# 4-2 Ubiquitous Communications Technology for Disaster Mitigation

**TAKIZAWA Osamu**

This paper describes ubiquitous communications technology for disaster mitigation.

***Keywords***
Disaster prevention, Ad hoc network, Sensor network, Public radio system, Firefighting

## 1 Introduction

Disasters may strike at any time. To remain prepared, it is important to take a practical approach to minimizing damage, given the available resources. The concept of "disaster mitigation"—rather than "disaster prevention"—has become established to describe this approach to policies in anticipation of disasters as well as subsequent rescue and recovery efforts. Unlike the concept of "disaster prevention", which has become somewhat of a catchphrase, "disaster mitigation" is focused on the practical matter of how to respond when disasters do occur.

Ubiquitous networks, meanwhile, are now being established for use in many different contexts, drawing on the increasingly pervasive presence of computers (hence the term "ubiquitous"). Communications technology in an age in which computers are everywhere is thus referred to as "ubiquitous communications technology". As used below, this phrase carries the added meaning of proven communications technology that can be used anywhere. Disasters represent one threat to society, and this technology is useful both in preventing and mitigating disaster damage.

In terms of preventative and mitigating ubiquitous communications technology, this paper mainly discusses two types of research in which the author has participated: research on widespread technology that can be used to secure means of data transmission during disasters, and research on the use of ubiquitous devices to gather information during disasters.

## 2 Disaster prevention and mitigation in context

### 2.1 Security and disaster prevention

The notion of security based on information and communications technology (ICT) calls to mind antivirus software and measures to prevent intrusion. These are methods of crime prevention in cyberspace. In contrast, the security equipment installed by security companies in homes is typically designed for real-world accidents and incidents alike. The equipment may include infrared systems or other means to detect intrusion to prevent crime, as well as smoke detectors and water leak sensors to prevent destructive events. In office buildings, emergency control centers work on a somewhat different principle. In many cases they address not only disaster control but also crime prevention, by monitoring access to buildings by employees. Preventing damage from disasters is thus linked with crime prevention, so broadly speaking, "security" covers a range of events from one purpose to the other. Table 1 classifies these elements within an overall concept of security.

In Table 1, the scope of item I extends to

**Table 1** Security, broadly conceived

| | Damage from natural calamities | Damage from intentional acts |
|---|---|---|
| Cyberspace | Ⅰ Countermeasures for obstructed communication and other damage | Ⅱ Network security and related policies |
| Everyday world | Ⅲ Prevention and mitigation of damage from disasters | Ⅳ Prevention of crime |

the use of conventional emergency communication. Item II corresponds to "information security" in a narrow sense, and includes measures against cyber-terrorism. For this special issue, we have selected papers focused on item II that also address issues relating to item I. In contrast, the Ubiquitous Communications Technology for Disaster Mitigation project discussed in this paper addresses R&D of ICT required for item III. Item III applies to the everyday world, leading to the inclusion of R&D incorporating knowledge from fields such as social psychology and behavioral science.

### 2.2 Environmental monitoring and prevention of damage from disasters

The relationship between security and the prevention of damage from disasters was introduced above, but from a different point of view, we must also consider the relationship between environmental monitoring and these preventative efforts. Indeed, one researcher has indicated that environmental monitoring and prevention overlap in many ways when viewed from the standpoint of ubiquitous communications technology[1]. For example, environmental monitoring equipment must often be operated without reliance on public networks—outdoors, for example, at sites without electricity. This resembles our predicament when communication is obstructed during disasters. In other words, we can apply the same technology routinely for environmental measures as for disaster management during emergencies. Global warming, representative of environmental problems, can be described as a calamity on a global scale that is taking place very gradually. These issues have given rise to a trend that is quite new, even among research organizations: dealing with environmental monitoring and prevention of damage from disasters as a compound issue. In fact, academic departments have been or are being established to reflect this approach, such as the College of Environment & Disaster Research at Fuji Tokoha University (the first of its kind in Japan) and a similar academic department at Kansai University.

## 3 Securing means of data transmission during disasters

Telecommunications providers are responsible for maintaining communication channels even in the event of large-scale disasters. However, during such disasters, communication is often completely obstructed. The obstruction can be traced to congestion or physical damage, such as severed lines; if the cause is physical damage, this can involve breaks in the lines between subscribers and the telephone station, or severed backbone circuits between telephone stations. Although congestion occurs most often during disasters, the backbone circuit between telephone stations is rarely cut off, except in cases of particularly severe disaster. Thus, we must clearly distinguish causes of obstruction when considering the likelihood of occurrence and our options for countermeasures. In this section, we describe various strategies to secure communications (particularly data transmission) through independent means if provider communication lines are somehow damaged in a disaster.

If the existing communications infrastructure is damaged in some areas by natural disasters or otherwise, wireless or radio communication can be useful in that lines can be secured by deploying communication equipment at the affected sites without the need to lay new cables. Even during severe disasters in which communication lines are severed and cannot be repaired immediately, alternative means can be established (such as deploying terrestrial equipment for a satellite connection) to enable a relatively prompt recovery of lines. On the other hand, terrestrial equipment for wireless communication consumes less energy for antenna power than land-based satellite communications equipment, which enables operation under lower power. This is a great advantage during disasters, in which the power grid is frequently down along with the communications infrastructure.

Thus, in this section, we discuss various techniques for data transmission using familiar, nearby terrestrial wireless equipment in major disasters.

### 3.1 Using long-distance wireless LAN to secure communications channels during disasters

Low-power data transmission systems for digital communication between computers connected wirelessly (referred to hereinafter as "wireless LANs") mainly transmit radio waves on the ISM band at 2.4 GHz. They are primarily used when connecting local area computers within a radius of several dozen meters to a wired network infrastructure. However, communication between access points several kilometers apart is possible via long-distance wireless LANs equipped with a certified external antenna (specifically, an antenna granted what is known as "Technical Standard Conformity Certification" in Japan). This equipment, which does not require an operator's license and can be set up by anyone, can be used immediately after installation. Long-distance wireless LANs can thus provide independent lines if the public network is disabled in a disaster. For these purposes, research has been conducted on the use of long-distance wireless LANs as a means to link fire department headquarters and disasters sites in large-scale disasters[2]. Other research focuses on systems to support information exchange (entering survival information and transmitting it to servers outside the affected site), using wireless LAN equipment normally stored at secure places but transported and installed at affected sites during disasters[3].

Over the five years from 1999 to 2004, the author collaborated with a local university in Wakkanai, Hokkaido to implement a research project on network equipment for information exchange (Fig.1). This was an independent network ("Wakkanai Information Network Equipment"), with a long-distance wireless LAN set up at the radio observation facility of NICT. In the project, local junior and senior high schools were selected as hypothetical shelters, from which access was investigated. For details on network development and results, refer to cited reference 4.

Wakkanai is located in a harsh natural environment along the Soya Strait, in a snowy region that is also one of Japan's windiest areas. The effect of cold weather, snowfall, and strong wind on the antenna and radio conditions cannot be disregarded in wireless digital communications over high frequencies. Thus, one purpose of the project was to verify the feasibility of using independent radio to secure a communication channel during disasters in this harsh environment. In contrast, conditions in populous cities pose a great risk of interference with transmissions over the ISM band, due to the use of microwave ovens and other devices. Thus, the practicality of long-distance wireless LANs in large cities is being verified in a study using a permanent

