http://www.icact.org/journal.asp

ICACT-TACT JOURNAL

Transactions on Advanced Communications Technology

Volume 3 Issue 5, Sep. 2014, ISSN: 2288-0003

Editor-in-Chief
Prof. Thomas Byeongnam YOON, PhD.

GIRI Global IT Research Institute

Volume. 3 Issue. 5

1 Study on design and implementation of web-based audience measurement platform for digital signage service 505

Wook Hyun*, MiYoung Huh*, SungHei Kim*, ShinGak Kang*

** Protocol Engineering Center, ETRI(Electronics and Telecommunications Research Institute), 218 Gajeong-ro, Yuseong-gu, Daejeon, Republic of Korea*

2 Multipath Channel Characteristics for Propagation between Mobile Terminals in Urban Street Canyon Environments 511

Myung-Don KIM, Juyul LEE, Jinyi LIANG, Jinup KIM

Electronics and Telecommunications Research Institute (ETRI) 218, Gajeongno, Yuseong-gu, Daejeon, 305-700, Korea

3 A TOR-Based Anonymous Communication Approach to Secure Smart Home Appliances 517

Nguyen Phong HOANG, Davar PISHVA

Institute of Information & Communications Technology, APU (Ritsumeikan Asia Pacific University), Japan

4 Smart Device Based Power Generation Facility Management System in Smart Grid 526

Young-Jae Lee*, Eung-Kon Kim*

**Department of Computer Science, Sunchon National University, 255 Jungang-ro, Suncheon, Jellanam-do, Republic Of Korea*

Study on design and implementation of web-based audience measurement platform for digital signage service

Wook Hyun*, MiYoung Huh*, SungHei Kim*, ShinGak Kang*

** Protocol Engineering Center, ETRI(Electronics and Telecommunications Research Institute), 218 Gajeong-ro, Yuseong-gu, Daejeon, Republic of Korea*

whyun@etri.re.kr, myhuh@etri.re.kr, shkim@etri.re.kr, sgkang@etri.re.kr

***Abstract*—Digital signage service provides advertisement and information to users using electronic displays with network capabilities. Compared to traditional DID (Digital Information Device) that just provides contents one-way, digital signage service can provide more advanced functionalities such as user interaction and audience measurements. By measuring audience behavior, it is possible to provide appropriate contents to user and increases advertisement effects. In this paper, we present implementations of audience measurement using Kinect camera since Kinect camera can track a human objects, distance calculation and gesture recognitions, and web-based analysis platform for audience measurement information.**

***Keyword*— audience measurement, digital signage, Kinect, AM, Web-based analysis platform, big data**

I. INTRODUCTION

DIGITAL signage service provides advertisements and useful information using terminal equipped with electronic displays, and it is also possible to aggregate information using various kinds of sensors including camera. Nowadays, digital signage services are evolving for providing interaction and more intelligence services. Especially, since digital signage terminals are installed in public space like bus stops, hallways, shopping mall, it is useful for gathering audience and ambient information. This information can be used for analysis of customer's behavior and venue characteristics.

When it comes to analyses the effectiveness of advertisement and provides interactive contents switching, it needs to extract audience behavior information. ITU-T SG16 is under standardization for audience measurement in digital signage. Different from audience measurements in IPTV that service providers already knows subscriber's information, digital signage service are targeting anonymous audience. Furthermore, it is forbidden to identify audience for privacy reason. In general, digital service providers use cameras to extract audience information, and there are several products that extract basic audience information such as ages and gender. In order to extract advanced attribute of audience's behavior, we uses Kinect[1] to extract height, distance, direction and staying duration, and OpenCV[2] for gender detection and deciding whether audience is watching or not. Each digital signage terminal downloads policies for audience measurement from preference server that resides in service provider's domain. Since audience information is reported periodically from massive number of digital signage terminals continuously, the information need to be stored into big data systems rather than using file systems for further analysis. We have surveyed several candidates for storing these log messages, and we have used mongoDB for this.

In this paper, we present brief surveys of standardization on audience measurement in digital signage services and related products regarding audience measurement in chapter 2, architectural service model for web-based audience measurement platform of our digital signage service in chapter 3, audience metrics and implementation of audience measurement functionalities using Kinect and OpenCV in chapter 4 and 5, and implementations of web-based audience measure platform in chapter 6. We conclude in chapter 7.

II. RELATED WORKS

In ITU-T Q14/SG16, the standard for audience measurement in digital signage is under development. Figure 1 shows a generic digital signage architecture including audience measurement. Terminal device can have audience measurement (AM) client, and the measured information will be delivered to AM aggregation in service provider's domain.

Manuscript received September 15, 2014. This research was supported by the ICT Standardization program of MSIP (The Ministry of Science, ICT & Future Planning).

