DESIGN OF A SECURE DISASTER NOTIFICATION SYSTEM USING THE SMARTPHONE BASED BEACON

Jae Pil Lee[1] and Jae Gwang Lee[2] and Jun hyeon Lee[3]
Ki-su Yoon[4] and Jae Kwang Lee[5]

[12345]Department of Computer Engineering,
Han Nam University, Dae-jeon City, Korea
{jplee,jglee,jhlee,ksyoon}@netwk.hnu.kr,
jklee@hnu.kr

ABSTRACT

The number of disaster occurrences around the world based on the climate changes due to the global warming has been indicating an increase. To prevent and cope with such disaster, a number of researches have been actively conducted to combine the user location service as well as the sensor network technology into the expanded IoT to detect the disaster at early stages. However, due to the appearance of the new technologies, the scope of the security threat to the pre-existing system has been expanding. In this thesis, the D-SASS using the beacon to provide the notification service to the disaster-involved region and the safe service to the users is proposed. The LEA Algorithm is applied to the proposed system to design the beacon protocol collected from the smartphone to safely receive the notification information as well as to provide the confidentiality during the data transfer between smartphone and notification server.

KEYWORDS

Disaster, notification, Beacon, Security, Smartphone, LEA, Google Chart

1. INTRODUCTION

According to the data announced by the CRED (Centre for Research on the Epidemiology of Disasters) in which the global disaster risk factors and the number of global disaster occurrences by the year are analyzed in accordance to the temporal/spatial distribution., the number of the disaster occurrences such as earthquake, surge, typhoon, flood and forest fire has been indicating an increase every year [1]. The disaster includes natural disasters (typhoon, flood, drought, tsunami and surge), man-made disasters (fire, collapse, explosion, environmental contamination and accident) and social disasters (energy, communication, traffic and infectious disease). The Centers for Disease Control and Prevention has been continuously developing and providing the manuals/measures on preparation for and management of the disaster/emergency. In addition, the Centers for Disease Control and Prevention also has been conducting cooperative projects by constructing the public health crisis management centers at the universities located in the main regions of the United States. Such cooperative projects provide services to individuals, workers and communities nationwide [2].

Natarajan Meghanathan et al. (Eds) : NETCOM, NCS, WiMoNe, GRAPH-HOC, SPM, CSEIT - 2016
pp. 01– 12, 2016. © CS & IT-CSCP 2016 DOI : 10.5121/csit.2016.61501

Based on the development/supply of the ICT (Information Communication Technology), the disaster communication has been making a transition from the control provided by the preexisting disaster management organizations to the construction of the full-range disaster communication system which allows the people regardless of their region to mutually communicate with others. The WORKPAD Project conducted in the European Union is a case where the state-of-the-art technologies are converged with the disaster communication to consider the safety of the field management team, and the Emergency 3.0 Project conducted in Australia is a case where the private/government-based cooperation is used to distribute the disaster information in real-time[3][4]. In Korea, the disaster field is faced with the limited management of the crisis related to the man-made disasters occurring due to the accident death rate and safety ignorance relatively high in comparison to the rapid economic development. To make progress in the disaster/safety areas, the following 4 strategies are being promoted: the construction of the public safety infrastructure, the construction of the natural disaster infrastructure, the connection/use of the private data and the exchange/expansion of the information for the citizen-participated services [5].

The IoT (Internet of Things) is a technology to which various companies and academic circles have been paying their global attention. Through this technology, the users may connect all devices including smartphone and resource-limited sensor to the internet. In addition, the IoT-based devices may be connected with one another to collect, process, exchange and share information. According to Gartner, more than 26 billion devices will be mutually connected by the year 2020, and such connection will create diverse innovations and business opportunities [6]. The smartphone is one of the popular high-performance devices mostly used to actualize the IoT. Such smartphone is a medium suitably used for communicating with the surrounding sensors, immediately applying the information collected through its own sensor to its services and transferring the information collected through the network to the necessary locations. Through the application of the IoT-based communication and sensor network technology, the importance of the system capable of providing the real-time disaster information to the smart mobile devices has been magnified.

The sophistication of the recent cyber threats has been causing social confusion and has been threatening the national security as well. The scope of its use has been expanding into causing financial damages to individuals. Accordingly, an issue has been raised on the information leakage as well as the security. In addition, the sophistication of the malignant codes and hacking technologies has been constructing a structure where the maliciously acquired contents are easily distributed. Since the BLE (Bluetooth Low Energy) based beacon provides a prompt communicative connection to the smartphone without requiring the pairing process, the communication can be conducted based on a small data transfer volume. In addition, the strength is that any smartphone capable of receiving messages is capable of receiving this message. Accordingly, there is no need to protect the data exposed from the smartphone. It is necessary to come up with a security technology which can be used to prevent the abuse of personal information contained in the smartphone, protect the privacy of the disaster notification service users and create a safe use environment.