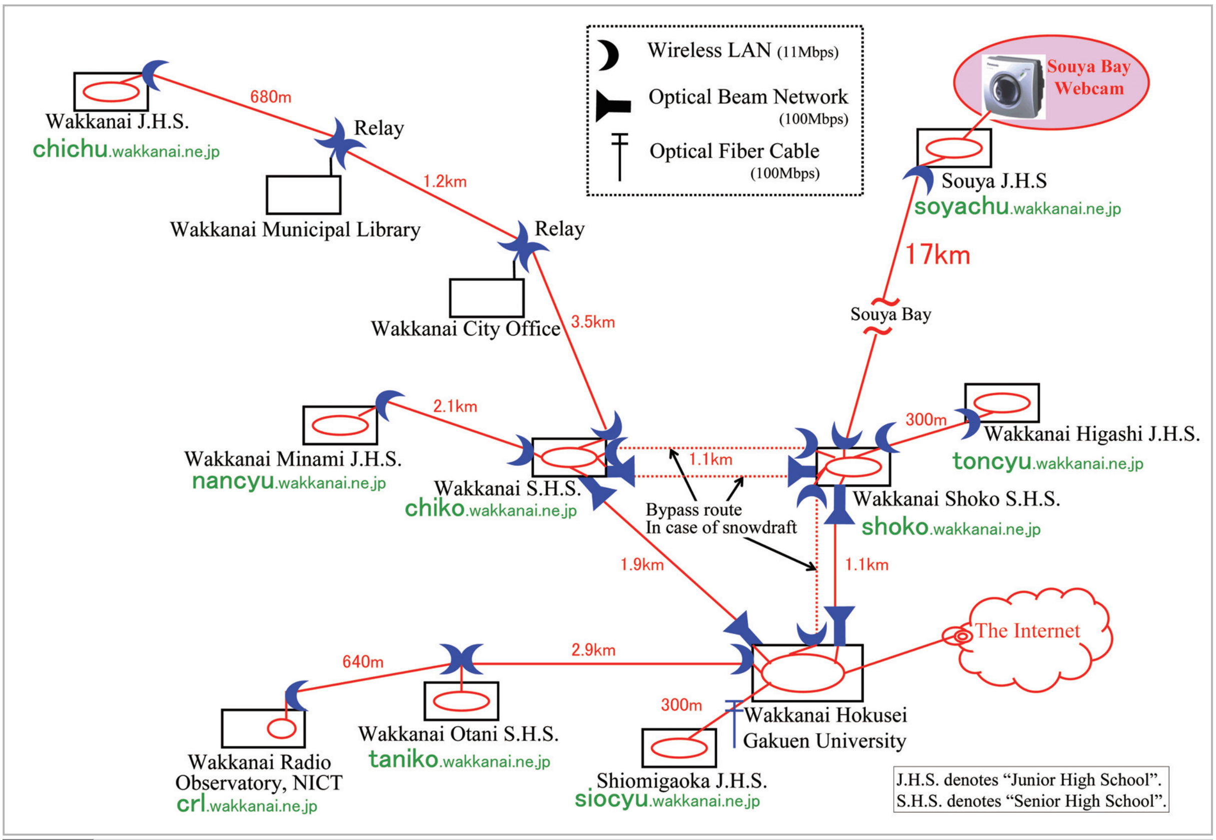


**Fig.1** Connection diagram for the “Wakkanai Information Network Equipment” project [4]

**Fig.2** Long-distance wireless LAN antennas installed at NRIFD (left) and NICT (right)

long-distance wireless LAN set up in 2002 between NICT Koganei Headquarters and the National Research Institute of Fire and Disaster (NRIFD) in Mitaka, Tokyo, 7.8 km away. Figure 2 shows the long-distance wireless LAN antennas at each site, and Fig.2b presents an image from the webcam installed at NRIFD, received at NICT.

## 3.2 IP communication via emergency digital PA radio on the 60-MHz band

### *3.2.1 Overview*

Throughout Japan, emergency PA radios operating on the 60-MHz band have been set up by local governments as a means of warning local residents promptly over loudspeakers in the event of disaster. Municipalities former-

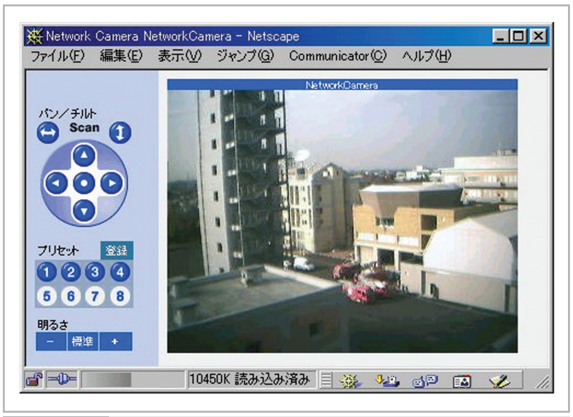


**Fig.2b** Image from the webcam installed at NRIFD, received at NICT

ly used analog systems, which mainly involved simplex public address from emergency management centers (the master station) through loudspeakers (the slave station). The adoption of digital technology starting in FY 2001 led to new functions and more robust systems, with bidirectional or multi-channel communication, data transmission, and other features. Soon after emergency digital PA radios were deployed, surveys of their effectiveness began at local bureaus of telecommunications of the Ministry of Internal Affairs and Communications (MIC). However, tests on communication using the standard protocol for digital communication—i.e., Internet Protocol (IP)—largely have yet to be implemented, as explained below.

At the Hokuriku Bureau of Telecommunications, a research committee was formed in FY 2003 to study general IP radio communications systems. The committee tested IP communication over a digital multi-channel access (MCA) system at 800 MHz and with mobile digital PA radios for emergency use[5]. However, IP communication was not conducted over emergency PA radios on the 60-MHz band.

At the Shikoku Bureau of Telecommunications, a research committee was formed in FY 2003 to study support systems that provide disaster information. This committee conducted verification testing on providing “disaster information over IP” using mobile IP equipment[6]. However, these experiments were focused on a regional IP network used with emergency PA radios on the 60-MHz band, not IP communication over emergency PA radio.

At the Chugoku Bureau of Telecommunications, a research committee was formed in FY 2002 to study the use of emergency digital PA radio over a broad area. This committee investigated the potential of wide-area emergency digital PA radio through data transmission experiments, and studied the difficulties involved[7]. However, instead of using emergency PA radios on the 60-MHz band, these experiments were focused exclusively on viewing MS Excel files that were originally on a web server connected to the master station, but ultimately viewed over the onsite LAN after uploading from the slave station via a serial connection (RS-232C). IP communication between the master and slave stations was not performed.

Since initial institutional deployment of emergency PA radio equipment in 2001, manufacturers of this equipment have commercialized a number of digital 60-MHz band systems, providing them to local governments in various regions. However, to date virtually none of these systems support IP communication from the slave station, with the exception of one system delivered to Kashimo village in Gifu prefecture (incorporated into Nakatsugawa city in February 13, 2005) by Fujitsu General Ltd. This system is one of the very few that is equipped with a LAN interface for an outdoor slave station, allowing transmission via e-mail and the gathering of information through Web during and after a disaster.

There are a few reasons that we find only few examples of IP communication testing between a master and slave station using emergency PA radio on the 60-MHz band. First, the transfer rate is slow (45 kbps or less). Second, under the radio station licensing system, accessing networks (inducing the Internet) operated by unlicensed administrators with emergency PA radios is not permitted. Thus, there was little advantage in developing support for IP communication. However, if IP communication is enabled from the slave station, “information outlets” can be established at schools, community centers, and other sites at which slave stations are installed. For example, if disaster control personnel cannot reach an isolated region after a large-scale disaster, local residents can connect to the slave station from a personal computer, enabling easy exchange of information with the master station and local government intranets through general means such as email. The real potential of this system lies in supporting the exchange of emergency information in large-scale disasters.

To test IP communication on emergency digital PA radios on the 60-MHz band, the author participated in a public experiment on a system for gathering disaster information conducted by the Kinki Bureau of Telecommunications in Kainan, Wakayama in February 2005[8].

### 3.2.2 System configuration

Time-division multiplexing of this emergency digital PA radio on the 60-MHz band involves dividing one frame (80 ms) into six slots, of which two slots are control data for transmissions between the master and slave stations. The IP communication experiment focused on duplex operation in which two slots each of the remaining four slots were allotted for upstream and downstream data transmission and error correction. Thus, one slot was used for data transmission. The ideal transmission rate was 6.4 kbps.

The configuration of the test system is shown in Fig.3. Emergency digital PA radios on the 60-MHz band were used as the test equipment (Oki Electric Industry Co., Ltd.; Fig.3b). These were connected to the master station (at the hypothetical emergency control center) and slave station (at the hypothetical shelter) by Ethernet/RS-485 converters, which converted the IP for serial transfer. The master station was installed at the Kainan Social Welfare Conference Center (on the second floor) and the slave station at Kainan City Hall (in the fifth-floor conference room). Indoor rod antennas were set up by the windows (Fig.3c). The stations were approximately 100 m apart. Figure 4 shows the Ethernet/RS-485 converter developed for this experiment. In addition to supporting Ethernet/RS-485 conversion, this converter is equipped with an interface for transmitting still images and sensor information (regarding structural collapse, fire, and flooding) from a concurrent public experiment.

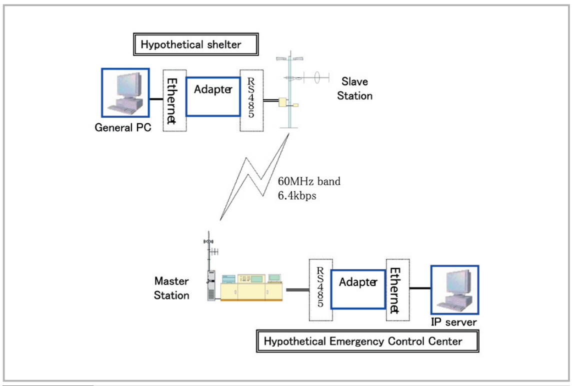


**Fig.3** System configuration in an experiment on IP communication using emergency digital PA radios on the 60-MHz band


**Fig.3b** Master radio station at the emergency control center Manufactured by Oki Electric Industry Co., Ltd.

Fig.3c Rod antenna
At the Kainan Social Welfare Conference Center


Fig.4 Ethernet/RS-485 converter

The transmission rate is slow with emergency digital PA radio on the 60-MHz band, so on the client computer, the maximum transmission unit (MTU) was changed to 130 bytes and receive window (RWIN) to 450 bytes. Regarding MaxDupAcks, to keep exchanges at a minimum, the regular setting of “3” was changed to “1” for the experiment. To secure as much bandwidth as possible, broadcasts were not supported, mainly to eliminate ARP signals. Thus, the client computer’s IP address was not assigned automatically via DHCP; a static address was used for the connection instead. Accordingly, this experiment did not recreate the ideal situation, in which users can establish a connection with their regular computer for immediate IP communication.