W. Hyun. Author is with the Protocol Engineering Center of ETRI, 218 Gajeong-ro, Yuseong-gu, Daejeon, Republic of Korea (corresponding author : phone: +82428601565; fax: +82428615404; email: whyun@etri.re.kr)

M.Y.Huh. Author is with the Protocol Engineering Center of ETRI, 218 Gajeong-ro, Yuseong-gu, Daejeon, Republic of Korea (email: myhuh@etri.re.kr)

S.H.Kim. Author is with the Protocol Engineering Center of ETRI, 218 Gajeong-ro, Yuseong-gu, Daejeon, Republic of Korea (email: shkim@etri.re.kr)

S.G.Kang. Author is with the Protocol Engineering Center of ETRI, 218 Gajeong-ro, Yuseong-gu, Daejeon, Republic of Korea (email: sgkang@etri.re.kr)

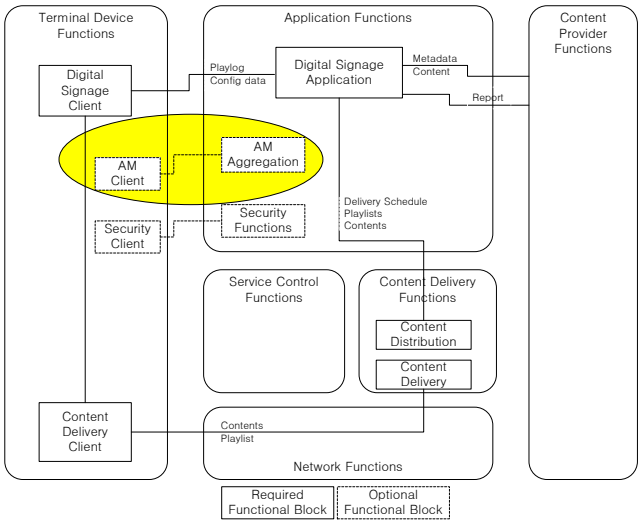


Figure 1. Generic digital signage architecture with audience measurement[3]

The audience measurement functionality of our implementation will be embedded into AM client of terminal device. It gathers audience and ambient information using various sensors, and report to AM aggregation functions. In this paper, we use Kinect 3D camera to extract related metrics.

As well as standardization, there are several prototypes that extract audience metrics such as gender and ages using generic 2D camera.

Figure 2. Prototypes supporting audience measurement in Digital Signage Expo 2013[4] and Digital Signage Japan 2013[5]

Figure 2 shows several products regarding audience measurement. As shown in Figure 2, most prototypes provide detections for gender and ages since these are most important factors for evaluation of advertisement. In this paper, we have used Kinect 3D camera, since Kinect camera trace human objects, distance calculation, moving directions of audience and gesture recognitions.

III. Architectural Model for Web-based Audience Measurement Platform within Digital Signage Systems

We designed digital signage server and terminal systems to be implemented as a web application using Tomcat 6.0[7].

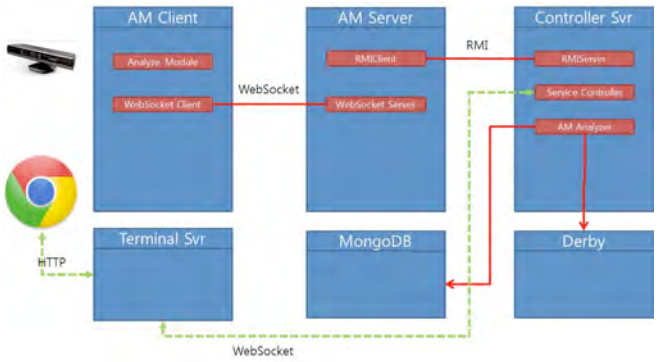


Figure 3. Architectrual model for audience measurement in digital signage system

As shown in Figure 3, the digital signage terminal is consists of AM client application and terminal server. The terminal server is a web application that is running on WAS platform, and it is implemented *Java*. The AM client application is implemented *C++* since it must use *Kinect* SDK library and *OpenCV* library. When digital signage application boots up, it retrieves operation policy from remote controller signage server. The policy includes play schedule, configuration of terminal that contains AM configuration and log server address. Whenever it generates AM report message, it sends it by using *WebSocket* to AM server that will be located in digital signage service operator

A. Audience Measurement Client Module

This module receives video stream from Kinect camera, and extracts audience metrics using Kinect SDK and OpenCV library. When it extracts audience information, it sends the record to remote digital signage server by use of WebSocket [8].

B. Local Terminal Server

Since digital signage terminal is designed to use generic web browser, it needs to build local web application server that prepares contents prior to play. As well as contents repository, it also acts as agency that receives configuration regarding audience measurement policies such as resolution, reporting frequency, reporting destination, etc.

C. Audience Measurement server

Unlike previous version of AM server [10], we have re-implemented it to use socket server, since the AM server does not need to be implemented as a web application server. When it receives AM report message, it just stores it to mongoDB for further analysis. When it needs to interact with controller server, it uses RMI (Remote Method Invocation), since those servers are tends to be located within service provider's domain.

D. Service Controller server

The service controller server manages overall digital signage services, and it provides web-based advertisement effect analysis. In this paper, an advertiser or administrator can take measures of effectiveness of advertisements or terminals by use of web browser. This server is designed to run as Web application server on top of tomcat server.

In order to provide web-based analysis of the AM information, we have designed user interface as shown in figure 4.

