独立行政法人
情報通信研究機構

NICT NEWS

National Institute of Information and Communications Technology

2013 DEC
No. 435
12

Massive Tornado-Producing Supercells Affect the Space Environment

−The first clear evidence that severe meteorological events affect the ionosphere−

Michi NISHIOKA

Researcher, Space Weather and Environment Informatics Laboratory, Applied Electromagnetic Research Institute

After completing a doctoral course and staying at Boston College (as a JSPS postdoctoral fellow) and Nagoya University, she joined NICT in 2011. She has been researching the monitoring, prediction, and correction of ionospheric disturbances that affect radio propagations. Ph.D. (Science).

Introduction

The Earth's atmosphere at an altitude of 60 km or higher is partly ionized by the solar X-ray and EUV (extreme ultraviolet), existing as plasma, or ionized gas, which consists of ions and electrons. This plasma-rich region at 60–1,000 km altitude is called the ionosphere, where the international space station and artificial satellites orbit (300–400 km altitude) and the auroras appear (100–500 km altitude). Therefore the ionosphere may be expressed as "the entrance to the space". It has been well known that the ionospheric condition is changed greatly under the influence of the activities of the sun. Recently, it has been reported that the lower atmosphere can cause ionospheric disturbances. The influence of a great earthquake to the ionosphere was observed after the 2011 Tohoku Earthquake. The atmospheric waves, which were excited on the surface of the sea near the epicenter, induced concentric waves in the ionosphere (see NICT News, December 2011). On the other hand, the effects of meteorological events on the ionosphere have not been understood yet. We have developed and operated a total electron content (TEC) observation system in order to monitor and research ionospheric disturbances. TEC is the total number of electrons in a unit column in the ionosphere, which is derived from pairs of a GPS satellite and a ground-based GPS receiver. It strongly reflects plasma density in the ionosphere at the approximately 300 km altitude where the density of plasma is the maximum. We collect the observation data of more than 6,000 ground-based GPS receivers in the world and calculate TEC. This makes it possible to create the wide-coverage two-dimensional TEC map in high resolution. Using the TEC map, we have succeeded in capturing the details of the wave generating the ionosphere.

Massive tornado—producing supercells affect the space environment

Concentric wave structures were observed in the TEC maps after the massive EF-5* tornado hit Moore, Oklahoma, USA in May 2013. Figure 1 shows the concentric waves of TEC detected by using data of more than 2,600 ground-based GPS receivers deployed in the North American continent. The center of the con-

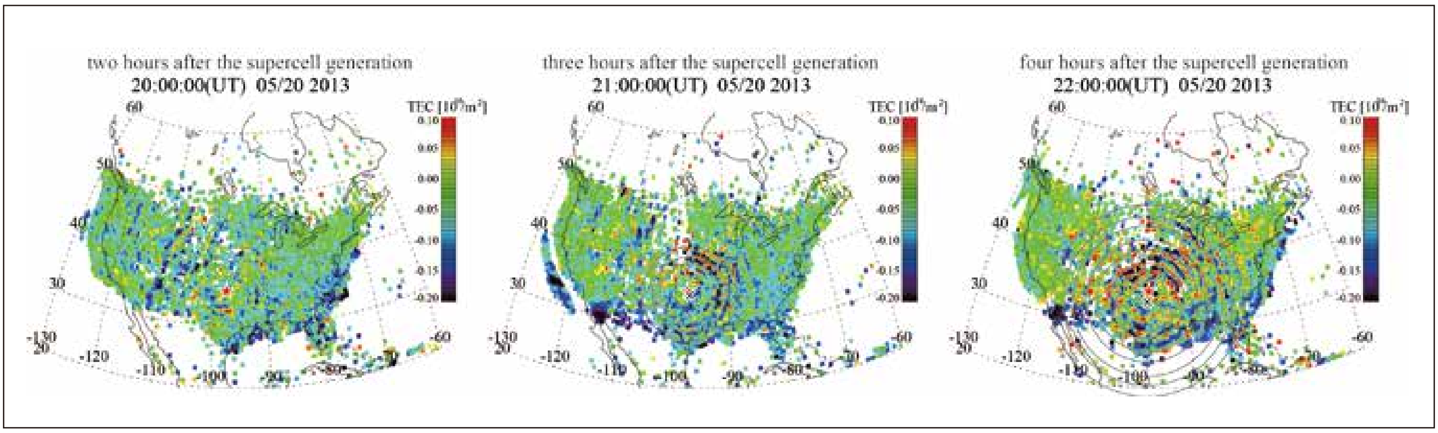


Figure 1　Concentric waves observed in the high-resolution TEC map over North America

TEC is the total number of electrons in a tube of one meter squared cross section. In general, a TEC Unit is defined as 1 TECU = $10^{16}/m^2$. The TEC data are detrended values derived by subtracting 20-minute running average data. The red star represents is the location of Moore, The cross mark represents the center of concentric waves which are indicated by the solid lines.

* Enhanced Fujita scale (EF)
The Enhanced Fujita (EF) scale rates the strength of tornadoes based on the damages caused by the tornado. The EF scale has six categories from EF-0 to EF-5.