### 3.2.3 Test items and results

(1) Entering and displaying entries in a personal information database

One test was focused on entering and displaying personal information (including hypothetical disaster victims) in the emergency control center database from the shelter. Users at the shelter launched a web browser on the client computer there to access the server computer at the emergency control center. First, users accessed the server from the client and downloaded a registration screen. This involved double-clicking on an icon on the client desktop to launch the web browser, after which users accessed the server and downloaded the screen as noted above. Seven seconds elapsed after double-clicking on the icon before the registration screen was displayed. Next, required information was entered on this registration screen. Users clicked a button on the registration screen for personal information to enter information in the database on the server. Here, nine seconds elapsed after clicking the button until registration was complete. Last, users clicked a button on the registration screen for personal information to view a list, after which a list of registered data in the server database was displayed. After users registered information for 10 records from client to server, they clicked the view button to download the data list from the server, which took five seconds. Fig.5 shows the screens displayed in this experiment for entering and viewing personal information.

(2) Sending email messages

In another test, the server at the emergency control center was used as a mail server accessed by the client at the shelter for email exchanges between the shelter and the emergency control center. For a message of 200 kanji characters (a little less than 100 words), 14 seconds elapsed after clicking the send but-

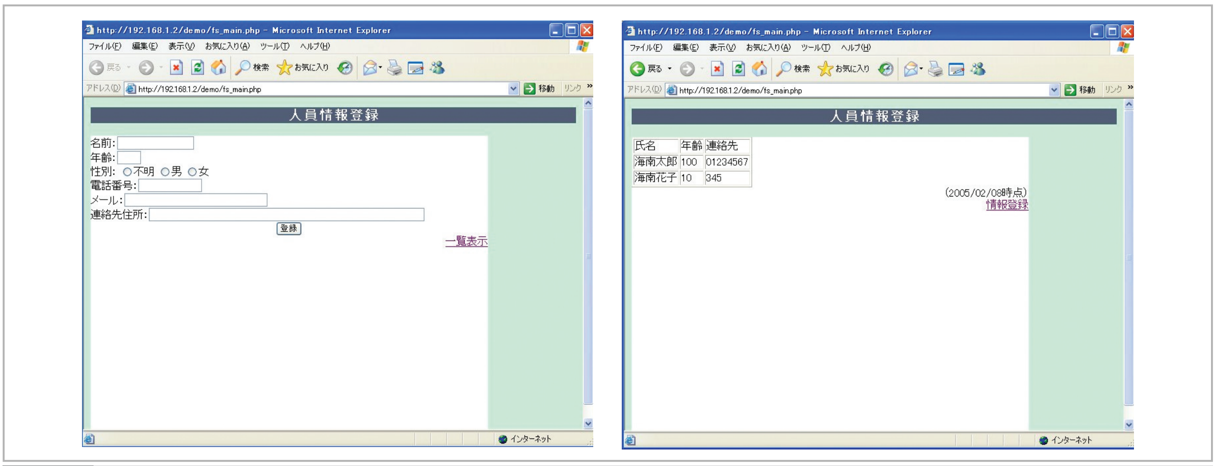


**Fig.5** Screens for entering and viewing personal information (left: registration screen; right: display screen)

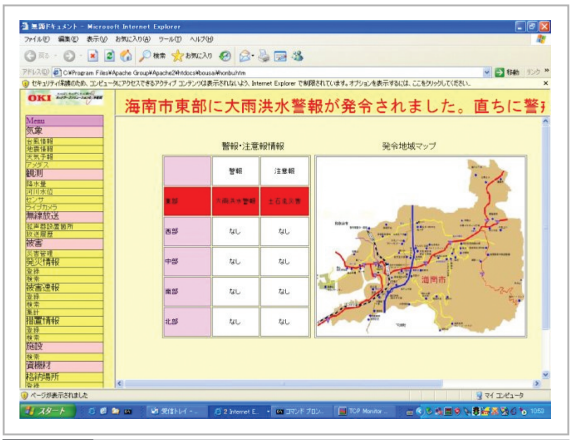


**Fig.6** Multimedia content used in this experiment

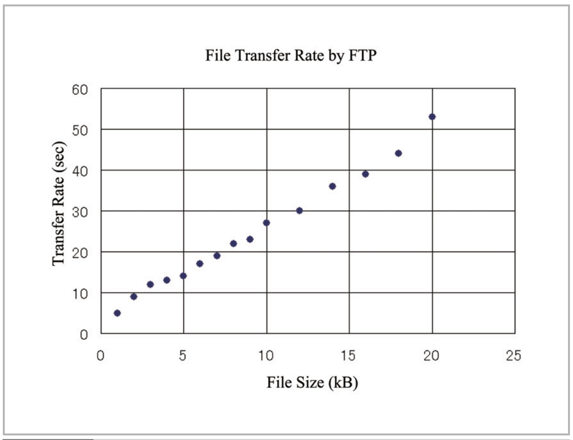


**Fig.7** Relationship of file size to transfer time in FTP transfers

ton of the email software on the client before the message was delivered.

(3) Viewing multimedia websites

Web browsing was the subject of another test. The server at the emergency control center was used as a web server accessed by the client computer at the shelter to display multimedia online content, including webpages with images. Users double-clicked on a shortcut icon on the desktop of client computer to download and view a webpage on the client computer. Figure 6 shows the displayed multimedia content. In this case, two minutes and three seconds elapsed after double-clicking on the shortcut icon before the webpage was displayed.

(4) Transferring files via FTP

In the final experiment, the server at the emergency control center was used as an FTP server accessed by the client computer at the shelter to browse files on the server and download the files to the client computer. Users launched FTP software on the client computer and designated a folder on the server for the connection. This presented a list of files in the selected folder on the server. Users chose a file from the list to download and dragged the file to a folder onto the client computer to begin downloading. Figure 7 shows the resulting transfer time for text files, with the file size plotted against time.

According to Fig.7, the average transmission rate was 2.96 kbps, a performance of less than half of the ideal value of 6.4 kbps.

#### 3.2.4 Survey results

Participants were given a questionnaire regarding this public experiment on IP communication. The distribution of respondent affiliation is shown in Table 2. Over half of the respondents were private citizens.

**Table 2** *Breakdown of respondent affiliation*

| | |
|---|---|
| National or regional government workers (involved with disaster control) | 13 |
| National or regional government workers (not involved with disaster control) | 8 |
| Private citizens | 32 |
| Others | 5 |

Table 3 shows the results of responses to the question "Do you think it is beneficial to enable IP communication from the slave station of a permanently installed emergency digital PA radio?" Approximately 80% responded that it was beneficial.

**Table 3** *Responses regarding the benefit of enabling IP communication*

| | |
|---|---|
| Greatly beneficial | 23 |
| Beneficial | 22 |
| Cannot say one way or another | 9 |
| Not very beneficial | 2 |
| Essentially no benefit at all | 0 |

Addressing the responses in Table 3, an open-ended question was posed regarding the ways in which IP communication may or may not be helpful. The results are as follows. Of particular note in these replies are the opinions on specific uses, as well as comments on the sluggishness of the transmission rate.

- As a means of conveying information during disasters (when information might only be available over the emergency radio broadcast system or radio)
- The widespread popularity of computers has made text-based data quite common, so IP communication is quite important during disasters.
- Who would use the system depends on where slave stations are installed, so who would use this system? It would be helpful to clarify how the radio stations would be operated.
- We must account for the worst-case scenario for systems during disasters. In this case, I do not think systems requiring electrical power, such as those for IP communication, would be very useful. If people rely too much on such systems, there would be even more chaos during disasters if they are unavailable.
- For gathering needed information at shelters (safety status, essential resources, and so on)
- For exchanging information via email
- Clarify the advantages of enabling IP
- Information would be detailed (real responses from local residents), but few people could operate the system (and it would probably be too difficult for seniors).
- During emergencies or disasters, we assume that phones will be unavailable, so it would be useful for collecting and exchanging information with areas outside the affected site.
- We must enable data transmission from computers during disasters.
- The slow speed poses a problem.
- It would be desirable to have needed information available to check on the slave station as well.
- We can foresee large volumes of data, so it would be better to provide a variety of communication methods.
- The solution should be essentially device-independent (any computer could be used, for example).
- The key is organizing the information and enabling operation by anyone, anytime.
- It would be helpful during disasters if ease of use when communicating with the outside was equivalent to that during normal use.
- Ought to enable anyone, anywhere to access the information online anytime
- Use broadcasts
- Ought to enable access with everyday devices
- I think existing technology can be used, eventually for conveying information to and from local residents.

**Table 4** Responses regarding desired uses (multiple responses accepted)

| | |
|---|---|
| Exchanging information via email | 29 |
| Obtaining information by browsing the web or accessing databases | 34 |
| Sending information, such as by posting messages on online bulletin boards | 36 |
| Transferring files via FTP | 8 |
| Accessing the local government intranet | 20 |
| Others | 2<br>Sharing and viewing information on the disaster, rescue efforts, and safety status<br>Information and status of public offices and institutions |

- Greater possibilities for use must be imagined in advance, not in 20/20 hindsight
- I think it will be useful for supplemental information conveyed from disaster sites, for example.
- Ought to allow for use with everyday devices, such as regular computers
- Useful because it can be linked with computer data
- Should provide information on safety status and the like, to let others know what is currently needed at the shelter and what is not
- If the transmission rate were a bit faster, the system could handle large amounts of data.

Table 4 shows responses to a question regarding the desired types of uses if IP communication is enabled from the slave station of a permanently installed emergency digital PA radio. Most respondents indicated the desire to use applications for typical IP communication activities, such as for email and web browsing.