In this thesis, to conduct a research on combining the user location-based service and the sensor network technology into the expanded IoT technology in order to cope with the home/overseas disaster-related, The D-SASS using the BLE-based beacon to provide the notification service to the disaster-involved region and a safe service to the users is proposed. The LEA (Lightweight Encryption Algorithm) is applied to the proposed system to design the beacon protocol collected by the smartphone to safely receive the notification information as well as to provide the confidentiality during the data transfer between smartphone and notification server. In addition, to monitor the status of the users in the disaster-involved region, the Google Chart is used to visualize the status of the people who received the notification in the disaster-involved region as well as the status of the people in the disaster-involved region on the web. This thesis is organized as follows. In Chapter 2, the precedent researches on the disaster management information system are examined. In Chapter 3, the system for collecting/analyzing the disaster notification system is designed and actualized. Lastly, the conclusion and the future researches to be conducted are proposed.

2. RELATED STUDIES

2.1. Big Data Disaster Prediction Service

The need to manage the disaster through the use of IT technologies is being expanded in order to detect at early stages and minimize the damages caused by enlargement, concentration and globalization of the disasters such as natural disaster and environmental contamination. Some of the IT technologies used to manage the disaster are disaster management robot, disaster safety wireless communications network, CCTV-based monitoring service, smartphone-based forecast/ notification service, computer-based disaster prediction and homeworking through the construction of cyber offices. Such technologies are being actively developed/applied at home and overseas [7]. The IT technology-based safety system can be used to prevent and promptly react to the damages caused by the disaster, and the intellectual image recognition technologies such as CCTV can be used to safely prevent the national level disaster.

In the precedent research [8], the damages caused by the natural disaster were measured to be restored, and the smartphone-based damage measurement standard work process was developed to develop a system which can be used to measure the damages caused by the disaster in the involved field through the use of the smartphone in order to input such measured data into the NDMS (National Disaster Management System. Through such development, the work process was decreased by 56% in comparison to the pre-existing work process. In Korea, a new government operation paradigm known as the Government 3.0 is proposed to provide the nation-customized service through positive disclosure, sharing, communication and cooperation among the departments. In addition to the attention paid by the private companies to the Big Data, a national level strategy is being established as well. The disaster management has been making a transition from the government-based management to the sensing model of disaster issues used for connecting/analysing the public/social data to sense and cope with the home/overseas issues and changes [9].

2.2. Smartphone-based Sensor Information Collection Service

Due to the changing patterns of the disaster management based on the supply of the smartphone, the need to develop diverse mobile apps featuring communication and interaction in the disaster situation has been expending [10]. The beacon is a BLE-based precision location information system and is highly evaluated as a short distance data communication technology. The beacon can be signified as a transmitter using the 2.4GHz bandwidth radio frequency serving as the ISM (Industrial Scientific and Medical) bandwidth to periodically create/distribute signals. In addition, it uses the RSSI (Received Signal Strength Indicator) to mutually interchange the data with the smart mobile to measure the location. It is impossible to confirm the location of the smartphone user through the GPS Signal. However, the Beacon can be used to confirm the precise location of the smartphone user within approximately 5cm distance error, and such beacon can be installed/used indoor/outdoor [11].

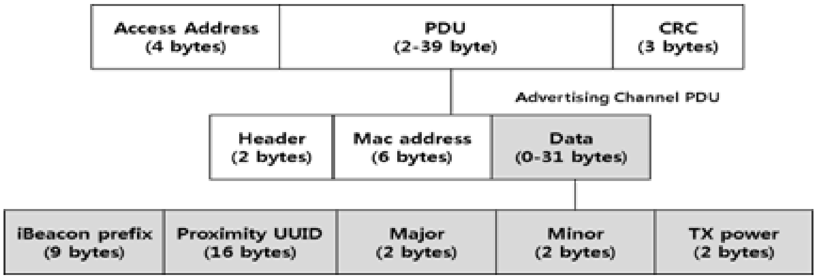


Figure 1. iBeacon Advertisement Packet Structure

The size of the data defined in the iBeacon [12] is 31bytes and the iBeacon prefix is 9bytes. The configuration is as shown in Figure 2. In general, UUID (Universally Unique Identifier) is the unique ID of the product and is constructed based on its own UUID depending on the service. The Major ID and Minor ID are respectively 2bytes and the setting range is from 0 to 65535. The Tx Power represents the RSSI value measures by the beacon at 1m distance. In this thesis, the combination of MAC/UUID/Major/Minor is used as the authentication factor among the authentication servers. In the precedent research [13], due to the expanded importance/value of the Big Data in the IoT environment, a number of home/overseas researchers have been proposing the convergence service through the Big Data analysis. The researches on how to most accurately/promptly collect information from rapidly changing spaces have been conducted. In such researches, the concept of the ‘majority living in the region’ instead of the ‘minority of experts’ is applied and the real-time information is accurately provided based on the information collected from the majority living in the region.

