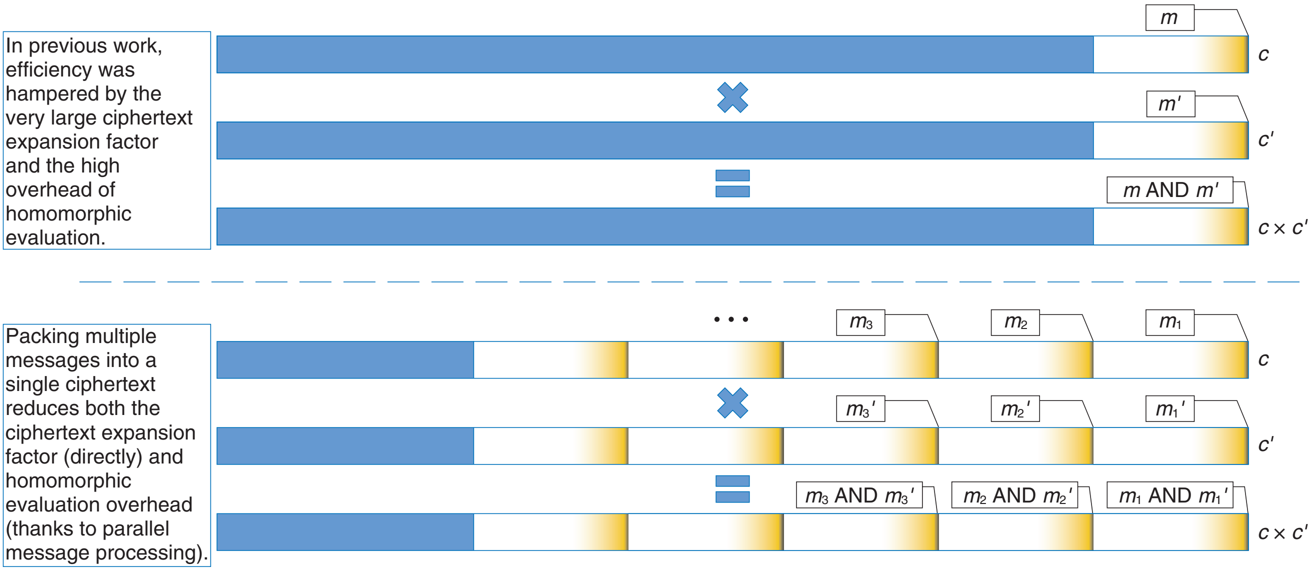

In previous work, efficiency was hampered by the very large ciphertext expansion factor and the high overhead of homomorphic evaluation.
m
c
m'
c'
m AND m'
c × c'
Packing multiple messages into a single ciphertext reduces both the ciphertext expansion factor (directly) and homomorphic evaluation overhead (thanks to parallel message processing).
• • •
m3
m2
m1
c
m3'
m2'
m1'
c'
m3 AND m3'
m2 AND m2'
m1 AND m1'
c × c'

Fig. 4. Batch ciphertexts in fully homomorphic encryption.

more ambitious applications in the near future.

5. Further work

Going forward, we intend to maintain our status as one of the world's top research groups investigating fully homomorphic encryption and to continue to innovate with the goal of achieving still more practical levels of efficiency. Since ciphertext compression techniques and other optimizations that were developed for earlier variants of fully homomorphic encryption over the integers cannot be used with our current best scheme, further efficiency improvements are now mainly hampered by memory requirements. Our first objective is to overcome that problem, so as to make the homomorphic processing of larger amounts of data practical. We will also move forward with research on cryptographic multilinear maps, another cutting-edge cryptographic technique with very important applications, the most prominent of which is certainly general program obfuscation. Multilinear maps share a number of structural similarities with fully homomorphic encryption; this has allowed us to propose a new way of constructing them, as well as the first ever implementation of a multilinear map-based protocol.

References

[1] Cloud Security Alliance, Cloud Vulnerabilities Working Group, "Cloud Computing Vulnerability Incidents: A Statistical Overview," 2013.

[2] J.-S. Coron, D. Naccache, and M. Tibouchi, "Public Key Compression and Modulus Switching for Fully Homomorphic Encryption over the Integers," EUROCRYPT 2012, LNCS 7237, pp. 446–464, 2012.

[3] J. H. Cheon, J.-S. Coron, J. Kim, M. S. Lee, T. Lepoint, M. Tibouchi, and A. Yun, "Batch Fully Homomorphic Encryption over the Integers," EUROCRYPT 2013, LNCS 7881, pp. 315–335, 2013.

[4] J.-S. Coron, T. Lepoint, and M. Tibouchi: "Scale-invariant Fully Homomorphic Encryption over the Integers," PKC 2014, LNCS 8383, pp. 311–328, 2014.

Mehdi Tibouchi
Researcher, Okamoto Research Laboratory, NTT Secure Platform Laboratories.

He is an alumnus of École normale supérieure in Paris, France and received a Ph.D. in computer science from the University of Paris VII and the University of Luxembourg in 2011. He joined the NTT Secure Platform Laboratories thereafter. His research interests include the design and analysis of public-key cryptographic schemes, with a particular view towards new feature-rich primitives. He is a member of the International Association for Cryptologic Research (IACR) and the European Association for Theoretical Computer Science (EATCS).

Understanding the Coordination Mechanisms of Gaze and Arm Movements

Naotoshi Abekawa and Hiroaki Gomi

Abstract

We report on the coordination mechanisms of gaze and arm movements in the visuomotor control process. The brain information-processing mechanisms underlying the eyes, arms, and their coordinated movements need to be understood in order to design sophisticated and user-friendly interactive human-machine interfaces. In this article, we first review the experimental research on visuomotor control, primarily from the viewpoints of eye-hand coordination and online feedback control. Then, we introduce our recent experimental studies investigating the eye-hand coordination mechanism during online feedback control. The experimental results provide evidence that reaching corrections that are rapidly and automatically induced by visual perturbations are influenced by changes in gaze direction. These results suggest that an online reach controller closely interacts with gaze systems.

Keywords: visuomotor control, eye-hand coordination, online feedback control

1. Introduction

We can make arm movements to grasp a cup, manipulate a computer with a mouse, or hit a moving fastball. These motor functions are achieved entirely by our brain's information processing system. Gaining a deep understanding of the brain mechanisms of human motor behaviors is fundamental in order to design user-friendly interactive human-machine interfaces using future information technologies.

Humans perform various visually guided actions in daily life. To perform movements that involve reaching the arm toward a visual target, we have to look at the target and then detect its location relative to the hand. In this situation, gaze behavior should be coordinated with hand movements in a spatiotemporally appropriate manner. Furthermore, visual information that falls on the retina is integrated with other sensory information related to gaze direction, head orientation, or hand location, so as to be transformed into desired muscle contractions. These cooperative aspects of gaze and hand systems are referred to as *eye-hand coordination* (discussed in detail in section 2.1).

In addition to eye-hand coordination, one important aspect of our daily actions is dynamic interaction with the external world. Consider playing tennis as an example. Tennis players have to run and hit the ball even though its flying trajectory irregularly changes. In this *dynamic* situation, the players must correct their reaching trajectory as quickly as possible in response to unpredictable perturbations such as a sudden shift of the target or body movement. The reaching correction of movement midflight is mediated by an online feedback controller (discussed in detail in section 2.2).

Based on the fact that the hand and eye always move cooperatively in our daily lives [1], both motor systems seem to be tightly coupled with each other during online feedback control. However, until now this issue had not been sufficiently addressed in related research fields despite its importance. In this article, we review recent studies on eye-hand coordination and online feedback control in section 2. In section 3, we introduce our experimental studies on eye-hand coordination during online feedback control. We conclude the article in section 4.

2. Background

2.1 Eye-hand coordination

We discuss eye-hand coordination in terms of two aspects. The first aspect is the spatiotemporal coordination of gaze and reaching behaviors. These behaviors were observed in an experimental task where participants looked at and reached toward a designated target. The arm movements in such a task are typically preceded by a rapid movement of the eye to the target, called a saccade. Saccadic eye movement before the hand reaction can provide some crucial information on the hand motor system, for example, visual information, target representation, or motor commands [2]. Indeed, several studies have found that eye movements affect concurrent hand movements such as reaction time, initial acceleration, or final position [3]–[6]. In addition, saccades and hand reaction times are temporally correlated with each other, suggesting that both motor systems share a common neural processing [7], [8]. Meanwhile, it is known that arm-reaching movements can also affect gaze systems. The reaction time of a saccade differs between when it was made with an arm-reaching movement and when it was made without such a movement [9], [10]. In addition to this temporal effect, arm-reaching movement affects the landing point of each saccade, while saccades track unseen arm-reaching movements from the participant [11]. These findings suggest that the hand and eye motor systems interact with each other in visually guided reaching actions.

The second point regarding eye-hand coordination is coordinate transformation from visual to body space. When making an arm-reaching movement, the brain should code the locations of both the target and the hand in a common frame of reference so as to compute the difference vector from the hand to the target. The classical ideas on this topic suggest that body-centered coordinates are utilized for this common reference frame [12], [13]. That is, visual information about the target location on the retina is transformed into body-centered coordinates by integrating the target location on the retina with the eye orientation in the orbit, the head rotation relative to the shoulder, and the arm posture. However, more recent behavioral, imaging, and neurophysiological studies have revealed that the locations of the target and hand are represented in a gaze-centered frame of reference, and the posterior parietal cortex (PPC) is involved in constructing this representation [14]–[17]. The difference vector between hand and target is also computed using this gaze-centered representation [18]. The gaze-centered representation of the target and hand should be updated quickly depending on each eye movement, and this updating process is called *spatial remapping*. This spatial remapping was found to occur predictively before the actual eye movement using oculomotor preparatory signals [19].

2.2 Online feedback control

Online feedback control in visuomotor processing has been investigated using a visual perturbation paradigm since the 1980s [20]–[22]. In this experimental paradigm, the location of the reaching target changed unexpectedly during a reaching movement. The results showed that participants can adjust their reaching trajectories rapidly and smoothly in response to such shifting targets. Interestingly, the reaction latency of this online correction is 120–150 ms after the target shift, which is much quicker compared to that for voluntary motor reactions to a static visual target (more than 150–200 ms) [23]. Furthermore, this correction can be initiated even when the participant is not aware of the target shift [24]. These results suggest that the online reaching correction to the target shift is mediated by reflexive mechanisms that differ from the mechanism underlying the voluntary motor reaction to a static visual target [25]. Patient [26], [27], transcranial magnetic stimulation [28], and imaging [29], [30] studies have found that the PPC plays a significant role in producing this rapid and reflexive online reaching correction.

As mentioned in the Introduction, we have to respond not only to external changes (i.e., target shifts) but also to our own body movements. When such body movements occur, the eyes on the head frequently receive background visual motion that is opposite that of the body movement. This can be easily understood if we consider a hand-held video camera. Since our hands usually shake during recording, the visual image on the screen of the camera moves in the opposite direction from our hand movements. This fact suggests that visual motion can be utilized to control reaching movements against the body movement. Indeed, this theory is supported by several studies [31]—[34]. In these studies, a large-field visual motion was presented on a screen during a reaching movement. The results showed that the reaching trajectory shifted rapidly (100–150 ms) and unintentionally toward the direction of visual motion. This is known as a *manual following response* (MFR).