The above survey results indicate that ordinary citizens can appreciate the benefits of adopting emergency digital PA radio on the 60-MHz band for IP use.

#### 3.2.5 Discussion

From this experiment, we determined that despite the slow transmission rate of emergency digital PA radio on the 60-MHz band, it is possible to exchange text-based email or enter information on text-based web pages and browse them without undue difficulty. In addition, many respondents liked the idea of being able to use familiar IP-based applications as usual. But unlike the rough transmission method of this experiment—converting Ethernet signals for serial communication (RS-485) over a radio channel—further research should investigate more effective transmission methods.

### 3.3 Simple data transmission using voice transceivers [9]

#### 3.3.1 Overview

In addition to applications for permanently installed means of data transmission such as radio stations (including long-distance wireless LANs and emergency PA radio as described above), we need to consider terrestrial data transmission systems that can be used on an urgent or supplemental basis immediately after disasters. When applying such systems for emergency transmission, particular care should be taken in considering the use of general radio terminals for a different purpose—as data transmission terminals—promptly after disasters occur. Thus, with respect to data transmission during disasters, this section discusses the feasibility of reconfiguring two types of voice transceivers widely used as radio terminals: amateur radio sets and radio sets classified as “Voice Communication Radio Equipment for Specified Low Power Radio Stations” (ARIB STD-20).

After large-scale disasters, the communications infrastructure is typically disabled in an essentially localized area, excluding widespread damage from subsequent congestion. In the case of the Great Hanshin-Awaji Earthquake, the infrastructure was probably disabled in a radius of approximately 20 km at most. Thus, a distance of 20 km can serve as a guideline for radio transmission to convey information from affected sites to areas in which the existing communications infrastructure is intact.

#### 3.3.2 Simple data transmission using amateur radio sets

Amateur radio has long been used as a means of communication in emergencies. For one thing, radio terminals have become widely popular, and for transmissions of approximately 20 km, the VHF and UHF bands are sufficient. Since 1998, "phone patches" have been authorized for use in Japan, which enable amateur radio users to connect to telephone networks. Thus, if users in a disaster zone can connect via radio to outlying areas in which the telephone network is intact, radio-set base stations outside the affected site can be connected to the telephone network to enable data exchange with the remote site. In other words, these radio links can be viewed as a means of extending telephone lines.

Packet radio has long been studied as a means of amateur radio data transmission. This technology is governed by its own protocol, AX.25. Additional research has also focused on wireless fax transmission. However, packet radio modems (terminal node controllers, or TNCs) and wireless fax interfaces are specialized peripheral devices, only in use among certain amateur radio enthusiasts interested in experimentation. These devices are thus unsuitable as a means to divert numerous radio terminals in cities during disasters. On the other hand, more amateur radio sets have recently been equipped with a function to transmit DTMF codes (touchtone codes), and many of these models even have a built-in numeric keypad for sending these codes. Our research was thus conducted to implement simple data transmission through the use of voice transceivers for transmission of DTMF codes. Figure 8 is a schematic diagram showing communication between a voice transceiver and data server using DTMF codes. The data server in this case is assumed to be equipped with an interface for connection to the telephone network and data transmission based on DTMF codes.

As for operation on the mobile station at the affected site, users enter DTMF codes for a command to take the base station telephone off the hook, to dial the access point of the data server, and, using additional DTMF codes, to transmit the data.

It is evident that amateur radio sets can support voice calls at a distance of 20 km without difficulty, but it was necessary to determine through testing whether DTMF codes from the phone patch could be consistently recognized. Thus, with the cooperation of amateur radio stations IAA Radio Club (JO1ZVH) and IAA Kansai Radio Club (JR3ZVA), we conducted an experiment on data transmission using this system. The appearance of the experimental system is shown in Fig.9. Telephones support full duplex communication, but for purposes of this experiment, half duplex communication was used (as typical in amateur radio communication). If communication with the data server is simply a back-and-forth session, half duplex communication is sufficient.

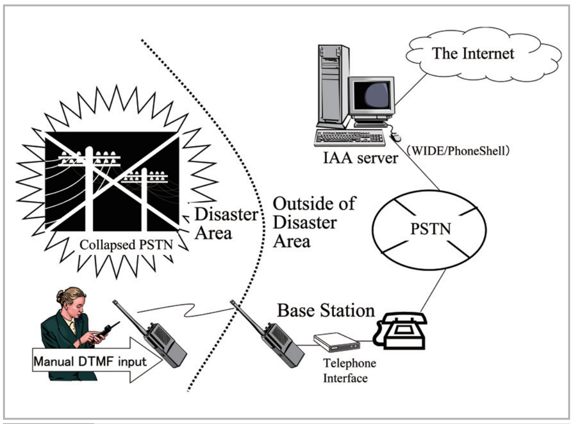


**Fig.8** *Schematic diagram of simple data transmission from an amateur radio voice transceiver using DTMF codes*

The experiment was conducted over FM at 430 MHz. The 430-MHz band was chosen due to its popularity on mobile transceivers, and FM was chosen because a modulation method with good tone quality provides more accurate transmission of DTMF codes. The base station was installed at NICT Koganei Headquarters (in Koganei, Tokyo). The base station antenna height was approximately 20 m, placed on the roof of a four-story building. Meanwhile, the mobile station at the location serving as the affected site was operated in Akishima, Tokyo, at a height of 15 m (on the balcony of a fourth-floor condominium). The stations were approximately 10 km apart. Antenna


**Fig.9** *One set of experimental equipment for simple data transmission using an amateur radio to transmit DTMF codes*

Left: radio set for the mobile station at the affected site (equipped with a numeric keypad for transmitting DTMF codes); top right: radio set for the base station outside the affected area; bottom right: telephone interface equipment for the phone patch

power of approximately 4.5 W was used for the mobile station at the affected site.

The results of the experiment confirmed that DTMF codes could be successfully sent from the mobile station at the affected site to place a call from the telephone at the base station.

As for the telephone interface (KTI-12, manufactured by Kenwood Corporation), under the terminal device conformity certification, output was limited to DTMF codes from voice or manual operations, so for the experiment, DTMF codes were produced manually. However, simple data transmission requires mechanical transmission and reception of DTMF codes. Thus, further investigation is required on resolving the applicable legal restrictions. Furthermore, because the data transmission rate of DTMF codes varies depending on sound separation performance, verification is required of the effect on transmission rate of sound-quality loss over the radio channel and telephone line.

#### 3.3.3 Simple data transmission using radio telephony from specified low-power radio stations

For amateur radio in Japan, certification for operation and a radio station license are required. Communications are not for business use—they are restricted to amateur radio content. However, no license or certification is required for equipment under the category of “Voice Communication Radio Equipment for Specified Low Power Radio Stations” (this equipment is referred to below as “specified low-power radio stations”), and there are no restrictions on use. Radio telephony for specified low-power radio stations is assigned to the 420–440 MHz band. Many such terminals can be found in cities, where they are used at construction sites, restaurants, and the like to relay instructions and orders. Communication is conducted over FM with an antenna power of 0.01 W. Relaying via repeater is permitted.

As for the types of specified low-power radio stations, various standards have been established for different uses, such as data transmission or telecontrol (as described in ARIB STD-T67). Thus, for data transmission, terminals conforming to these standards may be used. However, the terminals that have become most popular in Japanese cities are for radio telephony (conforming to ARIB STD-20). Accordingly, as in our experiment using amateur radio, we investigated simple data transmission by sending DTMF codes through radio telephony using specified low-power radio stations. No radio telephony transceivers that can transmit DTMF codes are currently available with specified low-power radio stations. We thus resorted to generating DTMF codes with a separate device and sending the tones through the transceiver microphone. A schematic diagram is shown in Fig.10 for this method of simple data transmission using radio telephony with specified low-power radio stations. Because phone patches are not authorized for radio telephony with specified low-power radio stations, the radio set of the base station is assumed to be directly connected to the data server, as shown in Fig.10. Use of a repeater is also assumed, for a longer transmission distance.

We first tested the maximum transmission distance of the system. To investigate the suc-

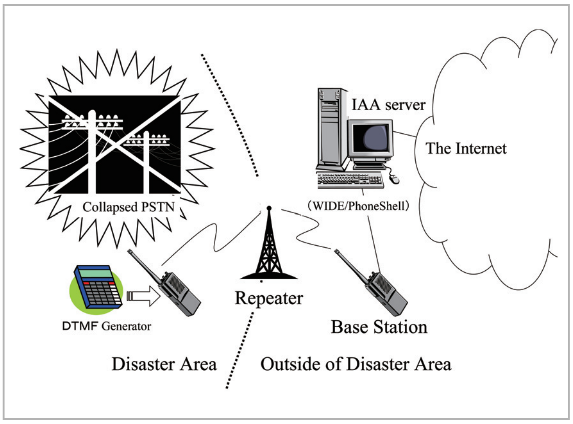


**Fig.10** *Schematic diagram of simple, DTMF code-based data transmission using a specified low-power radio station transceiver*

cess or failure of transmission, we tested activation of the repeater by transmitting tone squelch from the mobile station to the repeater to determine whether or not the repeater was launched. Tone squelch refers to injecting one sound (a tone signal) out of 38 varieties (e.g., a 60-Hz tone) into an audio signal. This sound is detected after reception to control operation, as a means of limiting calls to the party involved. Tone squelch is a standard feature of radio telephony with specified low-power radio stations. Repeater startup is controlled when the tone signal in the carrier is detected. If radio waves are weak and the tone signal cannot be detected, the repeater is not activated even if the radio waves reach the receiver. Tone squelch resembles DTMF control in that both control operation through detection of sounds. Thus, if radio waves are strong enough to trigger the repeater, we can infer that DTMF codes are likely to be recognized.