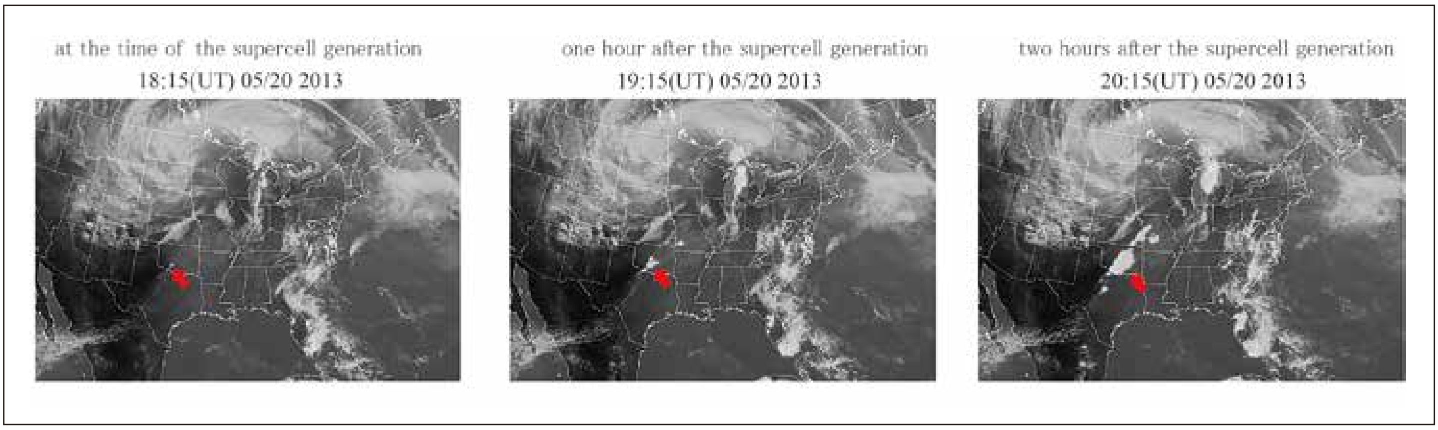


Figure 2 Supercells captured by infrared images by the GOES-13 satellite
GOES satellites, which are meteorological satellites operated by the National Oceanic and Atmospheric Administration of United States, observe clouds. The Figure 2 shows infrared image of clouds observed by the GOES-13 satellite. In the infrared images, low clouds show up as more gray and higher clouds show up as more while. The supercell which brought the massive tornado to Moore at 19:45(UT) May 20, 2013, shows up as bright white, as indicated by the red arrow.

centric waves coincide with the location of a supercell which produced the massive tornado in Moore. Figure 2 shows the infrared image of supercells observed from a meteorological satellite. The concentric TEC structure had been observed traveling throughout North America for more than seven hours. The period of the concentric TEC waves was about 15 minutes. We concluded that the concentric TEC structure was induced by atmospheric gravity waves, which are transverse waves of the atmosphere restored by gravity and buoyancy. In addition to the concentric TEC structure, TEC periodic oscillation was observed above the supercell. The period of the TEC oscillation was about 4 minutes. We concluded that the TEC oscillation was caused by acoustic waves, which are atmospheric compression waves, resonating between the ionosphere and the earth's surface. This observation demonstrates the first clear evidence of a severe meteorological event causing atmospheric waves propagating upward in the upper atmosphere and reaching the ionosphere of around 300 km, using the wide-coverage and high-resolution TEC map (Figure 3).

Future prospects

This observation is important in identifying how the atmosphere affects the ionosphere, which is used for satellite navigations and communications. We have also observed concentric waves after a tornado hit Tsukuba city, Japan, in May 2012. These results imply that the ionospheric observation can provide information on meteorological events in the future.

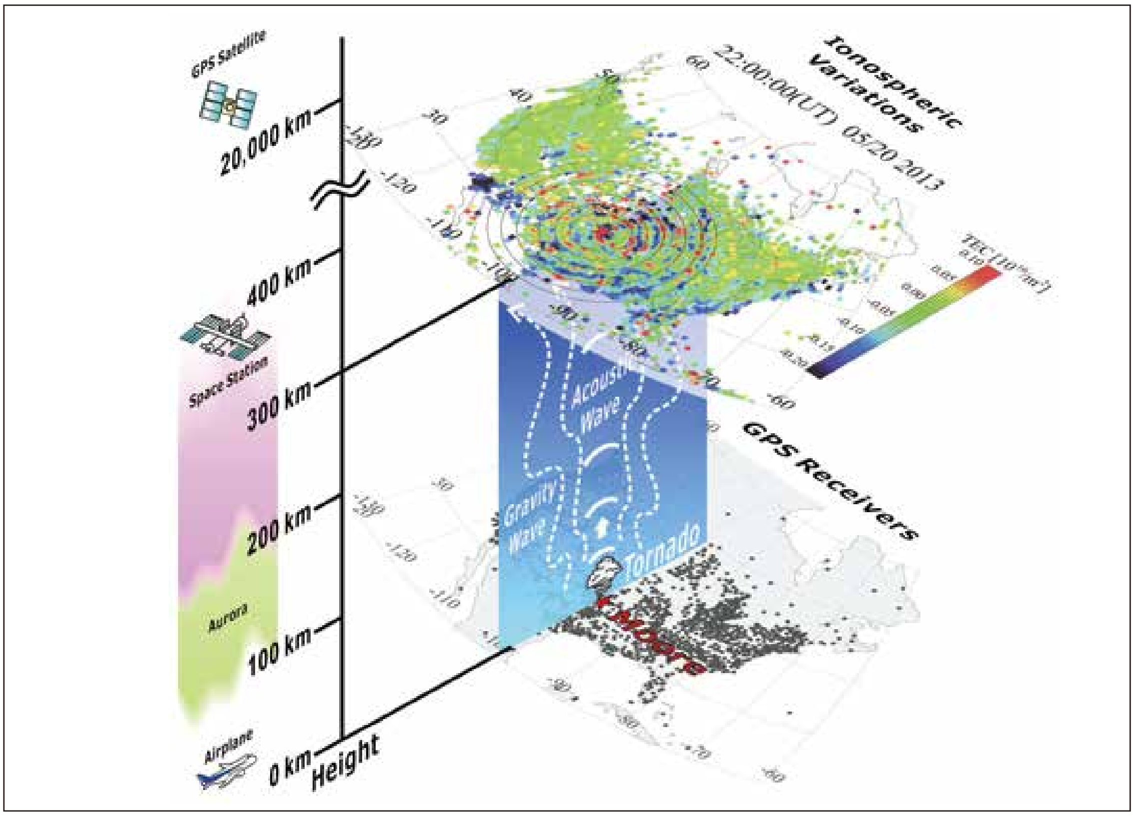


Figure 3 Schematic picture of atmospheric waves and the ionospheric disturbance after the 2013 Moore tornado
It is considered that the supercell which produced the massive tornados caused acoustic wave and atmospheric gravity wave propagating upward to the upper atmosphere, reaching to the ionosphere, and causing the ionospheric disturbances.