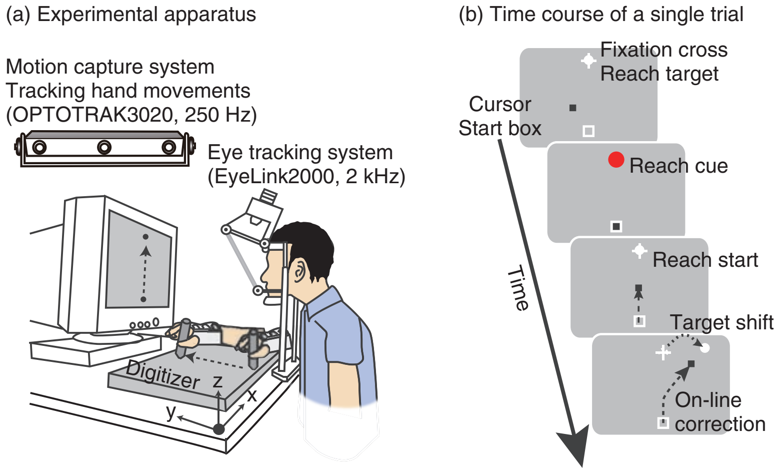


Fig. 1. Experimental paradigm in first study.

Several studies have shown the functional significance of the MFR by observing the reaching accuracy when visual motion and actual perturbations to the participants' posture were introduced simultaneously [32], [35]. The computational and physiological mechanisms underlying the MFR have not yet been fully elucidated; however, it is thought that some cortical areas related to visual motion processing such as the middle temporal or the medial superior temporal areas contribute to generating the MFR [36].

3. Eye-hand coordination in online feedback control

Although eye-hand coordination has been examined widely as described in the previous section, the experimental task used in those studies was restricted to a reaching movement from a static posture toward a stationary target. Therefore, the previous studies focused mainly on the coordination mechanism during the motor planning process. However, during the execution of reaching, it is necessary to correct reaching trajectories rapidly in response to unexpected perturbations. Visually guided online corrections would be mediated by the reflexive mechanism described in section 2.2. In this section, we describe our recent experimental studies, which focused on the eye-hand coordination mechanism during online visuomotor control.

3.1 Eye movements and reaching corrections with a target shift

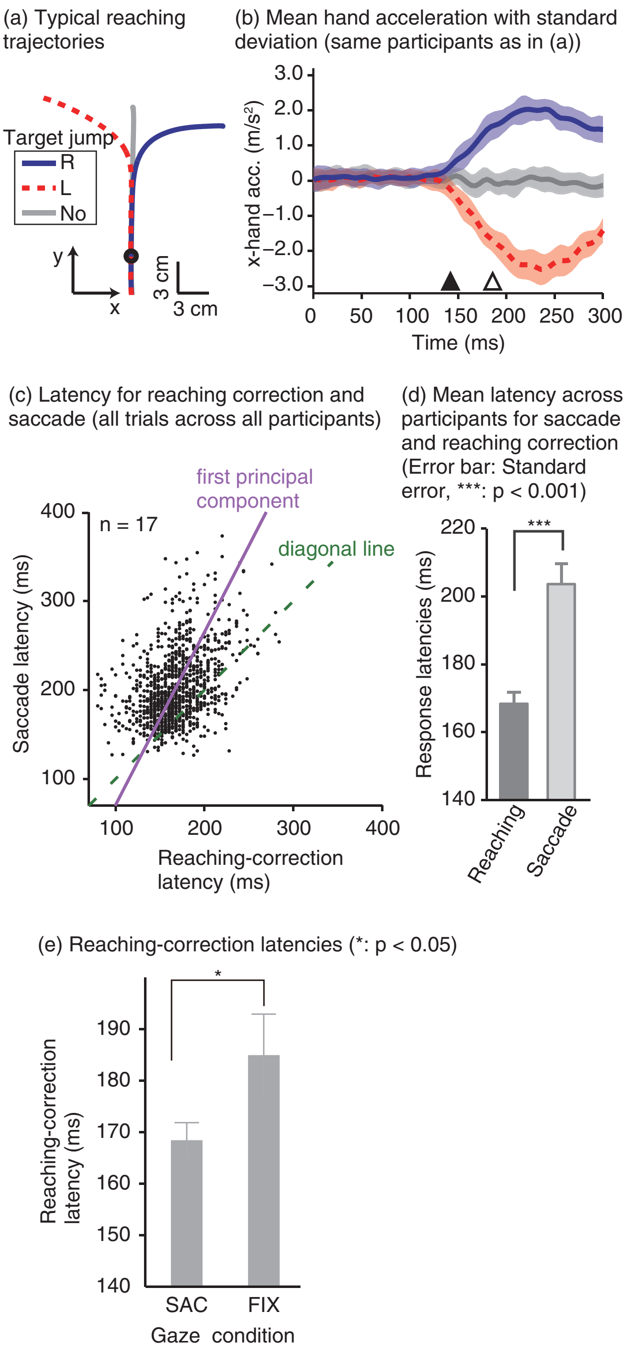
We observed eye movements and online reaching correction when a target was shifted during the reaching movement [37]. The experimental apparatus is shown in **Fig. 1(a)**. Participants (n = 17) made a reaching movement in a forward direction on a digitizer while holding a stylus pen. The pen location was presented on the monitor as a black cursor. At the start of each trial, participants placed the cursor into the start box (a square at the bottom of the monitor) while maintaining eye fixation on the central fixation cross (**Fig. 1(b)**). Then, a reaching target was presented over the fixation cross, cuing participants to initiate reaching (distance: 22 cm, duration: 0.6 s). In randomly selected trials, the target shifted 7.6 cm rightward (32/96 trials) or leftward (32 trials) 100 ms after the reaching initiation. In target-jump trials, participants were required to make smooth online reaching corrections to the new target location as quickly as possible. In the remaining 32 trials, the target was kept stationary, and participants continued to reach toward the original target location.

To examine the effect of gaze behavior on the reaching correction, we conducted this reaching task under two gaze conditions: saccade (SAC) or fixation (FIX). In the SAC condition, participants had to make the reaching correction with a saccadic eye movement to the new target location, whereas in the FIX condition, participants made the reaching correction while maintaining eye fixation on the central fixation cross (i.e., the original target location). Each gaze condition was run in separate blocks of 48 trials.

Reaching trajectories obtained by a typical participant in the SAC condition are shown in **Fig. 2(a)**. The trajectory deviated smoothly during a reach according to the direction of the target shift. To evaluate the initiation of the reaching correction in more detail, we calculated x-hand accelerations (the axis along the target shift), which are temporally aligned at the onset of the target shift (**Fig. 2(b)**). The hand response corresponding to each direction of the target shift rapidly deviated about 150 ms after the target shift. The response latency of the reaching correction and saccade is indicated by a filled (143 ms) and open triangle (187 ms), respectively. This temporal relationship (reaching correction that preceded saccade initiation) was obtained for all the participants. Hand and eye latencies for all trials across all participants are plotted in **Fig. 2(c)**. Most of the data (81.6%) fell above the diagonal line, indicating that the reaching correction was usually initiated prior to the onset of the eye movement. This temporal difference was statistically significant in a paired t-test ($p < 0.001$), as shown in **Fig. 2(d)**.

The hand-first and eye-second pattern observed in this study indicates that the online reaching correction can be initiated by peripheral visual information before the eye movement. This temporal order differs completely from that reported in conventional eye-hand tasks. The eye-first and hand-second pattern in the conventional task indicates that the reaches initiated from a static posture rely on the central visual information. A recent imaging study has shown that compared with central reaching, peripheral reaching involved an extensive cortical network including the PPC [38]. Thus, these findings again support the idea that distinct brain mechanisms are involved between motor planning for the voluntary reaching initiation and online feedback control during the motor execution.

We next investigated the dependence of the reaching correction on saccadic eye movements. Firstly, we observed that the initiation of the reaching correction was temporally correlated with saccade onset (correlation coefficient = 0.39, $p < 0.001$, Fig. 2(c)). Correlation was significant ($p < 0.05$) in 13 and marginally significant ($p < 0.1$) in 1 out of 17 participants. Secondly, we found that the latency of the reaching correction changed according to the gaze conditions. The reaching correction was significantly ($p < 0.05$) faster for the SAC than for the FIX condition, as shown in **Fig. 2(e)**.


(a) Typical reaching trajectories

(b) Mean hand acceleration with standard deviation (same participants as in (a))

(c) Latency for reaching correction and saccade (all trials across all participants)

(d) Mean latency across participants for saccade and reaching correction (Error bar: Standard error, ***: $p < 0.001$)

(e) Reaching-correction latencies (*: $p < 0.05$)

Fig. 2. Results of first study.

The correlation finding indicates that the hand and eye control systems do not act independently; rather, they share common processing at some stage. Furthermore, the dependence of the reaching correction on the gaze condition suggests that the hand and eye motor system interacts closely even during the online feedback control. Since a saccade was not yet initiated when the reaching correction started, the change in hand latency cannot be ascribed to any changes in visual or oculomotor signals obtained after the actual eye movements. Our findings imply that an online reaching controller interacts with oculomotor

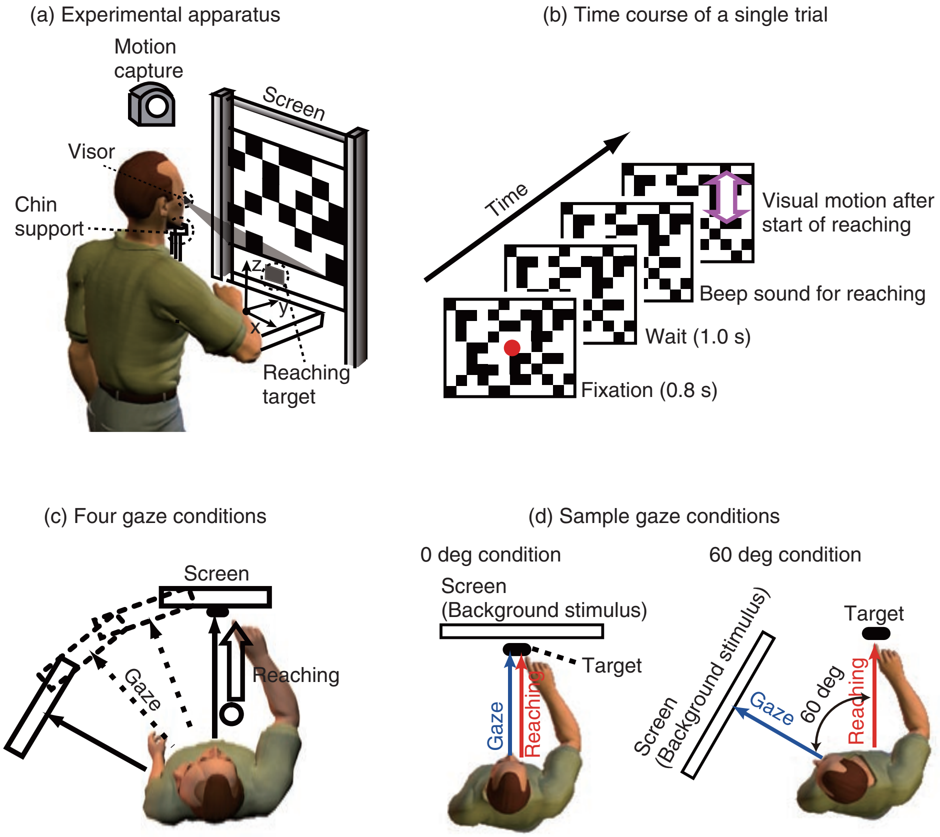


Fig. 3. Experimental paradigm in second study.

preparation signals before the actual eye movements.