In addition, the sensor information from the natural disaster situation and the sensor information from the region/area where the smart mobile device users participate are collected to conduct a research on the crowd sensing and beacon information collection to create new knowledge. However, a designing for protecting the sensor information is not added during the disaster information collection. Accordingly, it is necessary to create an atmosphere where the personal information of the users can be protected and safely used to create new information.

2.3. Smartphone-based Security Service

The security intelligence field defined by the Gartner [14] Group has been receiving attention as the main alternative, and the technologies for processing/analysing the Big Data are being used to process/analyse diverse types of the long-term accumulated Big Data. The cyber threats appearing from 2010 to the present include insider threats and entering of malicious codes through normal network services. The internal network can be infiltrated at any time through diverse routes/methods. Accordingly, the internal network behaviour analysis technology used for collecting/analyzing the diverse system log information and as well as the dynamic behaviour information occurring in the internal network has been attracting the attention [15]. Since the android platform involves the Java-based programs that can be easily reversed through the app reverse engineering, app pirating/plagiarizing have been occurring frequently [16].

In the precedent research [17], to stop the production/distribution of the illegal/malicious apps through pirating/plagiarizing/repackaging the codes from the android apps, the code obfuscation techniques used for protecting the software programs by modifying the codes so that it is difficult to conduct a counterattack is considered into using the strong Birthmarking to propose a technique detecting/identifying the program pirating through comparing the similarities between the features of the involved programs. The android apps are distributed in the APK (Android

Application Package) and the byte code-level execution file DEX (Dalvik Executable) is included in such apps. In the precedent research, the security is focused on the smart mobile apps featuring strong obfuscation and efficient/reliable anti-pirating..

In the precedent research [18], the block cipher LEA (Lightweight Encryption Algorithm) is an algorithm used for encrypting the 128-bit data block. The 128/192/256-bit keys can be used. The round function of the LEA only consists of the 32-bit ARX (Addition, Rotation, XOR)-based arithmetic operations and therefore is promptly processed in the universal 32-bit software platforms supporting such arithmetic operations. In addition, the arrangement of the ARX-based arithmetic operations within the round function not only sufficiently guarantees the safety, but also features the lightweight actualization through excluding the use of the S-box.

3. DESIGN OF SECURITY NOTIFICATION SYSTEM

In this thesis, the user location-based service and the BLE-based beacon are used to provide the notification service to the disaster-involved region, and the D-SASS is proposed to provide the prompt/safe service to the service users. This system is provided to the disaster information service users in the wireless communication environment and is provided to the smart device users.

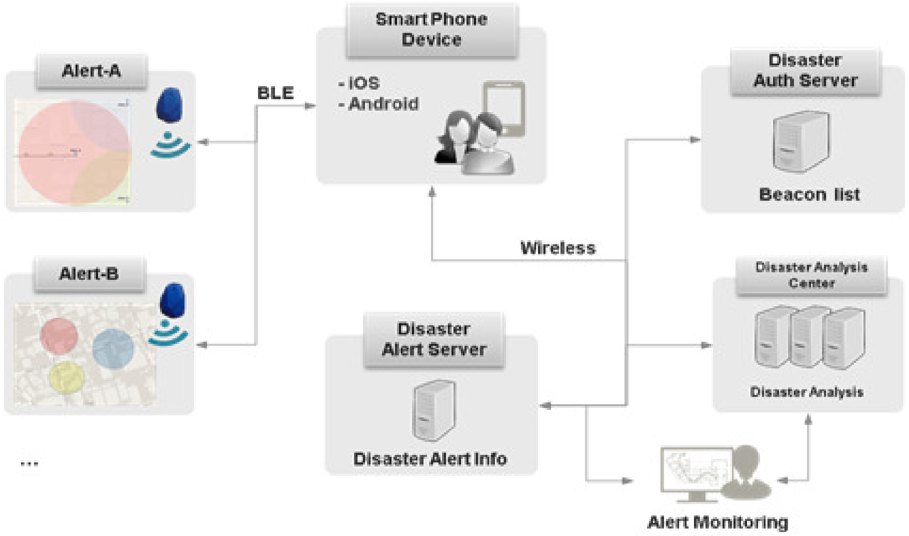


Figure 2. Configuration of Disaster Security Notification System

The proposed system proposes its scope consisting of the surrounding beacon sensor collected by the disaster notification service users within the smartphone, the user GPS information, the disaster notification service, the beacon authentication server and the analysis center. To protect the data collected by the service users during the disaster information collection, the LEA cipher algorithm is used to design the security system for protecting the disaster data collected by the users.