The Evolution of Superconducting Photon Detection Technology

—Success in drastic improvement of detection efficiency and response speed—

Shigehito MIKI
Senior Researcher, Nano ICT Laboratory, Advanced ICT Research Institute

After completing a doctoral degree, served as a researcher of the Japan Science and Technology Agency, he joined NICT in 2005. He is engaged in research about single photon detectors using superconducting nanowire. Ph.D. (Engineering).

Taro YAMASHITA
Senior Researcher, Nano ICT Laboratory, Advanced ICT Research Institute

After completing a doctoral degree, served as Research Fellow of the Japan Society for the Promotion of Science (DC2/PD), worked for KENWOOD Corporation (now JVC KENWOOD Corporation) before joining NICT in 2009. He is engaged in research about single photon detectors using superconducting nanowire. Ph.D. (Science).

Introduction

Superconducting nanowire Single Photon Detector: SSPD has excellent features such as less false positives (low dark count rate), smaller time fluctuation (low timing jitter), and it does not require gate synchronization (gate-free operation) compared to the Avalanche Photo Diode: APD that has been widely used as a single photon detector. From the features above, the application of SSPD in various research fields such as space optical communication technology, quantum communication, laser sensing and bio-imaging, are expected. We are conducting research and development for the practical application of SSPD at NICT. Previously, the performance of SSPD developed by NICT, had remained in the same performance as that of APD: detection efficiency with respect to the incident photon at communication wavelength band (1,550 nm) was about 20%, and the maximum count rate, which is a response rate of photon detection was also about 25 MHz. This time, at NICT we achieved a new light absorbing structure in SSPD device, and conducted the optimization of the nanowire design by the finite element analysis*. By this, we have succeeded in significantly improving the performance of response speed and detection efficiency.

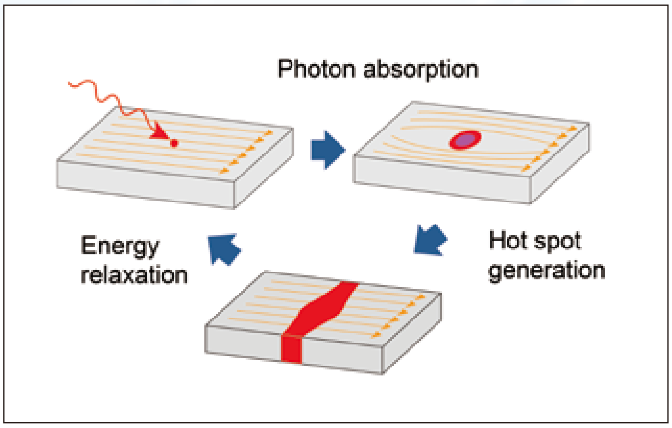


Figure 1 The principle of Superconducting nanowire Single Photon Detector

Improvement in detection efficiency by realizing new optical absorption structure

SSPD device is composed of meandering superconducting nanowire made of 100-nm-wide and a few-nm-thick superconducting thin films. Then, onto this, supply bias currents slightly smaller than the superconducting critical current which can flow in the zero resistance. When a photon is absorbed by the incident on the superconducting nanowires, the superconducting state is destroyed locally, and resistive component is generated. By observing the voltage pulses generated during the time, this can be used to detect single photons (Figure 1).

Detection efficiency of the SSPD is highly dependent on the photon absorption rate to the superconducting nanowires. For example, as a case of simple structure with arranging superconducting nanowires on a substrate as shown in Figure 2 (a), a number of photons passing through the gap between the nanowires is large, and sufficient absorption can not be obtained. Thus, the detection efficiency would be a few percent. However, by adding an optical cavity layer that confines the photons at the top of the device, as shown in Figure 2 (b), the light absorption rate is increased and the detection efficiency is improved. This time, we improved the optical absorptance further by adopting a structure in which the nanowire was sandwiched by the upper and lower cavity layers, as shown in Figure 2 (c), it is now possible to increase to 95% or more light absorption rate. Detection efficiency will be improved as increasing the current value of bias in superconducting nanowires, but it will increase the dark count (the number of times that outputs an error signal in the absence of incident photons) at the same time. We have found that with the SSPD that we have developed, a detection efficiency of 80% would be obtained in the bias region when the dark counts are lowered in 50–100 Hz counts / sec (see Figure 2 (d)). In Figure 2 (d), we have also noted the performance of the InGaAs APD, and you can see the SSPD we have developed showing much higher performance.

---

* Finite element analysis
Method of obtaining an approximate solution of the differential equation by dividing by a slight space object having a complicated shape.