We tested access (that is, repeater startup) with respect to a repeater installed on top of the tower at a height of 60 m at NICT Koganei Headquarters (in Koganei, Tokyo) from transmissions in the vicinity. The repeater and tower are shown in Fig.11.

Results of the access experiment are given in Table 5. Access was successful from pedestrian overpasses and at other positions with a clear line of sight in Mitaka, Musashino, Tachikawa, Akishima, Hino, and Hachioji. The transmission distance of radio telephony with specified low-power radio stations in urban areas is generally expected to be approximately 1 km. This experiment demonstrated that if one terminal (the repeater) is raised and the other is at a position within a relatively clear line of sight, transmission is possible from approximately 10 km, even in urban areas. Furthermore, placing a repeater between terminals on both sides (as shown in Fig.11) not only increases inter-terminal transmission distance several-fold, but this arrangement enables communication even if both terminals are not in high positions (given a relatively clear line of sight). From the experimental results, we determined that transmission at 20 km, the objective in Section **3.3.1**, was feasible.

Next, on the roof of a nine-story building by the North Exit of JR Tachikawa Station (approximately 6.8 km from the repeater) we conducted an experiment using a computer to generate and transmit DTMF codes, which were received at the same location from which the repeater transmitted the relayed signals, for recognition of these codes on a computer at the same location. Thus the round-trip transmission distance was 13.6 km (6.8 km × 2). DTMF codes were generated and recognized using a software program of DTMF Controller 1.1c[10]. The DTMF code string used in this experiment consisted of five pound signs (#) followed by a random string of 50 codes of twelve types: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, *, or #. The random code string was produced using RANer, a software application that generates random number sequences[11]. The DTMF code string for the experiment is shown below.

#####*10470#83532#54546#9355941799
796910464566#752104#0

The initial five consecutive pound symbols are used because errors in recognition frequently occur with the first character. Experience has shown that sending the actual data after several characters of dummy code

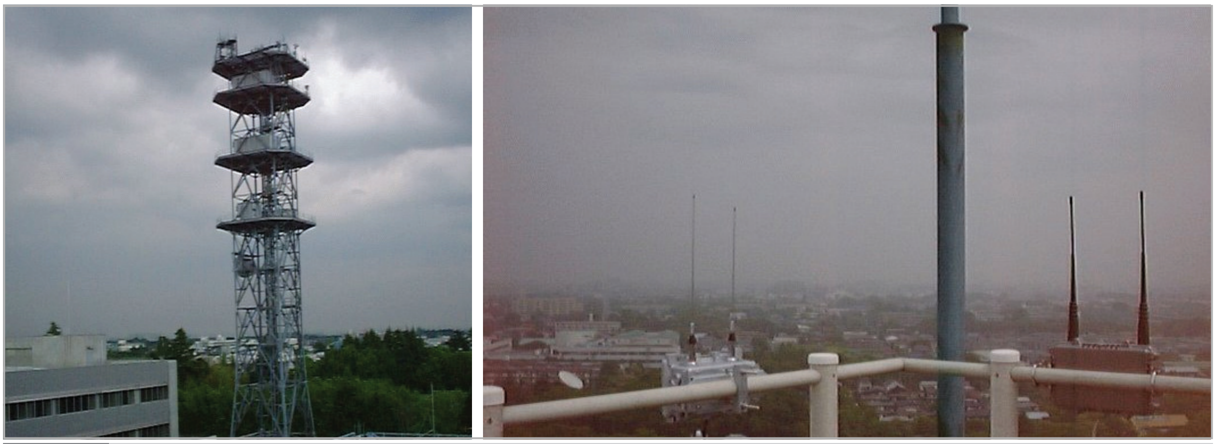

**Fig.11** Tower (at left) and repeater on top (right)

**Table 5** Positions from which access was possible using radio telephony of specified low-power radio stations

| Site of Mobile Station | Distance from Repeater |
|---|---|
| JR Mitaka Station, South Exit (on the pedestrian overpass) | 6.8 km |
| JR Tachikawa Station, North Exit (on the pedestrian overpass) | 6.8 km |
| In the city of Musashino (on the fifth floor of a building) | 6.9 km |
| Showa Kinen Park in Tachikawa (on the ground) | 7.5 km |
| In the city of Akishima (on the fourth floor of a building) | 9.7 km |
| Hirayama Bridge, Hino (on the ground) | 11.1 km |
| Hodokubo, Hino (on the ground) | 11.1 km |
| JR Hachioji Station, North Exit (on the roof of a ten-story building) | 14.4 km |

improves the recognition rate. Several types of recognition errors occurred: codes were counted twice, skipped, misinterpreted, and so on. Actual data from recognition results is given in Table 6. The combination of the length of one DTMF code and the space between codes were varied in the experiment. Each variation was tested either one or more times. The interval for checking recognition data was set at 17 ms, and the signal-to-noise ratio for signal selection was 3.5.

Of note among these experimental results is the prevalence of the recognition error in which a nonexistent code (“1”) was inserted before and after transmission. This can be attributed to misinterpretation of a response sound issued by the repeater when repeating is initiated or during standby. The prevalence of recognition errors with different combinations of code and blank space length varied considerably depending on the radio wave conditions at the time. It is difficult to generalize, but favorable results tended to occur only with code lengths of roughly 200 ms or more. However, even disregarding the misinterpretation that occurred after all codes were transmitted (as described above), 100% recognition occurred only once, for the combination of a 200-ms code length and a 50-ms blank length, underlined in Table 6. Thus, 100% recognition is quite difficult to achieve, considering that short codes are often skipped and long codes are often counted twice.

Before these field tests, nearly 100% recognition was obtained when testing transmission and reception in the area around the repeater. However, at this transmission distance (13.6 km), regardless of the fact that the reduction in transmission level did not hamper intelligibility as an audible signal, achieving a recognition rate of 100% for DTMF codes is quite difficult. Based on these results, it is evident that practical implementation of radio transmission of DTMF codes would be challenging without devising a framework for error correction.

### 3.4 Discussion

As with systems described in Section **3.3**, mobile digital emergency PA radios on the 260-MHz band are one means of data transmission using mobile radio sets during disasters. In addition to voice transceiver functions, such systems support data transmission, including TCP/IP communication. However,

**Table 6** *Experimental results for DTMF code recognition using a specified low-power radio station transceiver*

| Length of One Code (in ms) | Length of Blank Space between Codes (in ms) | Recognition Result |
|---|---|---|
| 80 | 20 | 1478353254546935941979691464566675214 |
| | | 1#7833255693559499969104645667 5214# |
| | | 1#####10470#83532#54546#935594179979691464566#75210401 |
| | | ##1470#83532#54546935941799796914645 66#75214 |
| 100 | 50 | ####140#83532#54546#935594179979691065 66#752104#0 |
| 120 | 20 | 14783532545469359417997969146456 75214 |
| | | ###*1470#83532#545469355941797969146456675214 |
| | 50 | #14783532545469355941799796910464566#752140 |
| | | 1#147#835325454693559417997969146456675214 |
| | | ###10470#8353254546#935594179979691046 4566#752104#* |
| | | 1#####1470#83532#54546#935594179979691464566#752104#0 |
| | | ####1047#83532#545469355941799796914645 66#75214# |
| 150 | 20 | ###14700#83532#54546#935594179796910464566752140 |
| | 50 | #######*10470083532#54546#935594179979691046 4566#75214 |
| 180 | 50 | ###*147#83532#54546#9355941799796914645 66752104001 |
| 200 | 50 | #######*10470#83532##54546#935594179979691046 4566#752104##0111 |
| | | #####*10470#83532#54546#935594179979691046 4566#752104#011 |
| | | 1#######*1470#83532#54546#935594179979691046456666#7552104##00 |
| | | A1#####**1047#8353254546#935594179979691046 4566#752104#011 |
| | 100 | ##1477#83532#54154693559417997969146 4566#75214# |

these systems have been deployed assuming that users will be disaster control personnel of local governments, or members of fire departments or community associations. It is not necessarily a perfect plan, considering the shortage of personnel caused by rescue efforts after large-scale disasters, and given the need to use the system on an emergency basis immediately after disasters strike. It is therefore important to build on a familiar, nearby means of communication as described above to secure a method of data transmission during disasters.

## 4 Using ubiquitous devices to gather information during disasters

RFIDs (smart tags) and sensors have become popular examples of devices in ubiquitous networks. Developers envision transmitting information gathered from these devices over ad-hoc networks or by other means. These devices are also important in the environmental monitoring mentioned in Section **2.2**. In this section, we describe several examples of techniques using RFIDs and sensors with ad-hoc networks to gather information during disasters.

Other papers in this issue address related topics: research on RFID-based support systems for gathering information after disasters[12] and current ad-hoc network technology that can be used in emergencies, as well as trends in this field[13].