Figure 2 is the configuration of the disaster security alarm system for the DISU (Disaster Information Service Users). The configuration of the security alarm system consists of the smart mobile device collecting the disaster information and displaying the alarm, the disaster notification server providing the disaster information notification/visualization service, the disaster authentication server providing the disaster information beacon and the smartphone information authentication service, and the disaster analysis center server detecting/determining the disaster situation. In this thesis, to provide the safe service to the disaster information service users, the authentication procedures between smartphone and disaster alarm server is designed, the secret key is produced by combining beacon information and user membership information and the produced secret key is used for encrypting/decrypting the personal information data of the disaster information service users within the smartphone.

3.1. Design of D-SASS Encryption Protocol

In this thesis, the beacon packet structure is partially used to product the secret key used for the LEA encryption algorithm in order to design the safe security alarm system providing the notification Beacon (authenticated) information received from the notification server to the smartphone.

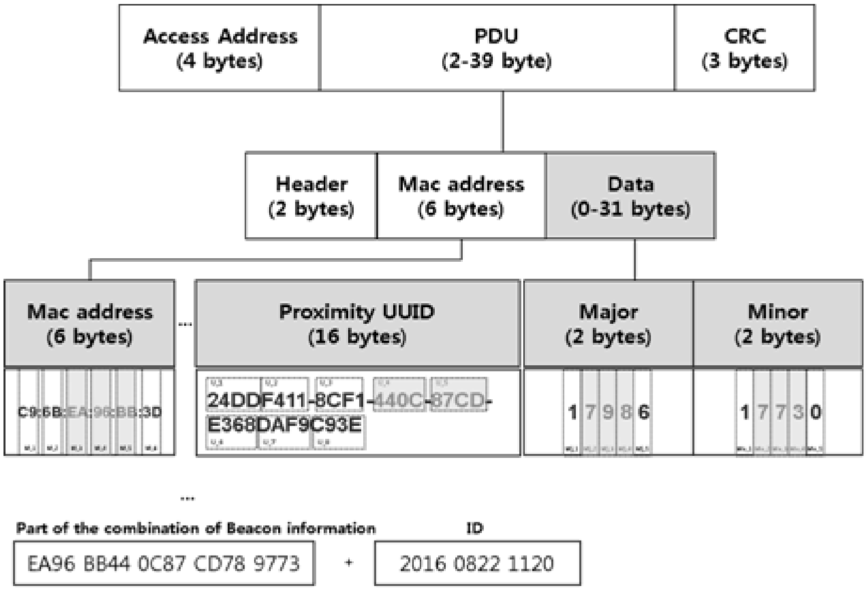


Figure 3. Design of Beacon Encryption Protocol

As shown in Figure 3, in accordance to the IEEE 802.11 Standard [19], the data frame is set, the 4 types of information (MAC, UUID, Major, Minor) are converted into the character string format, the B_Pinfo is combined with the DISU ID, and the secret key is produced. The LEA [20] is used to protect the data of DISU during the transfer of the notification information created in the disaster-involved region. The LEA is a 128-bit block cipher algorithm developed to provide the confidentiality in the high speed environments such as Big Data and Cloud and the lightweight environments such as mobile device. The LEA is included in the target algorithms validated through the CMVP (Cryptographic Module Validation Program) in June 2015[21].

The design of the LEA algorithm is as follows. To use the LEA algorithm, the secret key used for encryption/decryption and the information (IV: Initial Vector) used in the CBC (Cipher-Block Chaining) mode are used. Then the 16-bit secret key of the disaster notification system as well as the initial value is used to encrypt the 128-bit plain text of the disaster notification information.