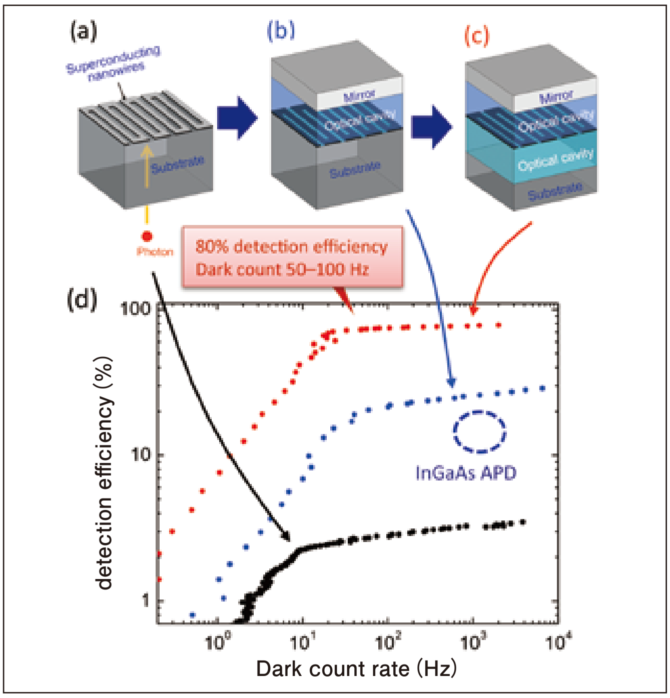


Figure 2　(a), (b), and (c): Superconducting nanowire device structure (d): Detector performance transition (dark count rate vs detection efficiency)

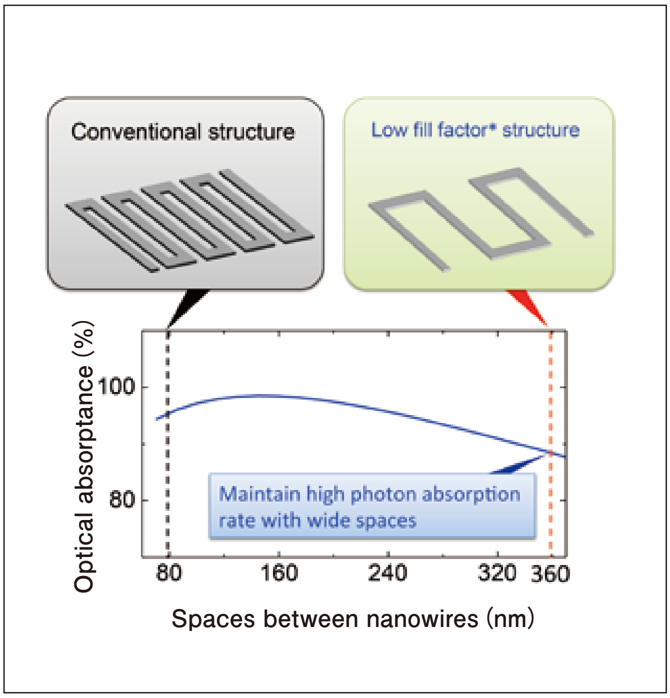


Figure 3　The simulated result of optical absorption rate to the SSPD device according to finite element analysis

＊ Low fill factor
The ratio of the nanowire width and the space between the nanowires is called fill factor. The larger the nanowires spaces, the lower the fill factor become.

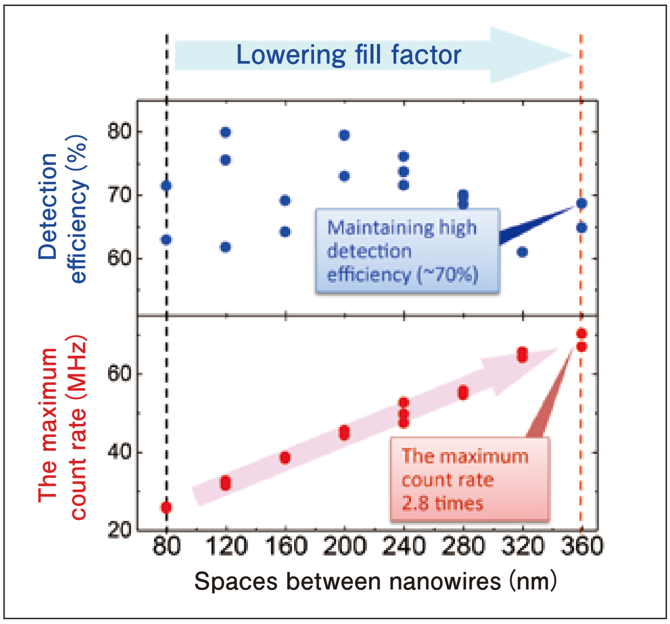


Figure 4　Performance evaluation results of the SSPD device having a space between different nanowires

Optimization of superconducting nanowires design by finite element analysis

In order to enhance the detection efficiency of the SSPD device, it is important to allow incident upon superconducting nanowire to efficiently receive photons by increasing the size of the active area. However, lengthening the superconducting nanowires to increase the size of the active area increase the inductance of the superconducting nanowire. Therefore, the dead time after detecting a photon becomes larger and the maximum count rate of SSPD (the maximum number of photons can be detected for a certain time) is reduced. With SSPD that we have developed, employing the structure in which the nanowire was sandwiched by the upper and lower optical cavity layers as described before, and thickening the nanowire about twice the thickness of the conventional nanowire, we have found that shortening the length of the nanowire (to increase the space between the nanowires) is possible while maintaining the light absorption efficiency high and light-receiving area wide. Figure 3 shows the relationship between optical absorption rate and spaces between nanowires simulated by the finite element analysis. In the conventional structure, space comparable to the width of the nanowires (80–100 nm or so) had to be taken, but in the new structure, you can see the high optical absorption rate of about 90% can be maintained while sufficiently widening the space between nanowires than those of conventional ones. In addition, Figure 4 shows the performance evaluation of SSPD element of space varying in practice. In SSPD element with 360 nm nanowires spacing, we succeeded in reducing the full length of nanowire while maintaining the detection efficiency in a high value of 69%, and achieved the maximum count rate of 70 MHz, 2.8 times faster than that of the conventional.

Future prospects

The significant improvement in response speed and detection efficiency made this time was the result of having the device installed on a small mechanical refrigeration system with an application history and in which operation is simple. The small mechanical refrigerating system is expected to cause large ripple effects, for it is capable of smooth application in various applied researches as mentioned above. This is because handling it does not require liquid helium which is expensive and difficult to cool. In NICT, we are currently working on advancing the function of photon number identification and further improvement of the performance of SSPD, the development of SSPD array are conducted. We believe that in the future, the application field of the SSPD will expand even more as the highest performance photon detector, and its importance would continue to grow.