## 4.1 Advanced RFIDs in information systems to support firefighting

### *4.1.1 Overview*

In FY 2000, the Fire and Disaster Management Agency (FDMA) developed an information system to support firefighting[14]. This system is mainly designed to locate firefighters deep underground or in other areas in which firefighting is difficult, where GPS and wireless communications are unavailable. Inertial navigation system devices worn by firefighters obtain location information, which is conveyed via ad-hoc communication or other means to the field command center. Here, firefighter locations are displayed on a 3D numerical map. Absolute location information transmitted from RFIDs attached to the evacuation lights indicating the escape route is used for error correction of this location information, and RFID reader/writers worn by the firefighters are used to receive and correct the absolute location information. In this system, the RFIDs attached to the evacuation lights are battery-powered active tags that emit trace radio waves on the 300-MHz band. This type of RFID is expensive, and because it emits radio waves like a beacon, the battery must be replaced regularly. These RFIDs cannot be used for other purposes, as rewriting the requisite data afterward is difficult. Thus, several factors must be overcome before the system is likely to become popular. In addition, signals from active tags can be received from approximately 10 m away, a distance at which location information is much more accurate than data from the inertial navigation system devices; this has led to problems with location correction. Replacing these RFIDs with passive tags (which do not require batteries) would make the system more affordable and easy to maintain. It would also enable the addition of information and support logistical management of the evacuation lights. Firefighting surveillance information could be recorded after installation. Replacing the tags in this manner would thus prove an effective way to popularize the system. However, one concern with passive RFIDs is that their effective range is shorter than that of active RFIDs. A shorter range may result in unsuccessful location correction when firefighters are working near the evacuation lights, which defeats the system's main purpose. For passive RFIDs, the frequency band yielding the longest range is said to be the UHF band (950–956 MHz), but records of performance with this band are still unavailable in Japan. Restrictions on using this frequency were slated to be lifted at the end of FY 2004, but basic data is lacking to enable this move. Thus, the author, who has participated in the development of this system since FY 2003, verifies whether replacing the RFIDs with passive RFIDs transmitting in the UHF band would support location correction.

### *4.1.2 Verification testing*

It is assumed that alternative RFIDs will be used just as in the current system (that is, attached to the evacuation lights) for interaction with readers/writers worn by firefighters. Accordingly, to measure the range, we attached RFIDs to evacuation lights in a fixed position and determined the areas in which reading and writing was successful or unsuccessful when the reader/writer was moved. The assumed mode of use is shown in Fig.12.

As of March 2005, domestic restrictions on RFID systems operating on the UHF band are still in effect, so measurement of the characteristics was contracted to a professional with an anechoic room who was licensed to operate experimental radio stations. The measurement setup in the anechoic room is shown in Fig.13. The mode of use was as shown in Fig.12. High-output reader/writers (maximum: 1 W) were used, with evacuation lights and RFIDs at a height of 2.4 m and the antenna at

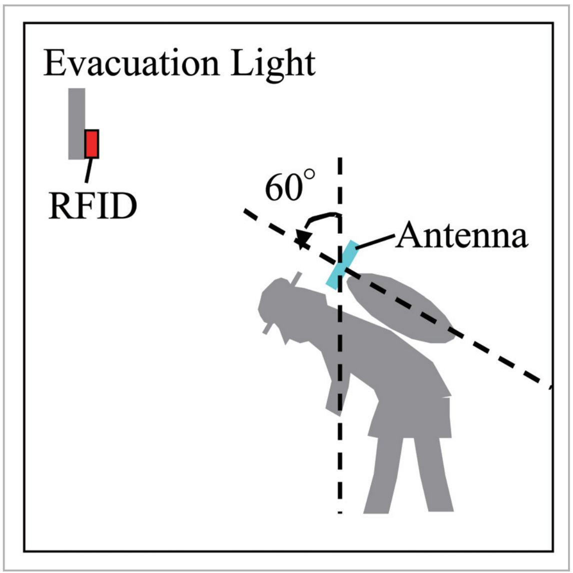


**Fig. 12** *Assumed mode of use*

a height of 1.5 m. Under these conditions, we varied the distance between the evacuation lights and antenna and the angle of measurement to determine the area in which RFID reading and writing was possible.

Figure 14 shows an example of the relationship of antenna position to successful read rate, with the evacuation lights and RFIDs at the starting point. The unit of the scale in Fig.14 is meters. We determined that the RFIDs could be read at a distance of approximately 4 m from the evacuation lights, if read in the area in front of the lights. Location correction requires reading at a distance of less than 4 m from the evacuation lights. Thus, because the experimental mode used did not differ in this regard from the current system using active RFIDs, we can conclude that replacing active RFIDs with passive ones will pose no difficulty in terms of location correction.

#### *4.1.3 Discussion*

Measurement of the characteristics involved high-output (maximum: 1 W) reader/writers, as reported in part by the Information and Communications Council[15]. However, taking size, power consumption, and radio station license requirements into consideration, it is more appropriate to use low-output types (maximum: 10 mW) that do not require a license, such as the reader/writers worn by firefighters. Technical requirements governing reading and writing performance by these low-output units will be established in time, and verification will be required after experimental devices are developed. Details of the results of these measurements have been published in an FDMA document; specifically, a FY 2004 report by a development committee working on information systems to support firefighting in challenging underground areas[16].

### 4.2 Wireless system for use in firefighting, employing multi-hop wireless LAN [17]

#### *4.2.1 Overview*

Current fire department radios are used almost exclusively for voice calls, but many other applications can be imagined if a wireless LAN, capable of transmitting large amounts of information, were to be employed as a fire department radio. Some research has appeared on using long-distance wireless LAN as a means of linking fire department headquarters and disaster sites (as described in Section **3.1**). However, there are many challenges in using wireless LANs at disaster sites, particularly in underground shopping areas inaccessible to radio waves. It is thus difficult to adopt wireless LANs for fire department radio, which is employed on an urgent basis and must perform reliably.

Instead, this section describes R&D on adopting multi-hop wireless LAN technology for use as a fire department radio at disaster sites.

#### *4.2.2 Adopting wireless LAN as a fire department radio*

Compared with conventional voice call systems on the VHF and UHF bands, a wireless LAN can transmit large amounts of data. This enables transmission of video, such as real-time footage captured by firefighters on the front line and sent to the command vehicle of the field headquarters. Such a system thus has the potential to contribute significantly to the coordination of firefighting. Reports have

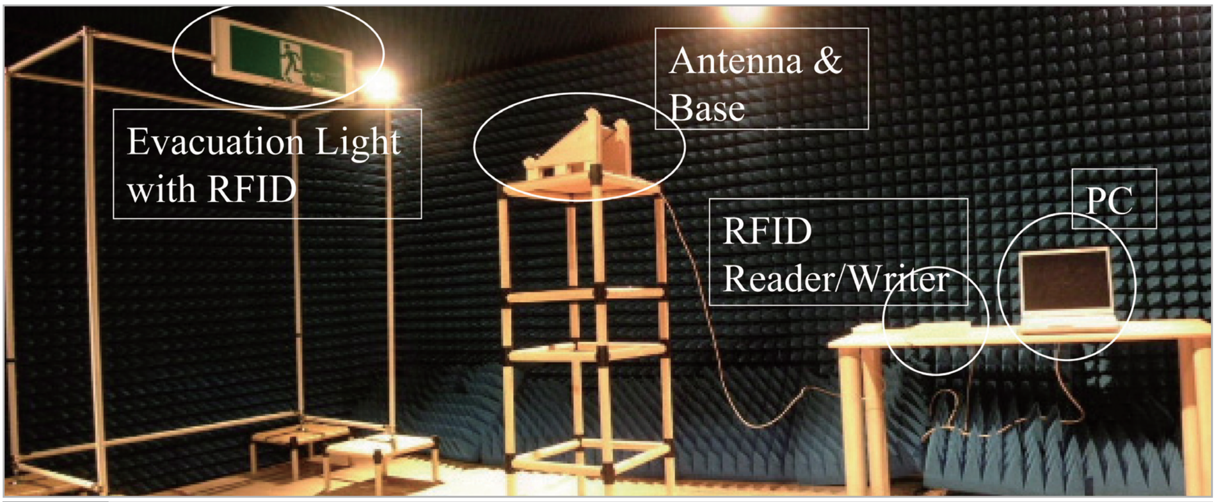


**Fig. 13** *Measuring the characteristics of passive RFIDs operating on the UHF band*

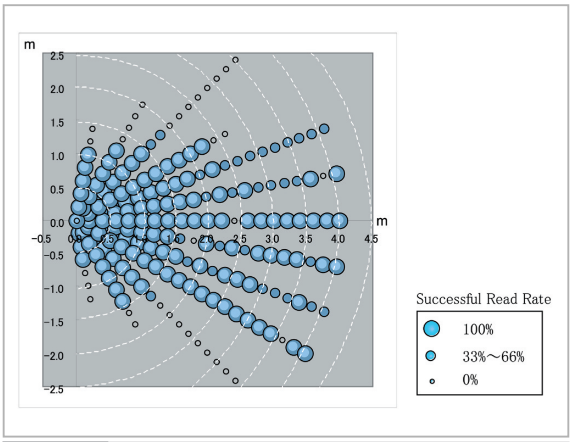


**Fig. 14** *One result of measuring characteristics*

indicated a need for the development of data transmission systems linking firefighters to field headquarters and to each other, providing information on their locations and the conditions at these locations. This proposed application has also been mentioned in the context of the FDMA's information system to support firefighting, described in Section **4.1** [14].