3.2 Gaze direction and reaching corrections to background visual motion

This study focused on reaching corrections induced by visual motion (MFR). In this case, visual motion that was applied during the reaching did not induce explicit eye movements. Thus, to address the mechanism of eye-hand coordination, we examined the effect of gaze direction on MFR [39]. Gaze direction relative to the reaching target is known to be a key feature in constructing gaze-centered spatial representation, as described in section 2.1.

The experimental apparatus is shown in **Fig. 3(a)**. Participants (n = 6) were seated on a chair in front of a back-projection screen. The participants were asked to make a reaching movement in a forward direction (distance of about 39 cm) toward a 1 cm^2 piece of rubber. The target and the participant's hand were completely occluded from view. The time course of a single trial is shown in **Fig. 3(b)**. At the start of each trial, participants touched the target location to confirm its location. Then, participants pressed a button followed by the presentation of a stationary random checkerboard pattern and a fixation marker. After the eye fixation marker was presented, beep sounds were made to cue participants to initiate a reaching movement while maintaining the eye fixation. In randomly selected trials, a background visual stimulus moved upward (16/48 trials) or downward (16 trials) for 500 ms shortly after the reaching initiation. In the remaining 16 trials, the visual stimulus was kept stationary. Participants were asked to reach toward the target location regardless of whether or not the visual motion was presented.

Participants performed this reaching task under four gaze-reaching configurations (0, 20, 40, and 60°), as shown in **Fig. 3(c)**. In the 0° condition (left panel in **Fig. 3(d)**), the head was oriented straight ahead, and the screen was located in front of the participants. In this condition, the gaze direction matched the target location. In the 60° condition (right panel in **Fig. 3(d)**), the head was rotated 60° to the left, and the

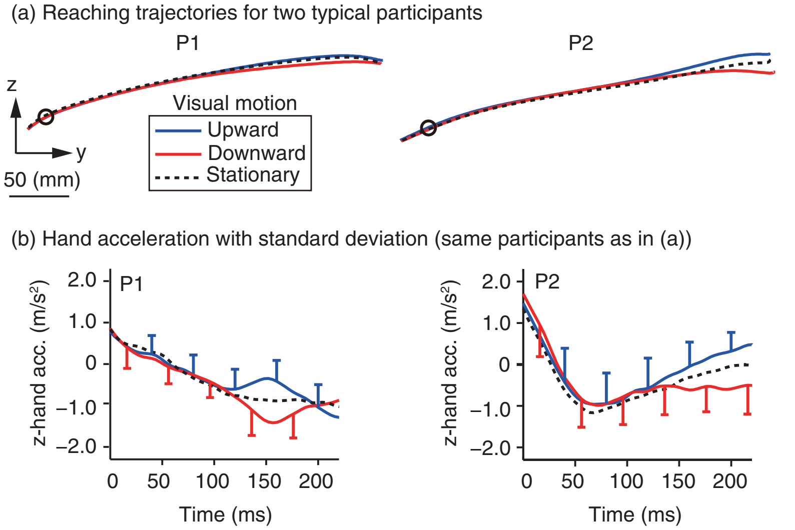


Fig. 4. Results of second study.

screen location changed so that the visual stimuli on it were presented to participants in the same way in the four gaze conditions. In this condition, the gaze direction was away from the reaching target. Thus, in the 20° and 40° conditions, the rotation angle was 20° and 40°, respectively. In all the conditions, participants made the same reaching movements toward the identical target location. Therefore, this paradigm allows us to examine the effect of gaze-reach coordination on the online manual response to the visual motion.

Typical reaching trajectories in the 0° condition (two participants: P1 and P2) are shown in **Fig. 4(a)**. When the background visual stimulus moved during a reaching movement, the reaching trajectory deviated in the direction of visual motion (blue line for upward and red line for downward). This reflexive MFR was observed in all participants. To analyze the response in more detail, we calculated the hand accelerations (acc.) along a z-axis (the direction of visual motion) that were temporally aligned at the onset of visual motion (**Fig. 4(b)** with the same participants as in Fig. 4(a)). We obtained the difference in the hand acceleration between the upward and downward visual motions. This temporal difference for the 0° and 60° conditions is shown in **Fig. 5(a)** (data for P1). Interestingly, the manual response was larger for the 0° condition than for the 60° condition even though the identical visual motion was applied in both conditions. We quantified the response amplitude by estimating the mean response between 100 and 200 ms after the onset of visual motion (black solid line in Fig. 5(a)). A comparison of the response amplitudes averaged across participants for all gaze conditions (0, 20, 40, and 60°) is given in **Fig. 5(b)**. The MFR was largest for the 0° condition, and the response amplitude significantly decreased as the gaze direction deviated from the reaching target (ANOVA (analysis of variance), $p < 0.05$).

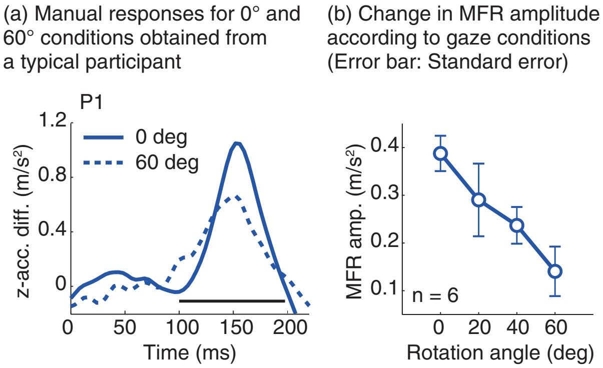


Fig. 5. MFR modulation.

These results indicate that the automatic manual response induced by visual motion is modulated flexibly by the spatial relationship between gaze and reaching target. This spatial relationship is computed by the gaze-centered target representation, which is constructed in the PPC during reach planning. The MFR gain modulation that is based on the gaze-reach coordination can be associated with our natural behavior, namely, that we usually gaze at the reach target when highly accurate reaching is required. Thus, we infer that visuomotor gain for the online reaching correction is functionally modulated by the gaze-reach coordination.

4. Conclusion

We investigated mechanisms of eye-hand coordination during online visual feedback control. When a target shift or background visual motion is applied during reaching, rapid and reflexive online corrections can occur. Our studies provide experimental evidence that the online controller for arm reaching interacts closely with gaze systems.

The first study showed that the reaching correction to the target shift was temporally correlated with saccade onset and changed according to the gaze behavior that started after the initiation of reach correction. This suggests that an online reaching controller interacts with gaze signals related to planning eye movements. The second study revealed that the amplitude of the reaching correction to the visual motion changed according to the spatial relationship between gaze and the reach target. This suggests that the visuomotor gain for the reflexive online controller is functionally modulated by the eye-hand coordination.

Eye-hand coordination is a basic aspect of visually guided motor actions that occur frequently in our daily lives. In addition, quick online motor corrections are one of the bases supporting our skillful motor actions in *dynamic* environments. Thus, we believe that understanding the brain mechanisms underlying these visuomotor functions will provide important guidelines on how to develop user-friendly human-machine interfaces in the near future.

References

[1] M. F. Land and B. W. Tatler, Looking and Acting: Vision and Eye Movements in Natural Behaviour. Oxford; New York: Oxford University Press, 2009.
[2] H. Bekkering and U. Sailer, “Commentary: Coordination of Eye and Hand in Time and Space,” Prog. Brain Res., Vol. 140, pp. 365–373, 2002.
[3] P. van Donkelaar, “Eye-hand Interactions during Goal-directed Pointing Movements,” Neuroreport, Vol. 8, No. 9–10, pp. 2139–2142, Jul. 1997.
[4] P. van Donkelaar, “Saccade Amplitude Influences Pointing Movement Kinematics,” Neuroreport, Vol. 9, No. 9, pp. 2015–2018, Jun. 1998.
[5] G. Binsted and D. Elliott, “Ocular Perturbations and Retinal/Extraretinal Information: the Coordination of Saccadic and Manual Movements,” Exp. Brain Res., Vol. 127, No. 2, pp. 193–206, Jul. 1999.
[6] J. F. Soechting, K. C. Engel, and M. Flanders, “The Duncker Illusion and Eye-hand Coordination,” J. Neurophysiol., Vol. 85, No. 2, pp. 843–854, Feb. 2001.
[7] U. Sailer, T. Eggert, J. Ditterich, and A. Straube, “Spatial and Temporal Aspects of Eye-hand Coordination Across Different Tasks,” Exp. Brain Res., Vol. 134, No. 2, pp. 163–173, Sep. 2000.
[8] H. L. Dean, D. Martí, E. Tsui, J. Rinzel, and B. Pesaran, “Reaction Time Correlations during Eye-hand Coordination: Behavior and Modeling,” J. Neurosci., Vol. 31, No. 7, pp. 2399–2412, Feb. 2011.
[9] L. Lünenburger, D. F. Kutz, and K. P. Hoffmann, “Influence of Arm Movements on Saccades in Humans,” Eur. J. Neurosci., Vol. 12, No. 11, pp. 4107–4116, Nov. 2000.
[10] S. F. Neggers and H. Bekkering, “Ocular Gaze is Anchored to the Target of an Ongoing Pointing Movement,” J. Neurophysiol., Vol. 83, No. 2, pp. 639–651, Feb. 2000.
[11] G. Ariff, O. Donchin, T. Nanayakkara, and R. Shadmehr, “A Real-time State Predictor in Motor Control: Study of Saccadic Eye Movements during Unseen Reaching Movements,” J. Neurosci., Vol. 22, No. 17, pp. 7721–7729, Sep. 2002.
[12] M. Flanders, S. I. H. Tillery, and J. F. Soechting, “Early Stages in a Sensorimotor Transformation,” Behav. Brain Sci., Vol. 15, No. 02, pp. 309–320, 1992.
[13] J. McIntyre, F. Stratta, and F. Lacquaniti, “Viewer-centered Frame of Reference for Pointing to Memorized Targets in Three-dimensional Space,” J. Neurophysiol., Vol. 78, No. 3, pp. 1601–1618, Sep. 1997.
[14] D. Y. Henriques, E. M. Klier, M. A. Smith, D. Lowy, and J. D. Crawford, “Gaze-centered Remapping of Remembered Visual Space in an Open-loop Pointing Task,” J. Neurosci., Vol. 18, No. 4, pp. 1583–1594, Feb. 1998.
[15] W. P. Medendorp and J. D. Crawford, “Visuospatial Updating of Reaching Targets in Near and Far Space,” Neuroreport, Vol. 13, No. 5, pp. 633–636, Apr. 2002.
[16] W. P. Medendorp, H. C. Goltz, T. Vilis, and J. D. Crawford, “Gaze-centered Updating of Visual Space in Human Parietal Cortex,” J. Neurosci., Vol. 23, No. 15, pp. 6209–6214, Jul. 2003.
[17] A. P. Batista, C. A. Buneo, L. H. Snyder, and R. A. Andersen, “Reach Plans in Eye-centered Coordinates,” Science, Vol. 285, No. 5425, pp. 257–260, Jul. 1999.
[18] C. A. Buneo, M. R. Jarvis, A. P. Batista, and R. A. Andersen, “Direct Visuomotor Transformations for Reaching,” Nature, Vol. 416, No. 6881, pp. 632–636, Apr. 2002.
[19] J. R. Duhamel, C. L. Colby, and M. E. Goldberg, “The Updating of the Representation of Visual Space in Parietal Cortex by Intended Eye Movements,” Science, Vol. 255, No. 5040, pp. 90–92, Jan. 1992.
[20] M. A. Goodale, D. Pelisson, and C. Prablanc, “Large Adjustments in Visually Guided Reaching Do Not Depend on Vision of the Hand or Perception of Target Displacement,” Nature, Vol. 320, No. 6064, pp. 748–750, Apr. 1986.
[21] D. Pélisson, C. Prablanc, M. A. Goodale, and M. Jeannerod, “Visual Control of Reaching Movements without Vision of the Limb. II. Evidence of Fast Unconscious Processes Correcting the Trajectory of the Hand to the Final Position of a Double-step Stimulus,” Exp. Brain Res., Vol. 62, No. 2, pp. 303–311, 1986.
[22] C. Prablanc and O. Martin, “Automatic Control during Hand Reaching at Undetected Two-dimensional Target Displacements,” J. Neurophysiol., Vol. 67, No. 2, pp. 455–469, Feb. 1992.
[23] B. L. Day and I. N. Lyon, “Voluntary Modification of Automatic Arm Movements Evoked by Motion of a Visual Target,” Exp. Brain Res., Vol. 130, No. 2, pp. 159–168, Jan. 2000.
[24] V. Gritsenko, S. Yakovenko, and J. F. Kalaska, “Integration of Predictive Feedforward and Sensory Feedback Signals for Online Control of Visually Guided Movement,” J. Neurophysiol., Vol. 102, No. 2, pp. 914–930, Aug. 2009.
[25] H. Gomi, “Implicit Online Corrections of Reaching Movements,” Curr. Opin. Neurobiol., Vol. 18, No. 6, pp. 558–564, Dec. 2008.
[26] L. Pisella, H. Gréa, C. Tilikete, A. Vighetto, M. Desmurget, G. Rode, D. Boisson, and Y. Rossetti, “An ‘Automatic Pilot’ for the Hand in Human Posterior Parietal Cortex: Toward Reinterpreting Optic Ataxia,” Nat. Neurosci., Vol. 3, No. 7, pp. 729–736, Jul. 2000.
[27] H. Gréa, L. Pisella, Y. Rossetti, M. Desmurget, C. Tilikete, S. Grafton,