XPIA, X.509 Certificate Public-key Investigation and Analysis System

Ryo NOJIMA

Senior Researcher, Security Fundamentals Laboratory, Network Security Research Institute

He joined NICT in 2006. He is mainly engaged in research about network security, especially in designing cryptographic protocol and public key cryptography. Ph.D. (Engineering).

Takashi KUROKAWA

Limited Term Technical Expert, Security Fundamentals Laboratory, Network Security Research Institute

He joined NICT in 2010. He is engaged in R&D about security evaluation of cryptographic technology.

Shiho MORIAI

Director of Security Fundamentals Laboratory, Network Security Research Institute

Graduated from University in 1993. After working for Nippon Telegraph and Telephone Corporation and Sony Corporation, she joined NICT in 2012. She is engaged in research about security evaluation and design of cryptographic technology as well as international standardization. Ph.D. (Engineering).

Introduction

We are conducting research and development of security technologies necessary for safe and secure information communication networks, especially we conduct research to enhance the credibility of Secure Socket Layer (SSL), the most widely deployed cryptographic protocol on the Internet. We would like to take this occasion to introduce XPIA (X.509 certificate Public-key Investigation and Analysis system) developed by NICT.

Background

Today, a vast amount of information is exchanged via networks as online services such as electronic commerce and online shopping became more popular. In websites providing such services, it is common to use HTTPS (Hypertext Transfer Protocol Secure) together with SSL. SSL is one of the most widely used protocols deployed to secure communication on the Internet. On the other hand, it has been reported that it contains various vulnerability issues in specifications and implementations including minor ones potentially exploited by attackers.

A team of researchers at University of California and University of Michigan reported a new threat against SSL in 2012, revealing risks of potentially exposing RSA secret keys of 20,000 SSL servers, an equivalent of 0.4 per cent of all SSL servers worldwide, which allows forging of SSL certificates. It has been an urgent challenge to grasp which SSL servers are insecure.

The new threat to RSA cryptosystem

The reported vulnerability of SSL has to do with RSA cryptosystem, the lifeline of SSL. RSA cryptosystem is a technology based on the difficulty of integer-factorization to support private communication between end-users and servers. The RSA factoring problem is to determine the p and q when two distinct prime numbers p and q, and N=pq are given. In RSA, N is referred as the public key, information that can be made public and be used ciphertext. The prime numbers p and q must remain secret to decrypt encrypted text. Therefore, when an attacker obtains the secret information p and q, one can decrypt all the messages between the user and the server. To operate SSL, RSA public key N is kept in each server. A user downloads N from the server prior to communication using SSL (Figure 1). To guarantee the security of a public key in each server, the public keys generated independently in each server are used. Since number of prime numbers is sufficiently large in theory, the use of the different public keys in all servers is expected. However, according to the aforementioned report, there are many cases where common p is used: $N_A=pq_A$ in server A is used as the public key and $N_B=pq_B$ is used as the public key in different server B. It is easy to obtain p, q_A and q_B by calculating the greatest common divisor of public key N_A and N_B where prime numbers are duplicate, allowing attackers to eavesdrop messages of server A and server B. At NICT, we have developed XPIA, a system to reveal the actual threat of such new methods of attacking and which SSL servers are insecure.