However, it is unrealistic to imagine using any existing wireless LAN access points at the scene of the fire, somehow reconfiguring these points for fire department radio in the course of firefighting. Thus, it is assumed that firefighters would bring a battery-powered access point for temporary installation at an affected site for use as the fire department radio. However, the range of wireless LAN is only within a few dozen meters of the access point, so in this case a network cable would have to be connected to the access point in large-scale fires or fires in complex structures. Such temporarily installed network cables are fairly unreliable, however, and might interfere with firefighting, or the installation work itself could be burdensome to the firefighters.

In view of these problems, to use a wireless LAN as a fire department radio, the applicable technology would have to include (1) a battery-powered access point, (2) multi-hop communication between access points, and (3) automatic configuration for multi-hop communication via detection of nearby access points, merely through installation of the wireless LAN. Figure 15 shows a schematic diagram of a multi-hop wireless LAN used as a fire department radio. To investigate the feasibility of use at the scene, we studied the application of this sort of technology to existing systems. Given that the equipment worn by firefighters must be as light as possible, it would be unrealistic to combine current transceivers for voice calls with a wireless LAN system. Thus, another of our aims was to enable voice calls over the wireless LAN system (VoIP).

#### 4.2.3 Overview of experiment enabling voice calls over multi-hop wireless LAN

The experiment in this case focused on "DECENTRA™" middleware, which dynami-

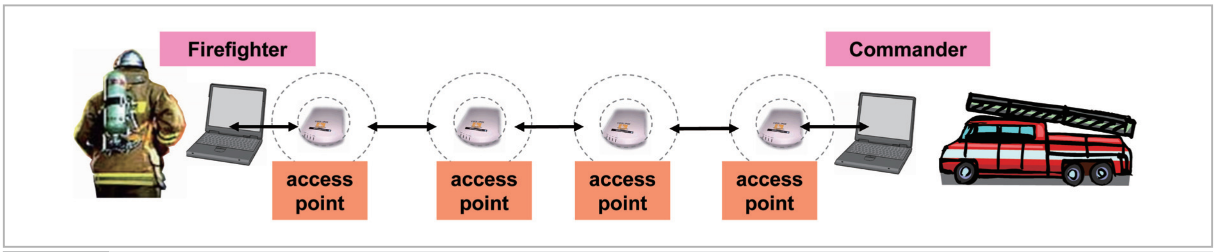


*Fig.15* Schematic diagram of a multi-hop wireless LAN used as a fire department radio

cally locates a channel of access points within a given area for use as relay stations (i.e., forming an ad-hoc network) and autonomously establishes a relayed (multi-hop) connection. DECENTRA uses a proprietary protocol over the transport layer (UDP) and original mechanisms to suppress surges of network channel data (a problem in wireless ad hoc networks, in which the network configuration changes frequently) and to lighten the load on terminals. Additionally, because bridging with ordinary IP networks is possible, the system can transmit data sent from the front line via multi-hop wireless LAN to field headquarters and then via an IP network to the remote fire department headquarters.

A wireless LAN access point used in this experiment is shown in Fig.16. Specifically, a wireless LAN conforming to the IEEE 802.11b standard was used for transmission over the ISM band at 2.4 GHz. DECENTRA was installed at this access point. A diagram of multiple installed access points is shown in Fig.17. Operation is shown in Fig.17, with firefighters setting up the access point en route to disaster sites as they prepare for firefighting and rescue activities. However, considering the access range of radio waves over a 2.4 GHz wireless LAN, in reality, the access point can be set up with more space than shown in Fig.17.

Notebook computers equipped with wireless LAN cards were used as the assumed terminals for use by the fire department headquarters (commander) and the firefighters. DECENTRA was installed on each. The screen displaying channel topology from fire department headquarters to the firefighters is shown in Fig.18. This screen shows there are two access points (ap2 and ap3) between fire department headquarters and firefighters, through which a multi-hop connection is established. This connection mode is changed dynamically in response to the radio-wave environment.

The terminals supported voice calls, using the OpenPhone libraries of the OpenH323 (open-source) software[18]. The OpenPhone screen is shown in Fig.19. Simultaneous bidirectional calls are supported. Here, output level is indicated by the left side of the red bar in the lower part of the screen. The input level is on the right side of the red bar.

#### 4.2.4 Experimental results and discussion

The computer at the fire department headquarters was run on the WindowsXP operating system, and the computer for firefighter use ran on Windows98. After testing voice calls between both parties, we determined there was no problem at up to two hops (from the fire department headquarters to the access point to firefighters), but additional hops caused noticeable delays in voice transmission, as well as connection instability. This problem may be attributable to the limited transmission rate in the IEEE802.11b standard (maximum: 11 Mbps) or terminal hardware performance (in particular, the firefighter terminal). In addition, the slow startup time for the access point (approximately two minutes) was an obvious problem. As a possible strategy to resolve these problems, a wireless LAN conforming to the faster IEEE802.11g standard could be employed, in addition to higher-performance hardware.


Fig.16 Wireless LAN access point used in the experiment (powered by an external rechargeable battery)

Fig.17 Diagram of access point setup

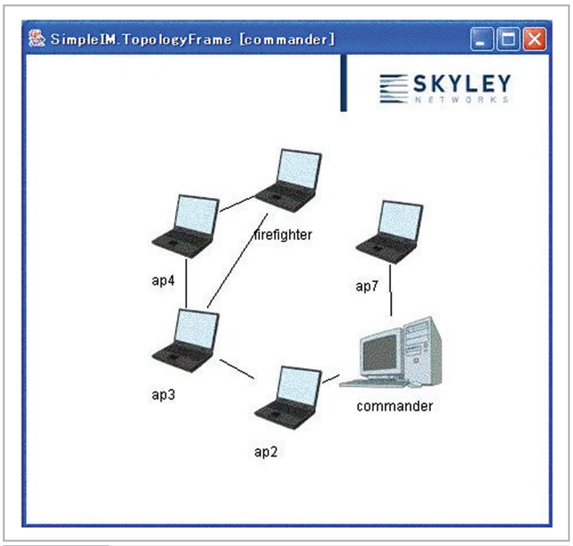


Fig.18 Screen showing channel topology


Fig.19 Software screen for voice calls

## 4.3 Development of a compact sensor network server for rescue

### 4.3.1 Overview

In FY 2002, some 32 organizations, including NICT, began participating in an R&D project launched by the Ministry of Education, Culture, Sports, Science and Technology, the "Special Project for Earthquake Disaster Mitigation in Urban Areas: Development of Advanced Robots and Information Systems for Disaster Response" (referred to below as the "DDT Project"). The project calls for R&D of technologies for use in disasters. Specifically, information from intelligent sensors, networked home appliances, portable terminals, robots, and the like throughout the affected site will be integrated to form dynamic ad-hoc networks. The data will help in assessing the situation at the disaster site and in drawing up an action plan to gather additional information. This section describes a compact sensor network server referred to as a rescue communicator, which serves as a common platform in the DDT Project.

#### 4.3.2 Rescue communicator functions

The rescue communicator was jointly developed in 2004 by a task force for rescue system infrastructure in the DDT. NICT is joined in this task force by the Institute of Physical and Chemical Research (RIKEN), the National Institute of Advanced Industrial Science and Technology (AIST), Mitsubishi Electric Corporation, the International Rescue System Institute (IRS), and others. At the core of this compact, lightweight, and long-lasting device is a Linux server. The device is equipped with search and rescue functions for disaster victims trapped in debris. It can audibly call out to victims, collect ambient sound, form ad-hoc networks via wireless LAN, and perform infrared communication. Additionally, it can control home robots and information appliances. The rescue communicator is depicted in Fig.20, and its specifications are listed in Table 7. The unit has functions to communicate with the mobile terminals of rescue squad members or airships over the site, and it can be expanded to form a comprehensive infrastructural device. Figure 21 shows the rescue communicator at an affected site. It is assumed that many of these units will be deployed in the disaster area. After a disaster strikes, the voices of disaster victims are received by the rescue communicators, which form ad-hoc networks with other units at the affected site. The developers envision these networks transmitting victims' voices to rescue airship overhead.

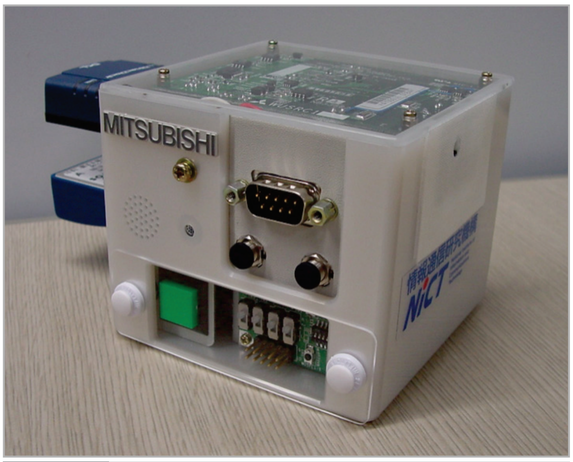


**Fig.20** Rescue communicator

#### 4.3.3 Tasks

In FY 2005, we aim to implement ad-hoc and multi-hop communications within the rescue communicator and establish the technology to form a sensor network. One of two platforms will be selected: either the Ubiquity Building ToolKit (UBKit, a set of software and hardware components under development by AIST for the construction of ubiquitous computing environments) or DECENTRA, described in Section **4.2**.