C. Prablanc, and A. Vighetto, “A Lesion of the Posterior Parietal Cortex Disrupts On-line Adjustments during Aiming Movements,” Neuropsychologia, Vol. 40, No. 13, pp. 2471–2480, 2002.
[28] M. Desmurget, C. M. Epstein, R. S. Turner, C. Prablanc, G. E. Alexander, and S. T. Grafton, “Role of the Posterior Parietal Cortex in Updating Reaching Movements to a Visual Target,” Nat. Neurosci., Vol. 2, No. 6, pp. 563–567, Jun. 1999.
[29] M. Desmurget, H. Gréa, J. S. Grethe, C. Prablanc, G. E. Alexander, and S. T. Grafton, “Functional Anatomy of Nonvisual Feedback Loops during Reaching: A Positron Emission Tomography Study,” J. Neurosci., Vol. 21, No. 8, pp. 2919–2928, Apr. 2001.
[30] A. Reichenbach, J.-P. Bresciani, A. Peer, H. H. Bülthoff, and A. Thielscher, “Contributions of the PPC to Online Control of Visually Guided Reaching Movements Assessed with fMRI-guided TMS,” Cereb. Cortex N. Y. N 1991, Vol. 21, No. 7, pp. 1602–1612, Jul. 2011.
[31] E. Brenner and J. B. J. Smeets, “Fast Responses of the Human Hand to Changes in Target Position,” J. Mot. Behav., Vol. 29, No. 4, pp. 297–310, Dec. 1997.
[32] D. Whitney, D. A. Westwood, and M. A. Goodale, “The Influence of Visual Motion on Fast Reaching Movements to a Stationary Object,” Nature, Vol. 423, No. 6942, pp. 869–873, Jun. 2003.
[33] N. Saijo, I. Murakami, S. Nishida, and H. Gomi, “Large-field Visual Motion Directly Induces an Involuntary Rapid Manual Following Response,” J. Neurosci., Vol. 25, No. 20, pp. 4941–4951, May 2005.
[34] H. Gomi, N. Abekawa, and S. Nishida, “Spatiotemporal Tuning of Rapid Interactions between Visual-motion Analysis and Reaching Movement,” J. Neurosci., Vol. 26, No. 20, pp. 5301–5308, May 2006.
[35] H. Gomi, K. Kadota, and N. Abekawa, “Dynamic Reaching Adjustment during Continuous Body Perturbation is Markedly Improved by Visual Motion,” Soc. Neurosci. 40th Annu. Meet., 2010.
[36] A. Takemura, N. Abekawa, K. Kawano, and H. Gomi, “Short-latency Manual Responses of Monkey are Impaired by Lesions in the MST,” Soc. Neurosci. 38th Annu. Meet., 2008.
[37] N. Abekawa, T. Inui, and H. Gomi, “Eye-hand Coordination in Online Visuomotor Adjustments,” Neuroreport, Vol. 25, No. 7, pp. 441–445, May 2014.
[38] J. Prado, S. Clavagnier, H. Otzenberger, C. Scheiber, H. Kennedy, and M.-T. Perenin, “Two Cortical Systems for Reaching in Central and Peripheral Vision,” Neuron, Vol. 48, No. 5, pp. 849–858, Dec. 2005.
[39] N. Abekawa and H. Gomi, “Spatial Coincidence of Intentional Actions Modulates an Implicit Visuomotor Control,” J. Neurophysiol., Vol. 103, No. 5, pp. 2717–2727, May 2010.

Naotoshi Abekawa

Research Scientist, Human and Information Science Laboratory, NTT Communication Science Laboratories.

He received the B.E. from Tokyo Metropolitan University in 2003, the M.E. from Tokyo Institute of Technology in 2005, and the Ph.D. from Kyoto University in 2013. He joined NTT in 2005 and has been engaged in research on human information processing. His research interests include human sensorimotor mechanisms, especially visuomotor control properties. He is a member of the Society for Neuroscience, the Japan Neuroscience Society, and the Japanese Neural Network Society.

Hiroaki Gomi

Distinguished Senior Research Scientist, Group Leader of Sensory and Motor Research Group, NTT Communication Science Laboratories.

He received the B.E., M.E., and Ph.D. in mechanical engineering from Waseda University, Tokyo, in 1986, 1988, and 1994, respectively. He conducted research on computational biological motor control at ATR (Advanced Telecommunication Research Labs., Kyoto) from 1989 to 1994, in two JST-CREST projects from 1996 to 2003, and in a JST-ERATO project from 2005 to 2010. He was an adjunct professor at Tokyo Institute of Technology from 2000 to 2004. His current research interests include human sensorimotor control mechanisms and interactions between perception and action.

Multiband Antenna Employing Multiple Metamaterial Reflectors

Hideya So, Atsuya Ando, and Takatoshi Sugiyama

Abstract

NTT Access Network Service Systems Laboratories has proposed and developed a multiband sector antenna for mobile wireless communication systems employing multiple metamaterial reflectors and a multiband radiator that is suitable for areas with limited space. We present in this article a design for a triple-frequency-band antenna that radiates at 800-MHz, 2-GHz, and 4-GHz bands as an example of the proposed antenna.

Keywords: multiband antenna, metamaterial, wireless communication

1. Introduction

Mobile wireless communication systems must now offer higher bit rates because of the increasingly widespread use of smartphones and tablet terminals. Mobile wireless communication systems such as cellular networks commonly utilize multiple frequency bands to achieve high system capacity. In addition, cellular systems use a sector configuration to improve frequency efficiency [1].

A conventional sector antenna is shown in **Fig. 1**. It has a radiator and metal reflector for each frequency band used in mobile wireless communication systems. As these systems begin handling more frequency bands, it is expected that the increased number of antennas and the larger space needed for these systems will become a problem.

2. Multiband sector antenna employing multiple metamaterial reflectors

NTT Access Network Service Systems Laboratories is developing a small-volume multiband sector antenna employing multiple metamaterial reflectors. Metamaterial reflectors have a periodic structure and consist of dielectric rods. They also have electromagnetic band gap (EBG) characteristics, meaning that they can reflect/transmit electromagnetic waves according to the frequency band [2]. The EBG characteristics enable the reflectors to act as a band-stop filter or a band-pass filter.

The concept of the proposed N-band sector antenna employing N metamaterial reflectors and a multiband radiator is shown in **Fig. 2(a)**. The center frequency of the desired frequency band is defined as f_n ($f_1 > f_2 > \ldots > f_N$). Metamaterial reflector #n reflects the electromagnetic waves of f_n similarly to the way a metal reflector does. On the other hand, metamaterial reflector #n transmits the electromagnetic waves of

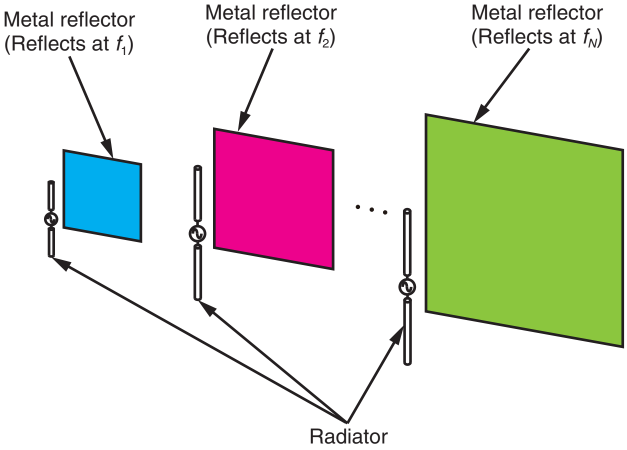
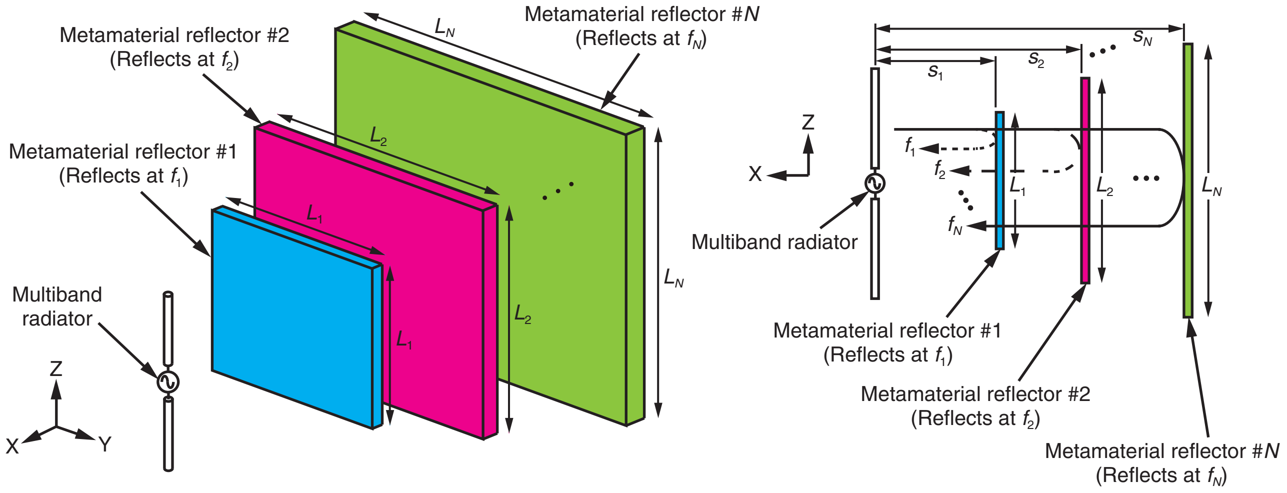

Metal reflector (Reflects at f_1)
Metal reflector (Reflects at f_2)
Metal reflector (Reflects at f_N)
. . .
Radiator

Fig. 1. Conventional sector antenna.