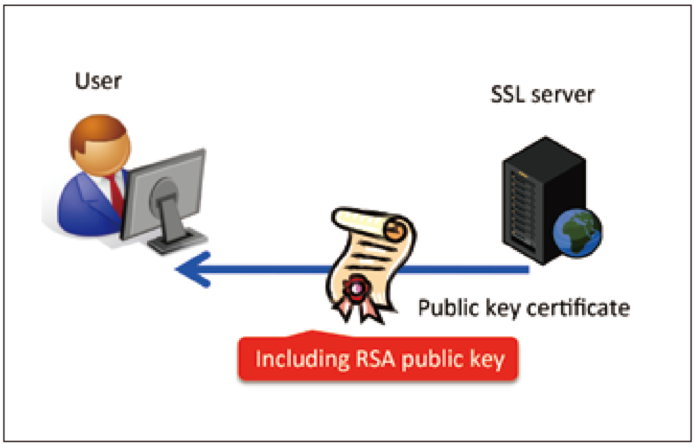


Figure 1　Downloading the certificate from SSL server

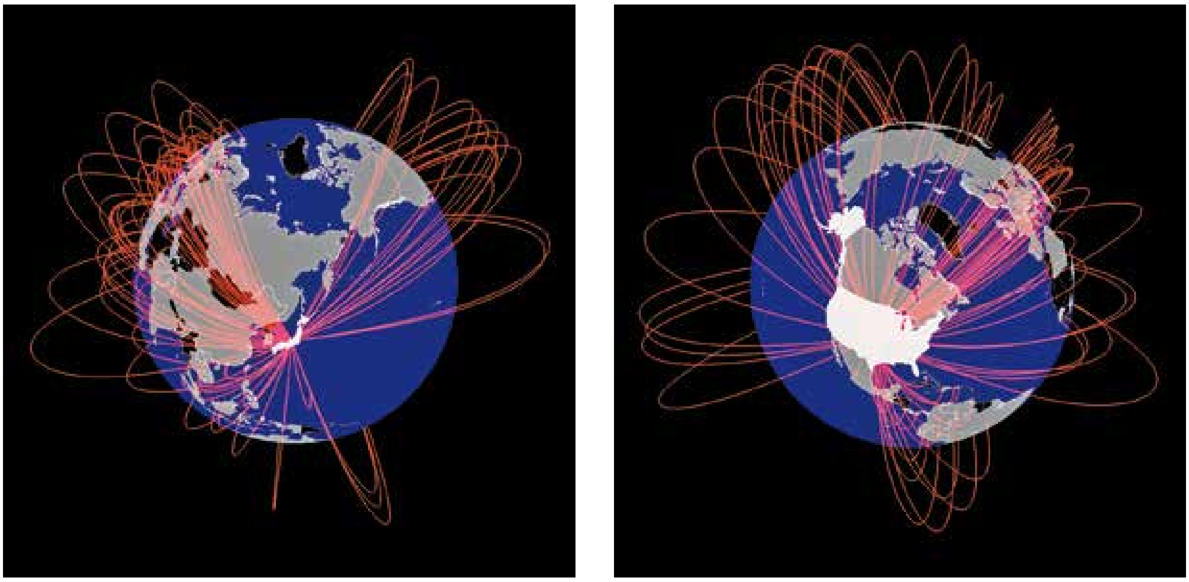


Figure 2　Example of vulnerability mapped by XPIA we developed

The framework of XPIA

1. Collecting public key certificate: By deploying a crawler, it connects to servers around the world and downloads public key certificates. We also used the public key certificates obtained by SSL Observatory*1 in this research.
2. Extracting of RSA public keys: It extracts the public key of RSA cryptography from the obtained public key certificate.
3. Analyzing RSA public key: It calculates the greatest common divisors of all the pairs of RSA public keys extracted from each server. When the greatest common divisor is not 1, it indicates that the pair contains common prime numbers and RSA public keys are factorable. With this process, the IP addresses of SSL servers using public key certificates and its corresponding factorable RSA public key can be obtained.
4. Visualization: Based on the information obtained by analyzing RSA public key, Figure 2 shows the pairs of SSL servers using RSA public key with common primes mapped in red lines.

Analysis result

According to our examination of vulnerability of RSA public keys extracted from public key certificates collected from SSL servers using XPIA, no service providers of online banking or online shopping sites using vulnerable public keys with factorizable prime numbers were found within the scope of this research. However, there are at least more than 2,600 SSL servers around the world using vulnerable public key as of October 2013 (Figure 3).

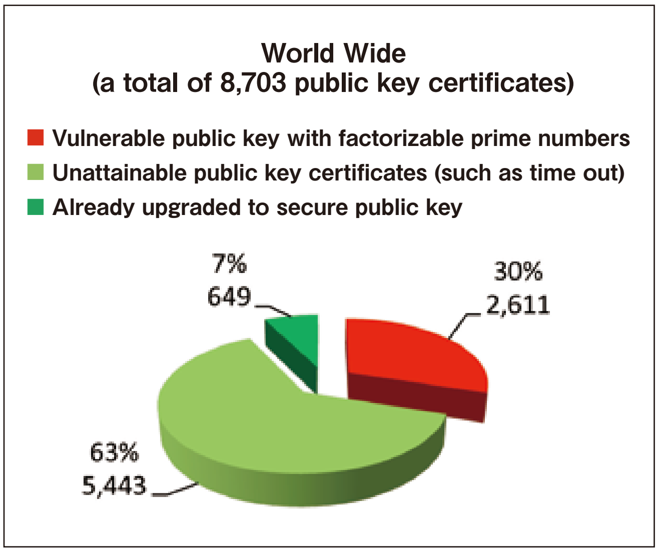


Figure 3　The latest condition of public key certificate with vulnerable public key

Future prospects

With XPIA, we grasped the actual threat of new attack method against SSL. We will advance research and development to extend the system to support to analyze BEAST attacks*2 and attacks against RC4*3, and secure network communication.

*1　SSL Observatory
The SSL Observatory is a project to investigate the public key certificate on the Internet by downloading datasets of all of the public key certificate publicly available on the IPv4 Internet

*2　BEAST attack
A kind of attacks that take advantage of the vulnerability of Cipher Block Chaining (CBC) in particular version of SSL.

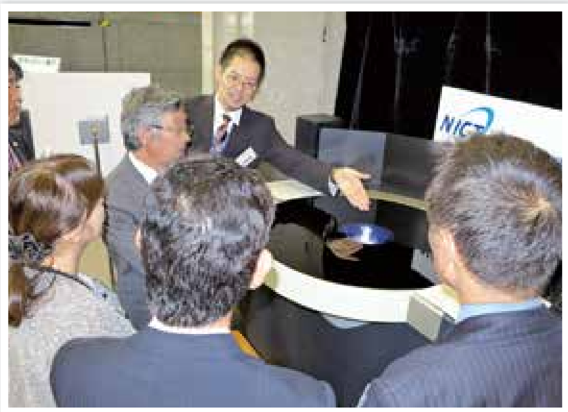
*3　RC4
One of the most widely used cryptographic technologies in the world developed by Ronald Rivest and adopted for SSL and wireless LAN protocol.

Report on "Keihanna Information and Communications Fair 2013"
—The future cultivated by Kansai Science City—

NICT Universal Communication Research Institute, in collaboration with information communication technology institutions in Kansai Science City, co-hosted the Keihanna Information and Communications Fair 2013 on November 7–9, 2013, as a collaborative community outreach event. Keihanna Information and Communication Fair is an annual event, and it was fifth this year. For three days of the event, a total of 3,600 participants visited the event where 13 lectures and exhibitions of 15 institutions were held. Nara Senior High School, a local high school, held the SSH (Super Science High School) event on the same time, just same as last year.