## 5 Conclusions

Resolving problems affecting the flow of information during disasters entails dealing with hardware issues, such as damaged communication equipment, as well as software issues, such as confusion in the event of conflicting or jumbled data, or problems with data authenticity. This paper has focused on research on resolving problems from hardware damage, but in terms of overall prevention and mitigation of damage from disasters, more efforts are needed. As stated in Section **2.1**, prevention and mitigation apply to real-world problems, so the relevant R&D will have to incorporate knowledge from fields such as social psychology and the behavioral sciences.

These information and communications technology (ICT)-based prevention and mitigation systems are often designed solely for prevention and mitigation; that is, many ICT-based systems simply help users get through current emergency conditions. Systems such as these are certainly warranted, but we adopt a broader perspective than that of prevention and mitigation specialists. More unified system design is required, from the broader perspective of experts in ICT. This involves designing a framework to deal with security, disaster control, and environmental issues that will enable the seamless switching of gears from routine operations to response, both in the event of small-scale incidents such as fires and upon occurrence of large-scale disasters. For these sorts of ICT-based systems to be truly effective in disasters, we must continue

**Table 7** *Rescue communicator specifications*

| | |
|---|---|
| CPU | SH7751R |
| OS | CE_Linux1.0 |
| SDRAM | 32 MB |
| FLASH ROM | 8 MB |
| Card slots | Accepts three compact flash cards |
| Voice-collection functions | Recording and playback (equipped with a microphone and speaker) |
| Serial port | RS-232C D-Sub 1, infrared port |
| Parallel port | I/O: 4 bits each |
| Case dimensions | 87.5(D) x 142.5/92.0(W) x 79.0(H) |
| Power | Five AA batteries or AC adapter |

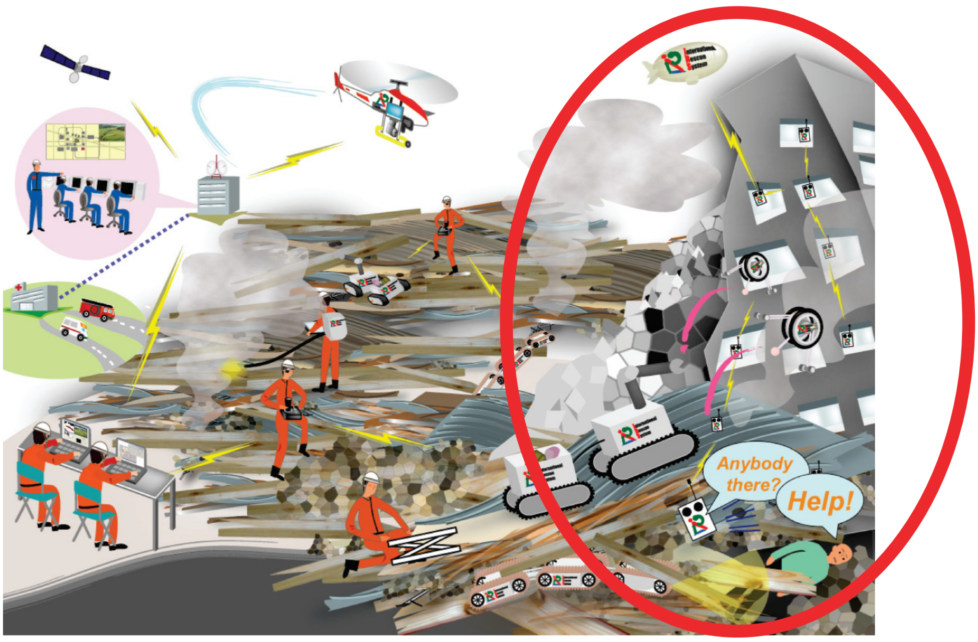


**Fig.21** *Rescue communicators in use at disaster sites (circled in red) (Source: International Rescue System Institute)*

rigorous evaluations in real-world applications.

## Acknowledgments

We would like to express our gratitude to the following organizations for their contributions to this research.

Section **3.1**: In the experiment to construct a long-distance wireless LAN, we thank Wakkanai Hokusei Gakuen College and the National Research Institute of Fire and Disaster (NRIFD) for their assistance. Section **3.2**: In the experiment on IP communication using emergency digital PA radios on the 60-MHz band, we thank the Kinki Bureau of Telecommunications for organizing the public experiments and Oki Electric Industry Co., Ltd., manufacturer of the Ethernet/RS-485 converter. Section **3.3**: In the experiment on simple data transmission using voice transceivers, we thank the IAA amateur radio club stations. Section **4.1**: In measuring the characteristics of RFIDs in information systems to support firefighting, we thank the Extraordinary Disaster Management Office of FDMA and the Fire Protection Equipment and Safety Center of Japan. Section **4.2**: In the development of a wireless system for use in firefighting that employs multi-hop wireless LAN, we thank Skyley Networks, Inc. Section **4.3**: In the development of a sensor network server for rescue we thank those involved in the DDT Project.

## *References*


1 Tohru Kishimoto, “Environmental Field × Ubiquitous ≒ Disaster Prevention Field × Ubiquitous”, 2nd Workshop of IEICE Ubiquitous Society and Lifestyle SIG, 2005. (in Japanese)

2 Hiroyuki Tamura, Masafumi Hosokawa, Matoko Endo, Shinsaku Zama, Takashi Shiga and Toshiya Murata, “Field Study on Communication of Wireless Disaster Prevention Network with Wireless LAN and PHS”, the Journal of Social Safety Science, No.4, pp.201-206, 2002. (in Japanese)

3 Hitoshi Kaiho, “A Trial of Distributing Dailylife Information to Sufferers in case of Large-scale Disaster”, master thesis of Keio University Graduate School of Media and Governance, 2000. (in Japanese)

4 Osamu Takizawa and Noriyo Kanayama, “Progress of Wakkanai Experimental Community Network Project”, Journal of the National Institute of Information and Communications Technology, Vol.51, Nos.1/2, pp.179-199, 2004.

5 Hokuriku Bureau of Telecommunications, “The report of a research committee of general IP radio communications systems (abstract)”, http://www.hokuriku-bt.go.jp/press/2003/image/040309-1.pdf, 2004. (in Japanese)

6 Shikoku Bureau of Telecommunications, “The report of a research committee of support systems that provide disaster information (abstract) ”, http://www.shikoku-bt.go.jp/press/2004press/200403/2004030201_1.html, 2004. (in Japanese)

7 Chugoku Bureau of Telecommunications, “The report of a research committee of the use of emergency digital PA radio over a broad area”, http://www.cbt.go.jp/kenkyuu/kenkyuu08_03_00.pdf, 2003. (in Japanese)

8 Kinki Bureau of Telecommunications, “A public experiment on a system for gathering disaster information”, http://www.ktab.go.jp/new/17/0120-1.pdf, 2005. (in Japanese)

9 Osamu Takizawa, Yoshinobu Saito and Hiroyuki Ohno, “A Consideration on the function of information registration over radio connection to a disaster victims information registration and retrieval system”, 4th Internet Technology Workshop (WIT2001), WIT2001-SP-1, Japan Society for Software Science and Technology, 2001. (in Japanese)

10 Nexus Co., Ltd. “Software DTMF Controller 1.1c”, http://www.vector.co.jp/soft/win95/net/se123346.html.

11 Hideo Tsukamoto, “Random number sequences generator RANer Ver 0.75”, http://www.vector.co.jp/soft/win95/util/se112992.html.

12 Osamu Takizawa, Akihiro Shibayama, Masafumi Hosokawa and Yoshiaki Hisada,“Research and Development of an RFID-based Disaster-relief System”, Journal of the National Institute of Information and Communications Technology, Vol.52, Nos.1/2, 2005.

13 Koichi Gyoda, “States and Trends of Technologies in the Ad Hoc Networks applicable to emergency communications”, Journal of the National Institute of Information and Communications Technology, Vol.52, Nos.1/2, 2005.

14 Fire and Disaster Management Agency, “FY2003 report of a development committee on information systems to support firefighting in challenging underground areas”, http://www.fdma.go.jp/html/new/pdf/040521_hokoku.pdf, 2004. (in Japanese)
15 Ministry of Internal Affairs and Communications, “Technical conditions for high-power passive tag systems using the 950MHz band (partial report from Information and Communications Council)”, http://www.soumu.go.jp/joho_tsusin/eng/Releases/Telecommunications/news041215_2.html, 2004.
16 Fire and Disaster Management Agency, “FY2004 report of a development committee on information systems to support firefighting in challenging underground areas”, 2005. (in Japanese)
17 Osamu Takizawa, “Next-generation firefighter communication system using multi-hop wireless LAN”, Annual Conference of System Integration Division, 1B3-2, the Institute of Systems, Control and Information Engineers, 2003. (in Japanese)
18 OpenH323 Project, http://www.openh323.org/.



***TAKIZAWA Osamu**, Ph.D.*

*Senior Researcher, Security Advancement Group, Information and Network Systems Department*

*Contents Security, Telecommunication Technology for Disaster Relief*