(a) Perspective view

(b) Side view

Fig. 2. Concept of multiband sector antenna employing multiple metamaterial reflectors.

specific frequency bands ($f_{n+1}, f_{n+2}, \dots, f_N, N > n$) as if the reflector was transparent. Each metamaterial reflector reflects/transmits different frequency bands, so the proposed antenna can radiate multiple frequency bands in an area with a small footprint.

The reflectors are square, and their side lengths are indicated by L_n. The distance between the multiband radiator and the front surface of each metamaterial reflector is s_n, as shown in **Fig. 2(b)**. Metamaterial reflector #*N*, which is furthest from the multiband radiator, can be implemented as a metal reflector in the proposed antenna.

The proposed concept yields better design prospects than those of other design concepts because when the reflected frequency bands change or the number of frequency bands increases, we only need to change the EBG bands or increase the number of metamaterial reflectors in the proposed antenna to adapt to the situation.

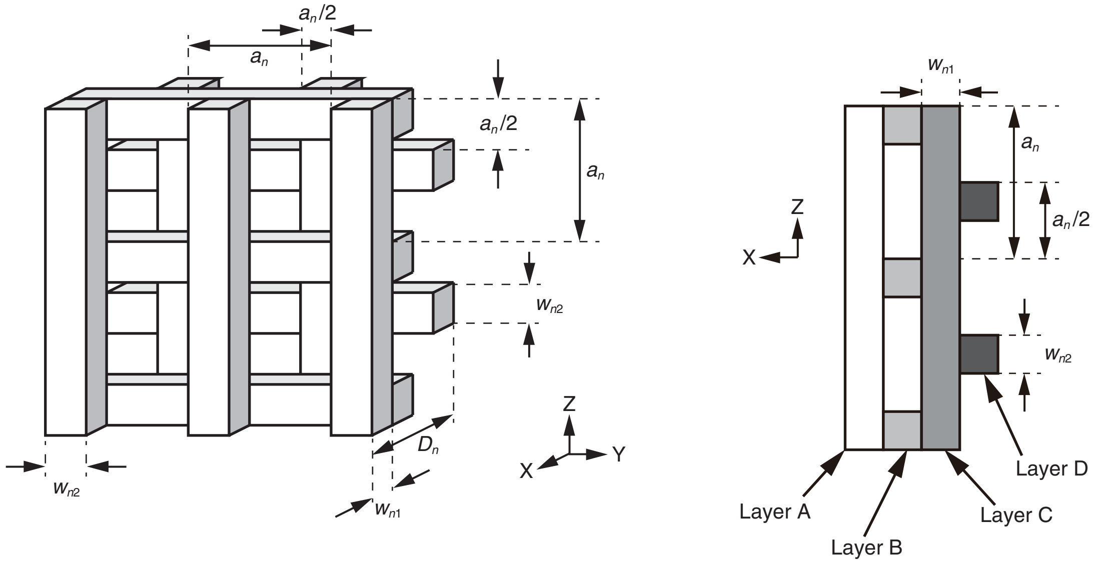
3. Woodpile metamaterial

We applied woodpile metamaterial [3] to the reflectors of the proposed multiband sector antenna. The woodpile metamaterial structure consists of layers of dielectric rods and is illustrated in **Fig. 3**. The rods have a base of $w_{n1} \times w_{n2}$, where w_{n1} is the rod depth along the X-axis, and w_{n2} is the rod width along the Y- and Z-axes. Layer B (D) is at right angles to layer A (C) in space, and the woodpile metamaterial consists of four layers of rods. The spacing between rods in each layer is indicated by a_n. The rods in layer C (D) are set to the spacing of half of a_n from the rods of layer A (B).

4. Triple-frequency-band antenna

We fabricated a triple-frequency-band sector antenna with the same 90° beamwidth that radiates at 800 MHz, 2 GHz, and 4 GHz in order to verify the concept of the proposed antenna [4]. The prototype is shown in **Fig. 4**. The triple-frequency-band sector antenna comprises a multiband radiator, metamaterial reflector #1 (reflects electromagnetic waves at 4 GHz), metamaterial reflector #2 (reflects electromagnetic waves at 2 GHz), and a metal reflector (reflects electromagnetic waves at 800 MHz). The multiband radiator is separated from the reflectors by distance s_n, which is a quarter of the wavelength of each frequency band. That is, $s_1 = 18.8$ mm, $s_2 = 37.5$ mm, and $s_3 = 93.8$ mm. The multiband radiator consists of a biconical antenna and a dual-band sleeve dipole antenna [5].

The metamaterial reflectors consist of ceramic rods with a relative permittivity of 9.6 and a loss tangent of 3.5×10^5. The parameters of both metamaterial reflectors are $w_{11} = 4.7$ mm, $w_{12} = 8.6$ mm, $a_1 = 37.5$ mm, $w_{21} = 14.1$ mm, $w_{22} = 14.6$ mm, and $a_2 = 75.0$ mm. The side lengths of the reflectors are $L_1 = 83.6$ mm, $L_2 = 164.6$ mm, and $L_3 = 375.0$ mm.



(a) Perspective view

(b) Side view

Fig. 3. Woodpile metamaterial structure.

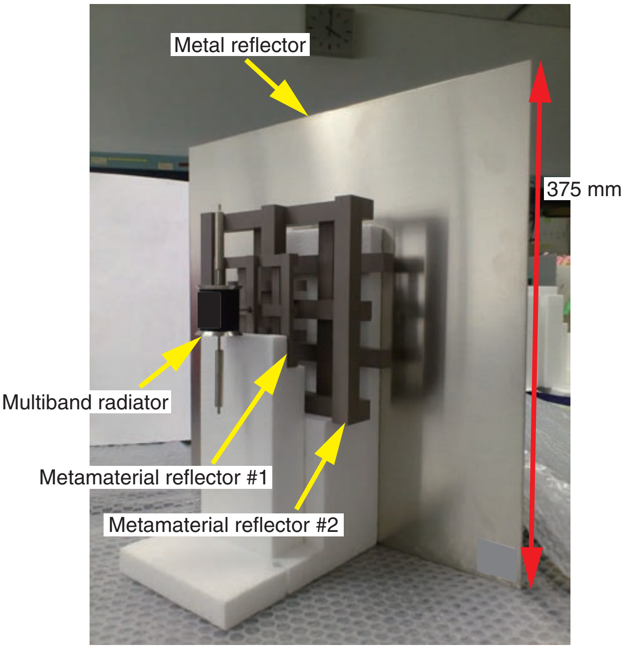


Fig. 4. Prototype antenna.

The EBG characteristics of the metamaterial reflectors are plotted in **Fig. 5**. It should be noted that each EBG characteristic corresponds only to the respective metamaterial reflectors. The center frequencies of the EBG band in the measurements and the electromagnetic field simulations are in good agreement. A finite array was used in the measurements, and consequently, the transmission characteristics degraded in comparison to those in the electromagnetic field simulations in which an infinite array was considered.

The radiation patterns on the horizontal plane for each frequency band are shown in **Fig. 6**. The proposed antenna has excellent directivity in each frequency band, and the measurement results match the electromagnetic field simulation results well. The beamwidth for each frequency band is indicated in **Table 1**. The proposed antenna achieves a beamwidth of approximately 90° at 800 MHz, 2 GHz, and 4 GHz, as designed.

5. Summary

We developed a novel multiband sector antenna employing multiple metamaterial reflectors and a multiband radiator for a sector antenna in mobile wireless communication systems. A triple-frequency-band sector antenna that radiates at 800-MHz, 2-GHz, and 4-GHz bands was designed, and a prototype was fabricated. We clarified the feasibility of the proposed small-footprint antenna in measurements and simulations.

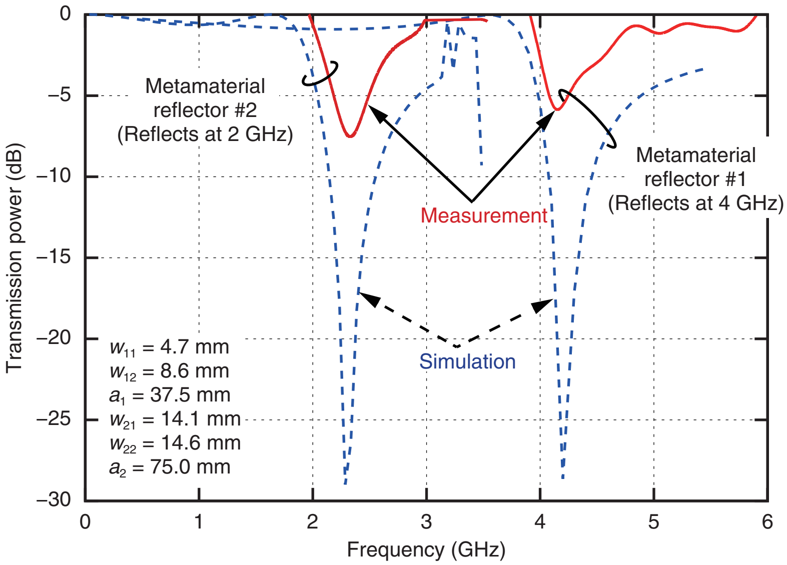
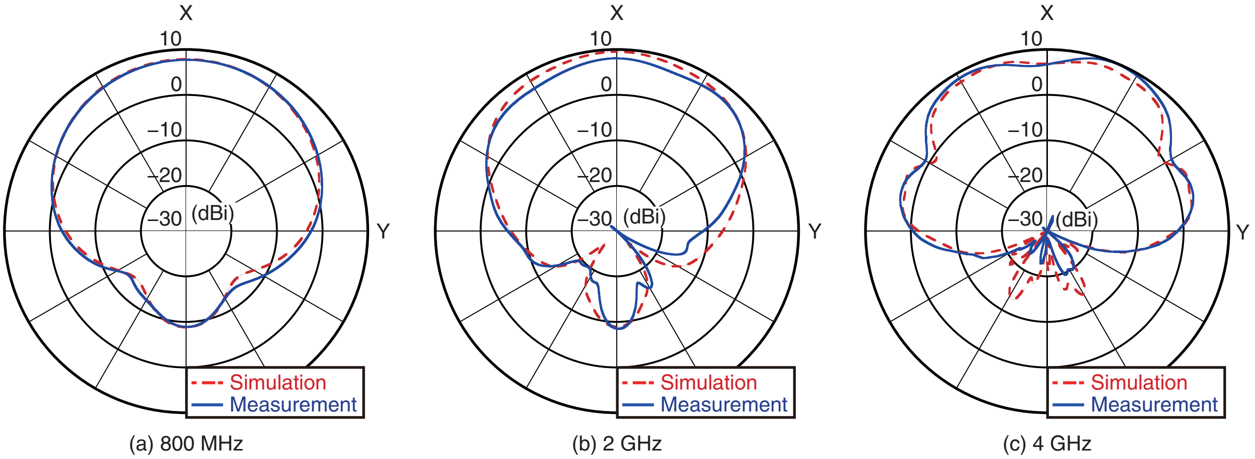


Fig. 5. EBG characteristics of woodpile reflectors.