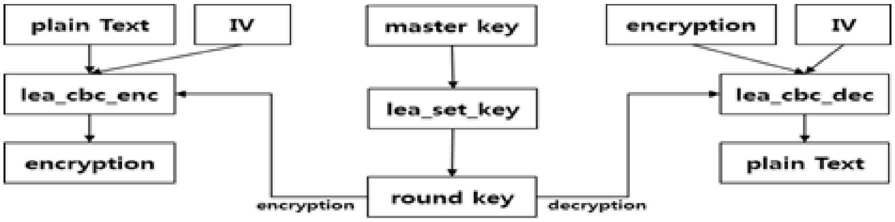


Figure 4. encryption and decryption of LEA Process

3.2. Process of D-SASS

Figure 5 shows the safe notification authentication process among DISU smartphone, notification server, authentication server and analysis center. The overall system consists of registration stage, authentication stage (TYPE_A) and service stage (TYPE_B). The overall system consists of DBS (Disaster Beacon Sensor), SUS (Service User Smartphone), DASS (Disaster notification Service Server), DAS (Disaster Authentication Server) and DACS (Disaster Analysis Center Server). The scope proposed in this thesis is Figure 5 and the security alarm process is as follows.

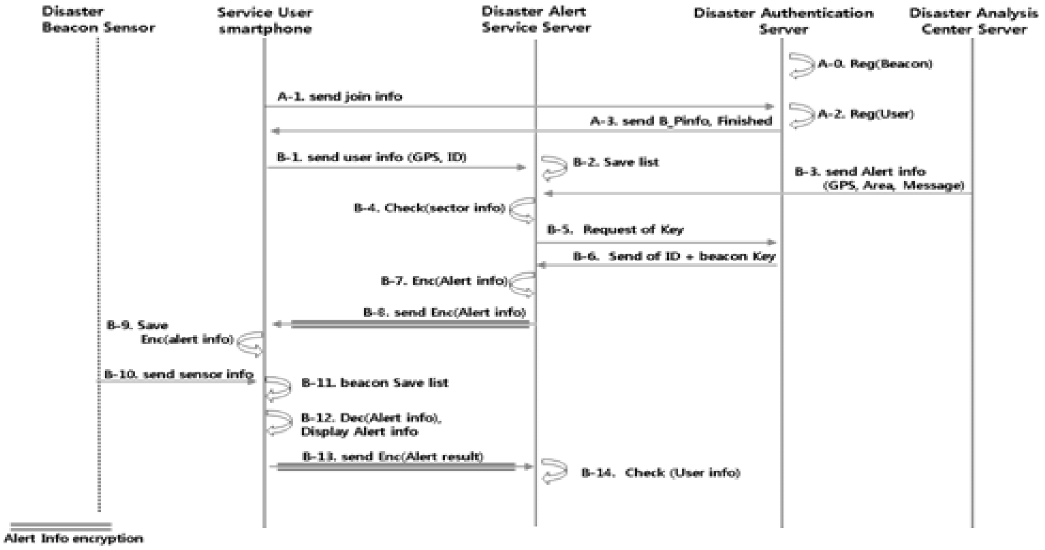

Disaster Beacon Sensor
Service User smartphone
Disaster Alert Service Server
Disaster Authentication Server
Disaster Analysis Center Server
A-0. Reg(Beacon)
A-1. send join info
A-2. Reg(User)
A-3. send B_Pinfo, Finished
B-1. send user info (GPS, ID)
B-2. Save list
B-3. send Alert info (GPS, Area, Message)
B-4. Check(sector info)
B-5. Request of Key
B-6. Send of ID + beacon Key
B-7. Enc(Alert info)
B-8. send Enc(Alert info)
B-9. Save Enc(alert info)
B-10. send sensor info
B-11. beacon Save list
B-12. Dec(Alert info), Display Alert info
B-13. send Enc(Alert result)
B-14. Check (User info)
Alert Info encryption

Figure 5. Disaster Security Notification Authentication Protocol Design

The disaster security alarm authentication protocol is processed in 3 steps. Step 1: A-0 is the step for registering the DAS prior to installing the beacon at the involved regions for providing the disaster service. Step 2: A-1, A-2 and A-3 are the steps for conducting the registration. Initially, the app is downloaded into the smartphone of the DISU to process the disaster service registration. For the registration, the ID/PW are issued and the registration information is transferred to the DAS to use the membership information as well as the ID/B_Pinfo as the encrypted key. Then the B_Pinfo is transferred to the SUS. Step 3: B-1 to B-14 are the steps for providing the service.

In Step B-1, the DISU transfers the user GPS information as well as the user ID information to the DASS at a constant interval. In Step B-2, the data transferred in the SUS step is received by the DASS, and the ID/GPS information of the DISU are stored in the database according to the time sequence. In Step B-3, the GPS/Beacon/Disaster Type/Message of the involved region is transferred to the DASS during the provision of the disaster notification from the DACS.