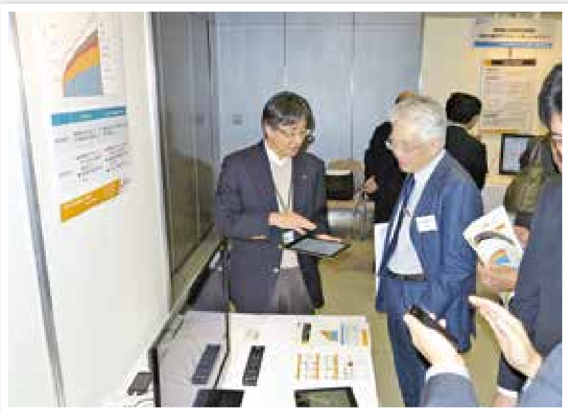
At NICT's lecture, Chiori HORI, Director of Spoken Language Communication Laboratory, Universal Communication Research Institute, gave a talk titled "The Spoken Language Communication Technoloty that Connects the World". In the exhibition session, we showcased "Kyomachi Seika", a mascot character of local town Seika-cho, on a glasses-free tabletop 3D display fVisiOn, and gave hands-on experience with remote controls of construction machines using the ultra-realistic system technology, as well as the demonstration of application software "KoeTra" for assisting communication. The event brought opportunities for people to experience the latest research achievements.

In addition, 210 people joined the event at "Umekita site" inside Knowledge Capital, Grand Front Osaka, where they enjoyed the live broadcast of the lectures and exhibitions from Kansai Science City in 4K ultra-high definition image. We also exhibited the program of "Kairyuouji-temple" using 200-inch glasses-free 3D image system, a collaborative work of NICT and the meeting for Kansai digital archives project established by Kansai Economic Federation, and welcomed 1,900 visitors.



Glasses-free tabletop 3D display (fVisiOn)

Multi-lingual speech translation app (VoiceTra4U)



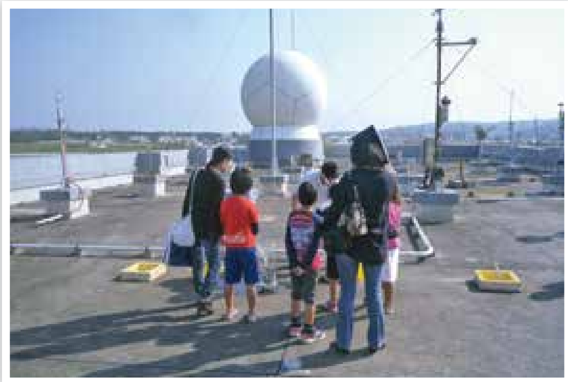
Demonstration of the application software "KoeTra" for assisting communication between hearing-impaired person and normal-hearing listener

Remote control of construction machines using the ultra-realistic system technology

Report on Facility Open House of Okinawa Electromagnetic Technology Center

NICT Okinawa Electromagnetic Technology Center held a facility open house on November 23, 2013. In addition to the introduction to the research of Okinawa Center and the guided facility tour, we showed observation images of Polarimetric and Interferometric Airborne Synthetic Aperture Radar System (Pi-SAR2), as well as images of global environment by Digital 4-Dimensional Globe and speed guns for participants to experience the principle of radar. And Okinawa Office of Telecommunications, Ministry of Internal Affairs and Communications, showcased the radio wave monitoring car and hands-on teach-ins of electronic handcraft. This time, we also conducted the demonstration dubbed "Aurora in the Tropical Island", and generated the light emission by applying high voltage to the gas in the glass container with reduced pressure. Many visitors enjoyed the visionary light emission. Blessed with fine weather, the open house welcomed more visitors than last year.

Children gazing at visionary lights of "Aurora in the Tropical Island"



Visitors listening to the explanation of the meteorological instrument installed on the rooftop

Report on Facility Open House of Kashima Space Technology Center

—Become familiar with the space!—

NICT Kashima Space Technology Center held a facility open house on November 23, 2013. Blessed with fine weather, more than 1,000 people visited the facility. Visitors showed special interests in the demonstration of communication systems helpful in times of disasters, and asked questions eagerly at the poster session of research for early detection of tsunami.

This year, we held sessions outdoor for visitors to find artificial satellites and experience the large-scale 34-meter antenna where they could climb and touch, which was unavailable last year due to disaster recovery efforts. Both sessions were popular and visitors lined up to participate these hands-on sessions.

"Looking for an artificial satellite" "Scavenger hunt"

"Climb and touch", the 34-meter antenna attracting the biggest audience

Report on NICT Open House 2013

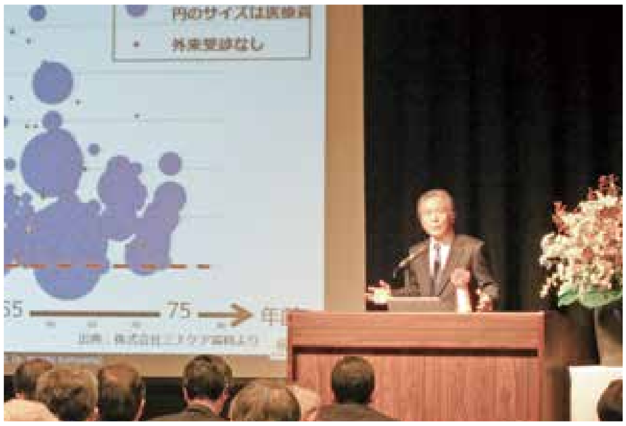
On November 28 and 29, 2013, NICT held "Open House NICT 2013". This event is subject to the demonstration, panel exhibitions, and lectures, and to introduce the latest research results of NICT under one roof, including the results of local research centers.

On the research results and research activities NICT is working on as well as R&D results of commissioned research, we held 16 talks, 58 demo panel displays, and a laboratory tour of 7 courses in the two-days, and we had a large number of visitors.

Opening Ceremony

At the opening ceremony of the first day, followed by the organizer's greeting of Masao SAKAUCHI, President of NICT, a special lecture entitled of "The 'Revitalization' for Japan —Platinum revolution by ICT—" was given by Dr. Hiroshi KOMIYAMA, President of Mitsubishi Research Institute, Inc./Special Adviser of the President, the University of Tokyo.