(a) 800 MHz

(b) 2 GHz

(c) 4 GHz

Fig. 6. Radiation patterns of proposed antenna on horizontal plane.

Table 1. Beamwidth for each frequency band in horizontal plane.

	800 MHz	2 GHz	4 GHz
Simulation	94°	90°	90°
Measurement	98°	103°	89°

References

[1] K. Cho, R. Yamaguchi, and H. Jiang, “Base Station and Terminal Antenna Technologies Required for Next Generation Mobile Communication Systems,” IEICE Transactions on Communications, Vol. J91-B, No. 9, pp. 886–900, 2008 (in Japanese).

[2] G. S. Smith, M. P. Kesler, and J. G. Maloney, “Dipole Antennas Used with All-dielectric, Woodpile Photonic-bandgap Reflectors: Gain, Field Patterns, and Input Impedance,” Microwave and Optical Technology Letters, Vol. 21, No. 3, pp. 191–196, May 1999.

[3] E. Ozbay, A. Abeyta, G. Tuttle, M. Tringides, R. Biswas, T. Chan, C. M. Soukoulis, and K. M. Ho, “Measurement of a Three-dimensional Photonic Band Gap in Crystal Structure Made of Dielectric Rods,” Physical Review B, Vol. 50, No. 3, 1945–1948, July 1994.

[4] H. So, A. Ando, T. Seki, M. Kawashima, and T. Sugiyama, “Directional Multi-band Antenna Employing Woodpile Metamaterial with the Same Beamwidth,” Proc. of the 2013 IEICE General Conference, B-1-148, March 2013 (in Japanese).

[5] Y. Kanda, M. Ishikawa, S. Kon, and T. Haga, “Development of Multiband Antenna for Indoor Small Power,” Proc. of the 2013 IEICE Society Conference, B-1-142, September 2013 (in Japanese).

Hideya So

Engineer, NTT Access Network Service Systems Laboratories.

He received the B.E. from Tokyo University of Science in 2009 and the M.E. from Tokyo Institute of Technology in 2011. He joined NTT Access Network Service Systems Laboratories in 2011 and has been engaged in research and development (R&D) of antennas for future wireless access systems. He is a member of the Institute of Electronics, Information, and Communication Engineers (IEICE) and the Institute of Electrical and Electronics Engineers (IEEE).

Atsuya Ando

Research Engineer, NTT Access Network Service Systems Laboratories.

He received the B.S. in electronic engineering from Kitami Institute of Technology, Hokkaido, in 1988, the M.S. in information engineering from Hokkaido University in 1990, and the Dr. Eng. in system information engineering from Tsukuba University, Ibaraki, in 2013. Since joining NTT Wireless Systems Laboratories in 1990, he has been researching and developing personal and base station antennas for wireless mobile communication systems. From 2000 to 2003, he was with the ATR Adaptive Communications Research Laboratories in Kyoto, where he was involved in analyzing antennas for wireless ad-hoc network systems. He is currently engaged in R&D of base station antennas using metamaterials. He is a member of IEICE and IEEE.

Takatoshi Sugiyama

Senior Research Engineer, Supervisor, Group Leader, NTT Access Network Service Systems Laboratories.

He joined NTT in 1989 and has conducted R&D on forward error correction, interference compensation, CDMA, and MIMO-OFDM technologies for wireless communication systems such as satellite, wireless LAN, and cellular systems. He is currently responsible for the R&D of intelligent interference compensation technologies, radio propagation modeling, and multiband antenna design for future wireless communication systems. He currently serves as the Vice Chair of the Technical Committee on Satellite Communications in IEICE. He is a senior member of IEICE and a member of IEEE.

ITU-T FG-M2M Meeting Report

Yasuo Ishigure

Abstract

The ITU-T (International Telecommunication Union-Telecommunication Standardization Sector) Focus Group on Machine-to-Machine Service Layer (FG-M2M) was established at the January 2012 meeting of the Telecommunications Standardization Advisory Group to study applications of M2M technology in the e-health field. The group held 12 meetings between then and December 2013. This article reports on the results of the FG-M2M meetings.

Keywords: ITU-T, e-health, M2M

1. Introduction

As societies have continued to age in recent years, it has become more important to deal with societal issues in the medical field such as increasing medical costs and shortages of doctors and other aspects of the medical services system. This applies not only to Japan, with its relatively aged population, but also to other regions, including developing countries. Anticipation of *e-health*, utilizing ICT (information and communication technology), is increasing as a strategy for addressing this.

The International Telecommunication Union (ITU), in cooperation with the World Health Organization (WHO), established the Joint ITU & WHO mHealth Initiative for Non-communicable Diseases (NCDs) in October 2012. The main objectives were to investigate the proactive use of mobile phones in developing countries for sufferers of NCDs such as cancer and diabetes and to stimulate international cooperation and verification activities. ITU-T (ITU-Telecommunication Standardization Sector) also agreed on resolution 78, *Information and communication technology applications and standards for improved access to e-health services*, at the November 2012 WTSA-12 (World Telecommunication Standardization Assembly) general meeting, the goals of which were to give higher priority to the medical field and accelerate cooperative efforts with standardization organizations such as WHO.

The ITU-T Focus Group on Machine-to-Machine Service Layer (FG-M2M) discussed in this article established a venue for studying M2M technology focused on the e-health domain. It held 12 meetings between April 2012 and December 2013. This article discusses the objectives and status of the FG-M2M and gives an overview of the working group structure and results documents.

2. Meeting overview

2.1 Objectives

The objectives of the FG-M2M, as described below, are defined in its Terms of Reference (ToR), in order to avoid duplicating work done by other standardization organizations, and to clarify its contribution to the field of e-health, among other things. The specific objectives are to:

- Collect and document information from the global M2M community and from vertical market entities on current activities and technical specifications including requirements, use cases, and service and business models.
- Draft technical reports to support the development of APIs (application programming interfaces) and protocols to enable M2M services and applications, focusing initially on services and applications for e-health.
- Facilitate and encourage the participation and contribution of vertical market stakeholders and liaise with other SDOs (standards development organizations) to avoid duplication of activities.
- Assist in the preparation and conduct of the ITU/WHO workshop on e-health (26–27 April 2012)

with respect to M2M applications and services for the health-care sector.

The FG-M2M agreed on the main task of creating five results documents (deliverables) that would reflect the results of its study. These deliverables are described in section 3.

2.2 Meeting status

Twelve meetings were held, with the last one in December 2013. Three of these meetings were held remotely through teleconferencing. Each meeting was managed by a corporate host, and the 12th and final meeting was held by the European branch of Japan's NEC Corporation. The number of participants and documents submitted for each meeting ranged widely, but usually about 25 participants from about 8 countries (about 6 from Japan) participated, and approximately 20 documents were submitted (about 5 from Japan). Relatively more of the participants were from Asian countries, but the meetings were internationally diverse, with participants from Europe, North America, the Middle East, and Africa. This demonstrates the broad international interest in M2M and e-health.

3. WG structure and deliverables

Discussions at the meetings were held in three working groups (WGs): WG1 focused on e-health Use Cases and Service Models, WG2 on M2M Service Layer Requirements and Architecture, and WG3 on APIs and Protocols. Each WG was responsible for creating a deliverable according to its respective theme, but meetings were held so that basically all participants could participate in all of the WGs, and the main proponents were the leaders and editors of the deliverables for each WG. An overview of each of the deliverables is given below.

3.1 (D0.1) M2M standardization activity and gap analysis in the e-health domain

This deliverable is composed of two main parts. The first part describes e-health standardization activities. It explains the activities of existing e-health standardization organizations and lists the technical specifications and reports they have issued. The second part describes the technical content of documents created by the FG-M2M and analyzes the differences between those documents and the documents issued by the e-health standardization organizations listed in the first part. It also discusses the relationship between FG-M2M and the other organizations. The analysis in this document will be useful in clarifying the overlap and differences with other standard specifications when creating specifications from other deliverables in the future, and we hope that other e-health standardization organizations will also use them to increase awareness of other technical areas that have not been standardized.

The investigation covered documents published by the following organizations:

- CEN TC251 (European Committee for Standardization, Technical Committee 251)
- Continua Health Alliance
- DICOM (Digital Imaging and Communications in Medicine)
- epSOS (European Patients Smart Open Services)
- ETSI (European Telecommunication Standards Institute), M2M for use cases
- GSMA (Groupe Speciale Mobile Association)
- HL7 (Health Level 7)
- IHE (Integrating the Healthcare Enterprise)
- ISO/IEC (International Organization for Standardization/International Electrotechnical Commission) TC215
- ITU-T (Q2/13 and Q28/16)
- M-Health Alliance
- WHO

3.2 (D0.2) M2M ecosystem in the e-health domain

This deliverable describes high-level requirements by defining terminology and concepts related to e-health and describing a conceptual model of the e-health ecosystem using M2M technologies (**Fig. 1**). There are differences in the way similar terms such as telehealth, telemedicine, and remote patient monitoring are understood in different countries and regions, even among specialists, and much time has been spent on reaching a common understanding in meetings. This is an important deliverable because the high-level requirements derived from e-health concepts and ecosystems form the basis for content in other FG-M2M documents.

3.3 (D1.1) M2M use cases in e-health

This deliverable describes typical use cases for M2M technology in the e-health domain. A total of ten use cases are described in two main categories: those using vital data monitoring sensor terminals and server systems, and those using devices other than sensors with server systems. The use cases described in the document are listed in **Table 1**.

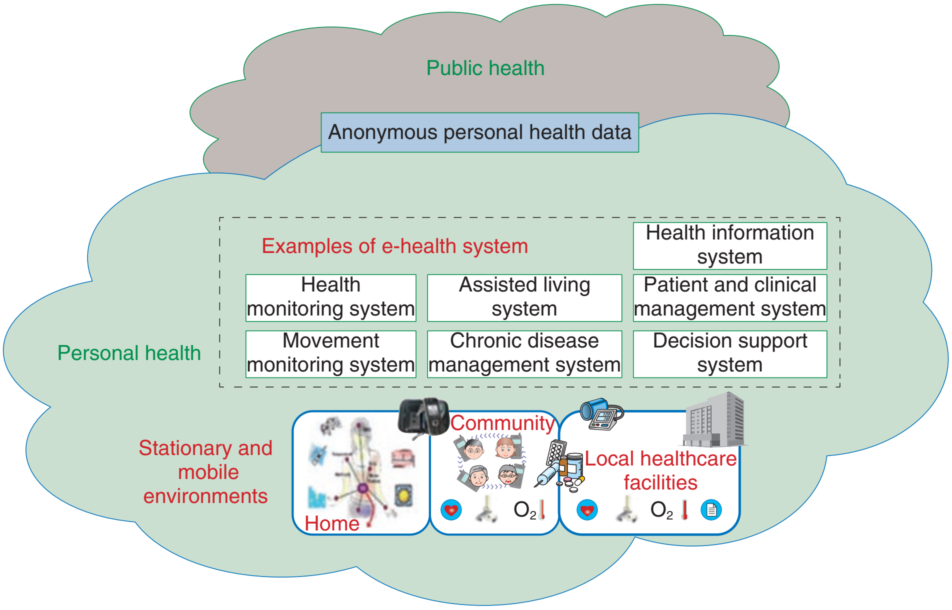

Public health
Anonymous personal health data
Examples of e-health system
Health information system
Health monitoring system
Assisted living system
Patient and clinical management system
Personal health
Movement monitoring system
Chronic disease management system
Decision support system
Stationary and mobile environments
Community
Local healthcare facilities
Home
O2
O2

Fig. 1. e-health system overview.