In Step B-4, the data transferred from the DACS is received by the DASS. After the data is received, the location information of the DISU located in the disaster-involved region is analysed to count the number of users in the involved region. In Step B-5, the information required for creating the secret key for encrypting/decrypting the LEA algorithm is requested from the DASS to the DAS in order to protect the disaster notification message. In Step B-6, the B_Pinfo from the advertisement packet structure of the beacon registered in the DAS is combined with the ID information of the DISU to create the secret key. The created secret key is then transferred from the DAS to the DASS.

In Step B-7, the secret key transferred from the DAS to the DASS is transferred, and the LEA algorithm as well as the secret key is used to conduct the encrypted arithmetic operations in order to encrypt the notification information (GPS/Beacon Information/Disaster Type/Message) related to the disaster-involved region. In Step B-8, the encrypted notification information is provided from the DASS to the users in the disaster-involved region through the SUS. In Step B-9, the encrypted notification information is received from the DASS to the SUS and stored in the smartphone.

In Step B-10, the information of the beacon installed in the disaster-involved region is provided to the smartphone of the DISU. In Step B-11, the beacon information received by the DISU is stored in the smartphone. In Step B-12, the ID of the DISU and the B_Pinfo from the received beacon information are extracted and used to create the secret key. In addition, the secret key created based on the encrypted notification information is used as the decryption key for the LEA algorithm to conduct the arithmetic operations required for processing the decryption.

In Step B-13, after the sound/message notification is received from the DASS to the DISU through the smartphone, the current location of the DISU as well as the beacon information is transferred to the DASS. In Step B-14, DASS provides the visualized data and measures the situation of the disaster-involved region based on the information received from the SUS of the DISU to measure the current situation of the DISU in the disaster-involved region.

3.3. Table Information of Development Environment

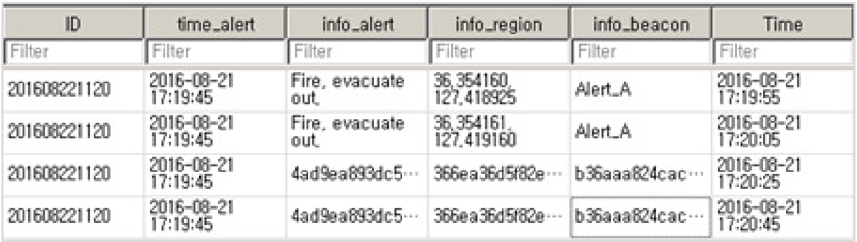
In this thesis, as shown in Table 1, the environment for testing the disaster security alarm system is constructed to apply the encryption between notification server and smartphone in order to design the safe disaster notification system using the smartphone-based beacon.

Table 1. Development Environment

Division	**Item**	**Specification**
Beacon	RECO	Bluetooth 4.0
	iBeacon	
NOTIFICATION Server	OS	Windows 7
	Apache	Version 2.2.14.
	PHP	Version 5.2.12
	MYSQL	Version 5.6.31
Smartphone	Galaxy Note4	Android version 6.0.1
Develop Server	OS	Windows 7
	Language	Java, C
	H/W	Intel Xeon, 16GB DDR3
	DB	SQLite
	Tool	Android Studio 1.5.1

The encrypted sections of the notification information are Step B-8 and Step B-13. The design needs to be set so that the disaster notification information received from the DACS to the DASS is stored in the database. As shown in Figure 6, the field of the disaster notification information table needs to be created. The received data as well as the notification time, notification information, region information, beacon information and user information is stored in the DACS.

The DASS uses the user ID value and the B_Pinfo value to create the secret key and uses the LEA algorithm to encrypt and store the data within the field. The stored data is transferred to the SUS in the encrypted format shown in Step B-8 and saved in the SQLite Database.