Snapshot of the opening ceremony



Special lecture by Dr. Komiyama

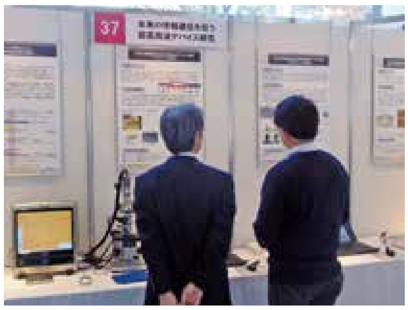
Snapshot of Exhibition Venues

Disaster-resilient network (NerveNet)

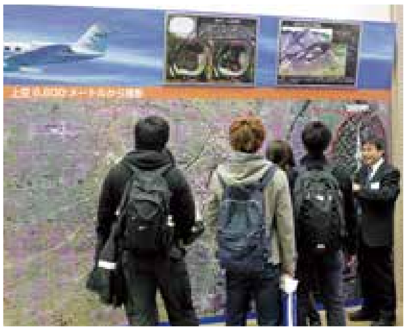
The world of high-precision time and frequency

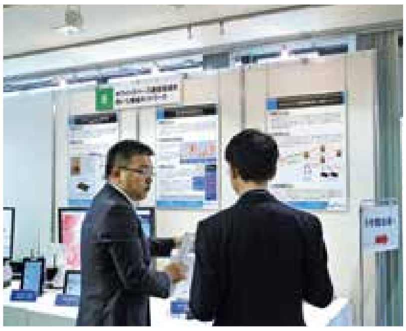
Experiencing the speed of Bolt by Five Senses Theater

Digital Olfactmeter
Experiencing the detection of odor

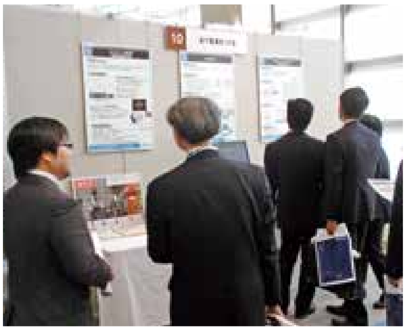


Research on ultra high frequency device


Observation of the ground surface using the airborne radar


Communication technology of White Space

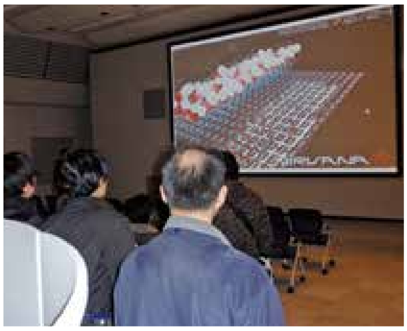

The booth on research related to information and neural networks


Making radio waves with light


Space Weather Forecast meeting


Demonstration test environment for research and development JGN-X/StarBED[3]


Radio relay system in times of disaster using the small unmanned aircraft


Cyber attack integrated analysis platform NIRVANA Kai

Snapshot of Laboratory Tour


Photonic Device Lab. (clean room)


Teraherz wave transmission/receiving system

Announcement of "Nano ICT Symposium 2014"

Admission free

~Social implementation of basic research results —towards the creation of innovative Information Communication Technology~

Date: January 29, 2014 13:00-17:00

Venue: Room 102, 1F, Conference Tower, Tokyo Big Sight

~ nano tech 2014 (The 13th International Nanotechnology Exhibition & Conference) symposium/seminar of nano week 2014 ~

Organized by: National Institute of Information and Communications Technology (NICT)

Overview

More than 10 years have passed since research and development of nanotechnology became full swing, and a variety of results have been put into practical use. However, most of the outcomes are the extension of existing technology. In order to create innovation by showing the true value of nanotechnology, it is important to create synergies through the integration of new material development with nanotechnology.

In this symposium, we will theme in the social implementation and deployment of the ICT commercialization technology of basic research results that combines nanotechnology and new materials, and introduce research results and future prospect from both sides of industrial application and basic research.

●Keynote lecture

Dr. Hideo HOSONO

(Professor of Tokyo Institute of Technology)

"Material Innovation Creating a Future —the Prospect of Transparent Oxide Electronics—"

●Lectures

As an example of practical application technologies, such as NICT embedded the result of basic research into the system, we picked up three following research areas,

1. **Electric-optic polymer devices for ultra-high-speed optical modulation**
2. **Quantum dot wide-band devices**
3. **Gallium oxide power devices**

Six lectures for each area will be presented by affiliate companies and NICT researchers to introduce basic research and development of practical application technologies.

Inquiry

For details, please contact Advanced ICT Research Institute, NICT. karc@ml.nict.go.jp

The Exhibition at "nano tech expo 2014"

NICT will attend the exhibition at nano tech 2014 to introduce high performance devices and systems with advanced features using nanotechnology or bio ICT as well as many results of research and development related to information and neural network.

We also hold an exhibition related to the lectures of nano ICT symposium, so please visit our exhibition.

Date: January 29-31 2014 10:00-17:00
Venue: East Hall 4, 5, and 6, Tokyo Big Sight
Details: Please visit nano tech 2014 website
http://www.nanotechexpo.jp/

Snapshot of the exhibition last year

Information for Readers

The next issue will feature New Generation Network Testbed JGN-X that NICT operates, and research and development utilizing the large-scale emulation environment StarBED^3.

NICT NEWS No.435, DEC 2013
ISSN 2187-4034 (Print)
ISSN 2187-4050 (Online)

Published by
Public Relations Department,
National Institute of Information and Communications Technology
<NICT NEWS URL> http://www.nict.go.jp/en/data/nict-news/

4-2-1 Nukui-Kitamachi, Koganei, Tokyo 184-8795, Japan
Tel: +81-42-327-5392 Fax: +81-42-327-7587
E-mail: publicity@nict.go.jp
<NICT URL> http://www.nict.go.jp/en/

〈Recycled Paper〉