Table 1. List of use cases.

No.	Title of use case
1	Legacy mass medical examination
2	Travelling mass medical examination with BAN
3	Remote patient monitoring
4	Telehealth counseling system
5	Telehealth management system using NFC e-health device and smartphone
6	Telehealth system for home care support
7	Ambient assisted living (AAL)
8	Easy clinic
9	Personal healthcare data management
10	Expert system for sharing medical information/applications

BAN: body area network

3.4 (D2.1) Requirements and architecture for the M2M service layer

This deliverable describes common requirements for the M2M service layer and requirements for e-health system applications. The M2M service layer is shown in relation to existing recommendations by mapping it to the IoT reference model diagram as described in ITU-T Recommendation Y.2060, Overview of Internet of Things (IoT) (**Fig. 2**). The M2M service layer requirements use the high-level requirements in the D0.2 M2M ecosystem document as a starting point, refer to the D1.1 use-case document and definitions in documents from other standardization organizations, and identify common requirements. They also describe architecture and basic concepts for reference points. Although a detailed study was beyond its scope, it should be useful for conducting a detailed study in the future.

3.5 (D3.1) Overview of M2M service layer APIs and protocols

This deliverable gives an overview of APIs and protocols desired for the reference points in the architecture deliverable (D2.1). It gathers information on

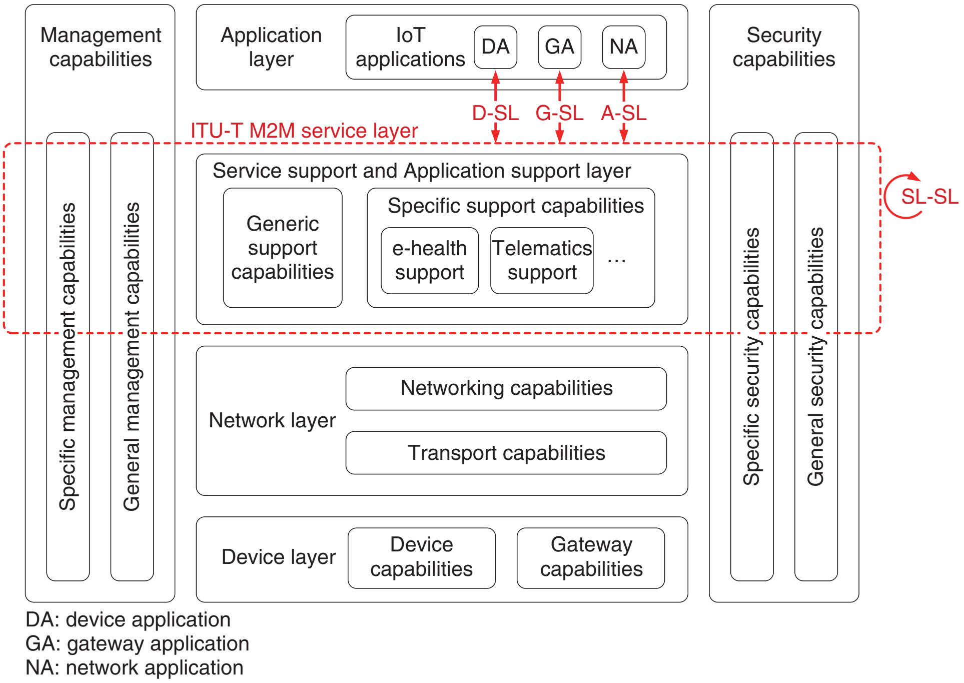


Fig. 2. ITU-T M2M service layer (SL) in the IoT reference model.

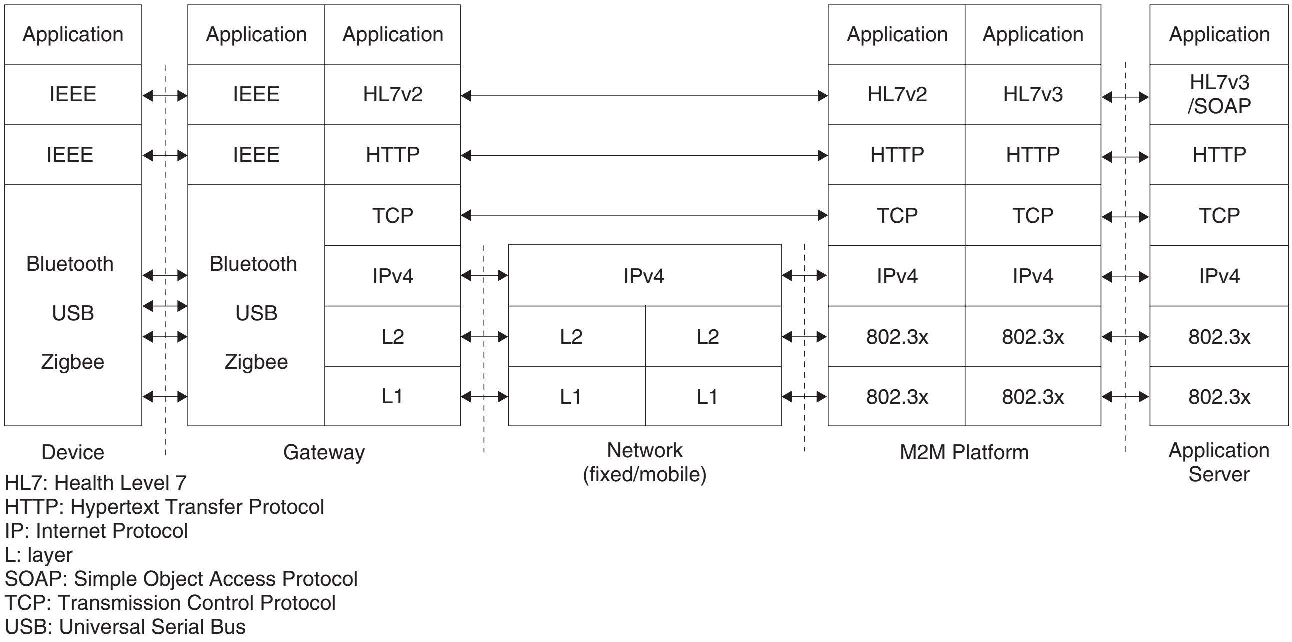


Fig. 3. Example of M2M protocol stacks for e-health application (using gateway).

existing APIs and protocols that are promising for application in the M2M service layer, analyzes protocol features, and gives protocol structure examples (**Fig. 3**). Analytical tools used in defining requirements for each reference point are also presented in order to provide information as a base for studying API and protocol specifications in the future.

4. Reflection and future prospects

Since the inauguration of FG-M2M about two years ago, there has been a gap in awareness of M2M and e-health between M2M technology members and e-health specialists, but mutual understanding increased as the meetings progressed, and in the end, they were able to cooperate in producing the deliverable documents. In particular, the participants from Japan discussed issues before each meeting in the e-Health Working Party of the Telecommunication Technology Committee, as a place for deliberation within Japan, and proactively submitted documents to FG-M2M. As a result, Japan contributed the most documents as well as four of the editors, and led the overall discussion in the meetings.

In the future, plans after FG-M2M will be discussed in Study Group 11 (Protocols and Test Specifications) and the Telecommunication Standardization Advisory Group meetings, which are high-level sections of the FG-M2M, and activities will continue toward making recommendations in the related study groups.

Anticipation is high from the e-health marketplace, and more activity in standardization and promotion will be needed in the future. To expand the technical domains related to e-health, it will be important to cooperate with study groups within ITU-T to create recommendations and with medically related organizations such as WHO to create the necessary standards.

Yasuo Ishigure

Senior Research Engineer, Medical and Healthcare Information Systems Development Project, Public ICT Solution Project, NTT Secure Platform Laboratories.

He received the B.E., M.E., and Ph.D. in electronic and information engineering from National Toyohashi University of Technology, Aichi, in 1995, 1997, and 2000, respectively.

He joined NTT Cyber Space Laboratories (now NTT Media Intelligence Laboratories) in 2000 and studied super-high-reality communication technologies including super-high-resolution (4K/2K) and 3D image display systems and their human factors. He promoted the Super High Reality Communication Service via the broadband optical fiber network, which led to him receiving an award at the 3D Image Conference in Japan in 2005.

From 2005 to 2007, he was Deputy Manager of the Life Science Business Promotion Office, Business Innovation Sector, at NTT DATA. From 2007 to 2010, he was Deputy Senior Analyst at the Research Institute for System Science, Research and Development Headquarters, at NTT DATA.

He has been active in proposing electronic health records (EHRs) and personal health records (PHRs) in Japan and has published some books on EHRs and PHRs.

Since 2010, he has been studying technologies related to e-health services including EHRs and PHRs in NTT Secure Platform Laboratories. Since 2012, he has been leading e-health standardization at the Telecommunication Technology Committee of Japan.

New NTT Colleagues
—We welcome our newcomers to the NTT Group

Here, we welcome newcomers to the NTT Group. This is a corner of the NTT Technical Review where we introduce our new affiliate companies.

Nexus — Established in 2004, Headquartered in USA, IT solutions service provider

Founded in 2004, and headquartered in Valencia, California, Nexus is a provider of advanced IT solutions serving enterprises, mid-sized business and public sector clients. The company employs over 650 staff and provides expertise in end-to-end technology solutions based on eight distinct connected solutions: Collaboration, Enterprise Networking, Security, Mobility, Data Center, Cloud, Consulting Services, and Managed Services. Nexus partners with industry leaders including Cisco, EMC, VMware, Citrix, NetApp, Apple, and Microsoft to ensure its customers are provided the most comprehensive and competitive solutions. Nexus serves the private sector, from small business to the Fortune 500; and the public sector including local, state, and federal government. Additionally, Nexus has highly specialized vertical market practices including education, retail, hospitality, and healthcare. For additional information, please visit www.nexusis.com.

Contacts:
Dimension Data
http://www.dimensiondata.com/Global/Downloadable%20Documents/Dimension%20Data%20Acquires%20US-based%20Nexus%20-%20Expands%20US%20Operations.pdf

External Awards

The Commendation for Science and Technology by the Minister of Education, Culture, Sports, Science and Technology—The Young Scientists' Prize—

Winner: Hajime Okamoto, NTT Basic Research Laboratories
Date: April 15, 2014
Organization: Ministry of Education, Culture, Sports, Science and Technology

For "A Study of the Quantum Nanomechanical Sensing Technology".

A new technology that enables highly sensitive mechanical detection has been developed by the integration of superconductor, optical light, and semiconductor low dimensional structures into nanomechanical resonators.

Conference on LED and Its Industrial Application (LEDIA '14) Young Researcher's Paper Award

Winner: Ryan G. Banal, NTT Basic Research Laboratories
Date: April 24, 2014
Organization: Conference on LED and Its Industrial Application (LEDIA '14)

For "Nonpolar M-plane AlGaN Deep-UV LEDs".

We demonstrated stronger deep-UV light emission from nonpolar M-plane AlGaN QW LEDs than conventional polar C-plane ones and explained their emission properties in terms of optical polarization and the quantum-confined Stark effect.