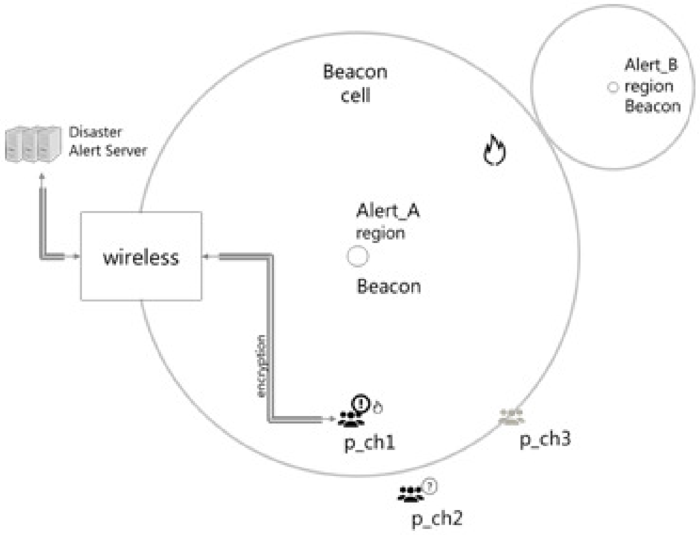


ID	time_alert	info_alert	info_region	info_beacon	Time
Filter	Filter	Filter	Filter	Filter	Filter
201608221120	2016-08-21 17:19:45	Fire, evacuate out.	36.354160, 127.418925	Alert_A	2016-08-21 17:19:55
201608221120	2016-08-21 17:19:45	Fire, evacuate out.	36.354161, 127.419160	Alert_A	2016-08-21 17:20:05
201608221120	2016-08-21 17:19:45	4ad9ea893dc5…	366ea36d5f82e…	b36aaa824cac…	2016-08-21 17:20:25
201608221120	2016-08-21 17:19:45	4ad9ea893dc5…	366ea36d5f82e…	b36aaa824cac…	2016-08-21 17:20:45

Figure 6. Design of Disaster-encrypted Notification Information DB

3.4. Scenarios of Disaster Notification system

The up of Figure 6 is the Beacon notification scenario model included in the disaster notification system for the DISU. If the DISU conducts movement within the Beacon-installed region, the GPS/ID is transferred to the DASS at a constant interval. If the disaster notification occurs in the wireless environment, the users are divided into 3 channels: the users included in the involved region (p_ch1), the users excluded from the involved region (p_ch2) and the users who escaped the involved region (p_ch3) 3.



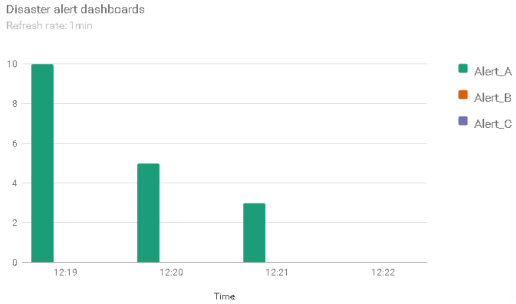


Figure 7. up: Safe Disaster Beacon notification Scenario, down: notification Dashboards

The information of the Beacon installed at the disaster-involved region is provided to the smartphone of the DISU. Only the Beacon information registered in the DAS can be collected and the Beacon information non-registered in the DAS serves as the filter during the collection. The p_ch1 users use the received Beacon information to produce the secret key and decrypt the encrypted notification information to receive the disaster notification sound/message through the smartphone. The down of Figure 6 shows a screen of the disaster notification information transferred to the 10 users included in the Beacon cell of the notification a included in the disaster-involved region as well as the current information of the users transferred from the SUS to the DAS. Then the situation of the p_ch2/p_ch3 within the disaster-involved region is displayed through the use of the Google Chart based on the received information to monitor the situation of the disaster-involved region.

4. CONCLUSIONS

To cope with the frequently occurring home/overseas disaster-related accident, various researches are being conducted to combine the user location-based service and the sensor network technology into the expanded IoT technology in order to detect the disaster at early stages. The preparation for and management of the disaster are considered essential for stabilizing and continuously developing the society. The need to develop a system capable of promptly/efficiently collecting/analysing the risk regions during the disaster occurrence has been expanding. However, the expanded scope of the IoT infrastructure increased the scope of the malicious actions applicable to the disaster system. In addition, an issue is being raised on the security due to the increased damages caused by the random exposure/leakage of the collected personal information.

In this thesis, the D-SASS (Disaster Secure Alarm Service System) using the BLE (Bluetooth Low Energy) based Beacon to provide the notification service to the disaster-involved region and the prompt/safe service to the service users is proposed. The LEA encryption algorithm is applied to the proposed system to design the secret key based on the Beacon protocol information collected from the smartphone to safely receive the notification information of the disaster service users as well as to provide the confidentiality during the data transfer between smartphone and notification server. In addition, to monitor the status of the users in the disaster-involved region, the Google Chart is used to visualize the status of the people who received the notification in the disaster-involved region as well as the status of the people in the disaster-involved region on the web.

It is estimated that the scope of the security threats which may occur to the IoT system from the collection stage to the authentication stage among the Beacon/smartphone/alarm server would be decreased and the damages to the personal information would be prevented. Based on the future disaster big data information, the communication protocol for transferring the real-time disaster notification is to be designed.

ACKNOWLEDGEMENTS

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT & Future Planning (NRF-2014R1A1A2055522).

REFERENCES

[1] Guha-Sapir D & Hoyois Ph. , Below. R. Annual Disaster Statistical Review 2013: The Numbers and Trends. Brussels: CRED; 2014.", Centers for Disease Control and Prevention, 2014.