Papers Published in Technical Journals and Conference Proceedings

Resilient Photonic Network Architecture with Plug & play Optical Interconnection Technology

T. Sakano, H. Kubota, T. Komukai, T. Hirooka, and M. Nakazawa

Proc. of the 18th OptoElectronics and Communications Conference (OECC), TuQ3-5, Kyoto, Japan, July 2013.

This paper proposes a resilient photonic network based on digital coherent optical transceivers and movable ICT resource units. We developed a 100-Gbit/s transceiver for the movable unit and experimentally confirmed its plug & play capability.

A Rapidly Restorable Phone Service from Catastrophic Loss of Telecommunications Facilities

T. Sakano, S. Kotabe, K. Sebayashi, T. Komukai, H. Kubota, and A. Takahara

Proc. of Humanitarian Technology Conference (HTC) 2013, IEEE Region 10, TS7, Sendai, Japan, August 2013.

This paper proposes a phone service system which enables us to rapidly restore telephone service even under the situation where the facilities for ICT services are catastrophically damaged due to a large scale disaster. In the proposed system, a movable ICT unit which accommodates an IP-PBX function is deployed to a damaged area, and it promptly launches a telephone service based on Voice over IP (VoIP) and WiFi technologies. Users are able to access the telephone service using their own smartphones and telephone numbers; thus, it is convenient to use. The authors developed a prototype system and performed subjective evaluation experiments by expected users such as the employees of telecom companies, local governments, and the Japanese government. Through the experimental results, we confirmed the effectiveness of the proposed system.

Multi-document Summarization Model Based on Redundancy-constrained Knapsack Problem

H. Nishikawa, T. Hirao, T. Makino, Y. Matsuo, and Y. Matsumoto

Journal of Natural Language Processing, Vol. 20, No. 4, pp. 585–612, September 2013.

In this study, we regard multi-document summarization as a redundancy-constrained knapsack problem. The summarization model based on this formulation is obtained by adding a constraint that curbs redundancy in the summary to a summarization model based on the knapsack problem. As the redundancy-constrained knapsack problem is an NP-hard problem and its computational cost is high, we propose a fast decoding method based on the Lagrange heuristic to quickly locate an approximate solution. Experiments based on ROUGE evaluation show that our proposed model outperforms the state-of-the-art text summarization model known as the maximum coverage model in finding the optimal solution. We also show that our decoding method finds a good approximate solution, which is comparable to the optimal solution of the maximum coverage model, more than 100 times faster than an integer linear programming solver.

Nonlinear Modeling and Analysis on Concurrent Amplification of Dual-band Gaussian Signals

I. Ando, G. Tran, K. Araki, T. Yamada, T. Kaho, Y. Yamaguchi, and K. Uehara

IEICE Trans. on Electronics, Vol. E96-C, No. 10, pp. 1254–1262, October 2013.

In a flexible wireless system, nonlinear distortion is increased in its wideband power amplifier (PA) because the PA needs to concurrently amplify multi-band signals. By taking higher harmonics as well as inter- and cross-modulation distortion into consideration, we have developed a method to analytically evaluate the adjacent channel leakage power ratio (ACPR) and error vector magnitude (EVM) on the basis of the PA's nonlinear characteristics. We devised a novel method for modeling the PA amplifying dual-band signals. The method makes it possible to model it merely by performing a one-tone test, making use of the Volterra series expansion and the general Wiener model. We then use the Mehler formula to derive the closed-form expressions of the PA's output power spectral density (PSD), ACPR, and EVM. The derivations are based on the assumption that the transmitted signals are complex Gaussian distributed in orthogonal frequency division multiplexing transmission systems.

Implementation and Evaluation of Real-time Distributed Zero-forcing Beamforming for Downlink Multi-user MIMO Systems

T. Murakami, K. Ishihara, R. Kudo, Y. Asai, T. Ichikawa, and M. Mizoguchi

IEICE Trans. on Communication, Vol. E96-B, No. 10, pp. 2521–2529, October 2013.

The implementation and experimental evaluations of distributed zero-forcing beamforming (DZFBF) for downlink multi-user multiple-input multiple-output (DL MU-MIMO) systems are presented. In DZFBF, multiple access points (APs) transmit to desired stations (STAs) at the same time using the same frequency channel while mitigating inter-cell interference. To clarify the performance and feasibility of DZFBF, we developed a real-time transmission testbed that includes two APs and four STAs; all are implemented using a field programmable gate array. For real-time transmission, we also implemented a simple weight generation process based on ZF weight using channel state information which is fed back from STAs; it is an extension of the weight generation approach used in DL MU-MIMO systems. By using our testbed, we demonstrate the real-time transmission performance in actual indoor multi-cell environments. These results indicate that DL DZFBF is more effective than DL MU-MIMO with time division multiple access.

Estimating Illuminant Colors by a Gray-world-assumption-based Method Using High and Low Chroma Gamuts and Opponent Color Properties

H. Kawamura, S. Yonemura, J. Ohya, and A. Kojima

IEICE Trans. on Information and Systems (Japanese Edition), Vol. J96-D, No. 12, pp. 3079–3089, December 2013.

We propose an illuminant color estimation method based on gray world assumption using opponent color properties and color gamuts. It estimates illuminant colors more correctly than the conventional method in cases where there are few colors in an image or when image colors are distributed unevenly in local areas in the color space. The method uses high-chroma gamuts for adding appropriate colors to the original image and low-chroma ones for narrowing down illuminant color possibilities. Experimental results show that the average estimation error derived by our method is statistically smaller than that derived by the conventional method.

Deriving the "Salience Level" of a Target Sound Using a Tapping Technique

S. Kidani, H. Liao, M. Yoneya, M. Kashino, and S. Furukawa

Abstracts of Proc. of the 37th Annual Midwinter Meeting of the Association for Research in Otolaryngology (ARO), Vol. 37, p. 385, San Diego, USA, February 2014.

The salience level obtained by the tapping method reflects the subjective salience of target sounds. The salience level is somewhat independent of the subjective loudness of a sound, as indicated by the lack of correlation between the salience level and the loudness value.

A Method of Estimating Scene Illuminant Colors from Color Images under Varying Illumination Taken by Fixed Camera

H. Kawamura, Y. Yao, S. Yonemura, J. Ohya, and A. Kojima

The Journal of the Institute of Image Electronics Engineers of Japan, Vol. 43, No. 2, pp. 164–174, 2014.

This paper proposes a method for estimating scene illuminant colors from two color images taken by a fixed camera under two different illuminations. Our method obtains two sets of surface reflectances of a scene area common to the two images, and estimates the colors of the two illuminations based on the property that the intersection of the sets could correspond to the common area. To obtain the sets of surface reflectance from the colors in the images, the relationship between surface reflectance and the colors in the image, which are calculated using surface reflectance called a "typical set" from the ISO/TR 16066 object color spectra database for color reproduction evaluation and possible illuminants, is used. Experiments using numerical simulation and actual images show that our method derives smaller estimation errors than conventional methods, and that it provides stable estimations for several kinds of illuminants and reflectances.

Improvement of 200-kHz KTN Optical Scanner Performance with Multiple Internal Reflection

S. Toyoda, Y. Sasaki, and J. Kobayashi

The Journal of Engineering, pp. 1–2, 2014.

The authors have realized a $KTa_xNb_{1\_x}O_3$-based optical beam scanner that has three- and five-pass configurations with internal reflection whose scanning angle is exactly proportional to the optical path length. They successfully increased the scanning angle to about 140 mrad with a 200-kHz modulation using a five-pass configuration. This beam scanner will provide an optical coherence tomography (OCT) system with a spatial resolution of 7 μm and advantages over other OCT systems.

Missing Sensor Value Estimation Method for Participatory Sensing Environment

H. Kurasawa, H. Sato, A. Yamamoto, H. Kawasaki, M. Nakamura, Y. Fujii, and H. Matsumura

Proc. of 2014 IEEE International Conference on Pervasive

Computing and Communications (PerCom), pp. 103–111, Budapest, Hungary, March 2014.

Participatory sensing produces incomplete sensor data. Thus, we have to fill in the gaps of any missing values in the sensor data in order to provide sensor-based services. We propose a method to estimate a missing value of incomplete sensor data. It accurately estimates a missing value by repeating two processes: selecting sensors locally correlated with the sensor that includes the missing value and then updating the training sensor dataset that consists of data from the selected sensors available for multiple regression. This procedure effectively helps to find more suitable neighbor records of a query record from the training sensor dataset and to refine the regression model using the records. We confirmed through a field trial and a life-log enrichment trial that our method was effective for estimating missing sensor values in a participatory sensing environment.

Large-scale Cross-media Analysis and Mining from Socially Curated Contents

A. Kimura

Progress in Informatics, No. 11, pp. 19–30, 2014.

This paper focuses on another emerging trend called *social curation*, a human-in-the-loop alternative to automatic algorithms for social media analysis. Social curation can be defined as a spontaneous human process of remixing social media content for the purpose of further consumption. What characterizes social curation is definitely the manual effort involved in organizing a collection of social media content, which indicates that socially curated content has potential as a promising information source against automatic summaries generated by algorithms. Curated content would also provide latent perspectives and contexts that are not explicitly presented in the original resources. Following this trend, this paper presents recent developments and the growth of social curation services, and reviews several research trials for cross-media analysis and mining from socially curated content.

Channel Coding and Lossy Source Coding Using a Generator of Constrained Random Numbers

J. Muramatsu

IEEE Trans. on Information Theory, Vol. 60, No. 5, pp. 2667–2686, May 2014.

Stochastic encoders for channel coding and lossy source coding are introduced with a rate close to the fundamental limits, where the only restriction is that the channel input alphabet and the reproduction alphabet of the lossy source code are finite. Random numbers, which satisfy a condition specified by a function and its value, are used to construct stochastic encoders. The proof of the theorems is based on the hash property of an ensemble of functions, where the results are extended to general channels/sources, and alternative formulas are introduced for channel capacity and the rate-distortion region. Since an ensemble of sparse matrices has a hash property, we can construct a code by using sparse matrices.

Eye-hand Coordination in On-line Visuomotor Adjustments

N. Abekawa, T. Inui, and H. Gomi

NeuroReport, Vol. 25, No. 7, pp. 441–445, 2014.

We examine the relationship between on-line hand adjustment and eye movements. In contrast to the well-known temporal order of eye and hand initiations where the hand follows the eyes, we found that on-line hand adjustment was initiated before the saccade onset. Despite this order reversal, a correlation between hand and saccade latencies was observed, suggesting that the on-line hand motor system is not independent of eye control. Moreover, the latency of the hand adjustment with saccadic eye movement was significantly shorter than that with eye fixation. This hand latency modulation cannot be ascribed to any changes of visual or oculomotor reafferent information since the saccade was not yet initiated when the hand adjustment started. Taken together, the hand motor system would receive preparation signals rather than reafference signals of saccadic eye movements to provide quick manual adjustments of the goal-directed eye-hand movements.

Reliable Data Transmission of 8K Video over Multi-domain Networks

T. Fujii, H. Uose, M. Stanton, and L. Ciuffo

Proc. of 15th Workshop RNP, Vol. WRNP15, pp. 1–40, Florianópolis, Brazil, May 2014.

We explained the technology to transmit 8K new generation video for a public-viewing event from Brazil to Tokyo. Shared networks are used to transmit 8K video to reduce the network cost and setup-time, but we need to take special care to ensure reliability against packet losses. Therefore, we developed an improved LDGM-FEC algorithm and implemented it in a system to enable robust IP transmission over long-distance shared networks.