[2] Centers for Disease Control and Prevention, "Emergency Preparedness and Response", Available on http://emergency.cdc.gov/planning/index.asp, 2015.

[3] Ministry of Government Administration and Home Affairs, "Disaster Safety Wireless Network Major Requirements", Vol. 2011, No. 76, pp1-5., 2011.

[4] W.S. Jun, "Disaster-Responsive IT Technology", ETRI, 2013 Electronics and Telecommunications Trends, pp145-153, 2013.

[5] National Information Society Agency, "The new ICT Convergence Strategy Information Security Policies of the disaster areas", Vol. 3, 2014.

[6] Gartner, "Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020", http://www.gartner.com/newsroom/id/2636073, 2013.

[7] Chun, H.W., Electronics and Telecommunications Trends, "Disaster Prevention Information Technology", 2013.

[8] National Disaster Management Institute, "Development of Technology on Linked with NDMS for Disaster Damage Investigation using Smartphone", 2012.

[9] Choi, S. H. & Bae, B.G., The Sensing Model of Disaster Issues from Social Big data, Journal of KIISE: Computer Systems and Theory, Vol.20, No.05, 2014.

[10] Sung, S. J., "How can we use mobile apps for disaster communications in Taiwan: Problems and possible practice," 8th Asia-Pacific Regional ITS Conference. 2011.

[11] ITWORLD, IDG Korea, "Apple's Beacon of position sensing technology operating principle", Available on http://www.itworld.co.kr/slideshow/85994, 2014.

[12] estimote, "Beacon Tech Overview", Available on http://developer.estimote.com/iBeacon/, 2012.

[13] Lee, J. P., International Journal of Applied Engineering Research, "Design of Disaster Information Collection System Base on In-memory in Crowd Sensing Environments", Vol. 5., No.1, pp217-218., 2015.

[14] Gartner, "Security and Risk Management Summit 2014", 2014.

[15] Kim, I. G., ETRI, "Big data analytics technology and cyber security", 2014.

[16] C. Davies, 95% Android game piracy experience highlights app theft challenge, Retrieved May, 15, 2013, Available on http://www.slashgear.com/95-android-game-piracy-experience-highlights-app-theft-challenge-15282064, 2013.

[17] Km, D.J., Android App Birthmarking Technique Resilient to Code Obfuscation, Journal of Korean Institute of Communications and Information Sciences, Vol.40, No.04, pp700-708, 2014.

[18] Hong, D.J., et al., International Workshop on Information Security Applications. Springer International Publishing, "LEA: A 128-Bit Block Cipher for Fast Encryption on Common Processors." 2013.

[19] IEEE Standard for Information technology, "802.11n-2009 - IEEE Standard for Information technology", Available on, https://standards.ieee.org/findstds/standard/802.11n-2009.html, 2009.

[20] KISA (Korea Internet & Security Agency), "Lightweight Encryption Algorithm", Available on https://seed.kisa.or.kr/iwt/ko/sup/EgovLeaInfo.do, 2013.

[21] NIST, "Lightweight Cryptography", http://www.nist.gov/itl/csd/ct/lwc-project.cfm, 2015.

AUTHORS

Lee Jae Pil

Obtained his Bachelor of engineering from Joongbu University, Master of Science degrees in computer science from Hannam University, South Korea. He is submitted his master's thesis on the title of Security framework of big data distributed processing environment using Hadoop. His current doctoral student, research area is in Network, Security, and Mobile Technologies.

Lee Jae Gwang

Obtained his Bachelor of engineering and Master of Science degrees in computer science from Hannam University, South Korea. He is submitted his master's thesis on the title of CCTV Mobile Monitoring System using Kinect with Linux HA. His current research area is in Sensor Network, IoT Security, and Beacon.

Lee Jun Hyeon

Obtained his Bachelor of engineering from Hannam University, South Korea. He has studied the indoor positioning algorithms to master's thesis theme. His current research interests include vulnerability analysis and the indoor positioning technology.

Yoon Gi Su

Obtained his Bachelor of Science from Chungnam University, South Korea. He is currently studying the trends and issues of Big Data with the theme of the master's thesis. His current research interests are Bluetooth Low Energy, Internet Of Things, and security.

Lee Jae Kwang

Obtained his Bachelor of Science, Master of Science and Doctorate degrees in computer science from Kangwoon University, South Korea. Prof. Jae Kwang Lee submitted his master's thesis on the title of Study on Using Text Editor Addressing Mapping Structure and Ph.D. thesis on the title of Information protection protocol in local area networks. His current research area is in Network, Security Technologies. At present he is working as a dean of research and professor of computer science in Hannam University.