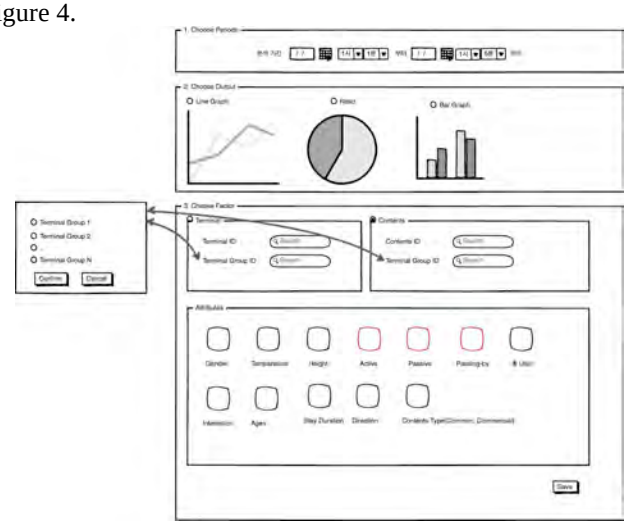


Figure 4. Design of web-based analysis user interface

It is designed to provide three types of graph; line graph, ratio graph and bar graph. An user can select the type of output for visual analysis of the result. In order to simplify the procedure, the analysis can be performed on one terminal group or one terminal. Since digital signage terminals are turned on during the service, it will accumulate huge volume of information; hence, it uses *MongoDB* [9] for storing the audience measurement information.

This platform can provide followings, but not limited;

- The number of audience as per time
- The number of audience as per temperature
- Stay duration for a specific content
- The moving pattern of audience as per time

Since our AM client does not support temperature sensor, it fetches the information from 3rd party open API services with the location information of the terminal. It is also possible to complex analysis by composing multiple conditional attributes, since this platform supports multiple selections of attributes for analysis.

IV. AUDIENCE METRICS DERIVED FROM AM CLIENT APPLICATION

Table 1 shows audience metrics that will be embedded into log message. When it comes to report log message, it should contain terminal identifier since terminal is installed in various location. This information is used for analysis of venue characteristics.

TABLE 1. METRICS FOR AUDIENCE MEASUREMENT

Element	*Attribute*	*Description*
TerminalId		Terminal identifier
ContentId		Content identifier that has been played
DateTime		Date and time for the log
Noise		Ambient noise (dB)
AudioVolume		Audio Volume (dB)
MoveInfo		Moving information of audience
	Direction	Direction (L2R, R2L)
	InTime	The time that audience come into the sight of camera
	OutTime	The time that audience go out from the sight of camera
Presence		Presence Detection Value
Audience	Count	Total number of audience
Person	Id	Identifier for differentiating each human object
Gender		Gender
Age		Rough Age
Distance		Distance between camera and audience
Height		Height of audience
Watching		Watching/Not watching

As well as venue characteristics, it is also possible to analyse the relevance with content that had been played at the time. This is useful for evaluating advertisement effect. Since we have used 3D camera, it is possible to extract moving direction, stayed duration, height and distance. Other metrics are derived from *OpenCV* library.

```
<audience-measurement>
    <terminal-id>terminal-1</terminal-id>
    <content-id>content-3</content-id>
    <date-time>2012/09/23 11:30:34</date-time>
    <noise>80</noise>
    <volume>60</volume>
    <movement-list>
        <movement direction="Left"
              enter-time="2012/09/23 11:30:40"
              exit-time="2012/09/23 11:30:50"/>
        <movement direction="Right"
              enter-time="2012/09/23 11:30:43"
              exit-time="2012/09/23 11:30:55"/>
    </movement-list>
    <presence>True</presence>
    <audience-list count="2">
        <audience>
            <gender>Male</gender>
            <age>20</age>
            <distance>100</distance>
            <height>170</height>
            <watching>True</watching>
        </audience>
        <audience>
            <gender>Female</gender>
            <age>40</age>
            <distance>150</distance>
            <height>150</height>
            <watching>True</watching>
        </audience>
    </audience-list>
</audience-measurement>
```

Figure 5. Example log message for measured audience metrics

Especially, moving direction of audience can be used for analyzing traffic pattern in accordance with time. This can be used for authoring content for effective advertisements, and advertisement strategy.

Figure 5 shows an example log message expressed using XML.

V. IMPLEMENTATION OF AUDIENCE MEASUREMENT USING KINECT CAMERA

In this chapter, we describe implementation details. We have implemented AM client in Windows OS environment, and used *OpenCV* for image processing in order to acquire gender and eye detection as shown in table 2.

TABLE 2. DEVELOPMENT ENVIRONMENT

OS	*Windows 7/Visual Studio 10*
Library	*Kinect SDK 1.6* *OpenCV*

A. Audience measurement procedure

When the AM client boots up, it initializes two modules as shown in Figure 5 after retrieving the configuration from local WAS. In order to construct internal model (*Initialize_openCV*) for analysing face, eye and gender detection, it loads pre-configured image for training. It also initializes and registers call back function (*KinectProc*) for controlling Kinect camera.

The call back function *KinectProc* takes event and streams from camera and performs main analysis.

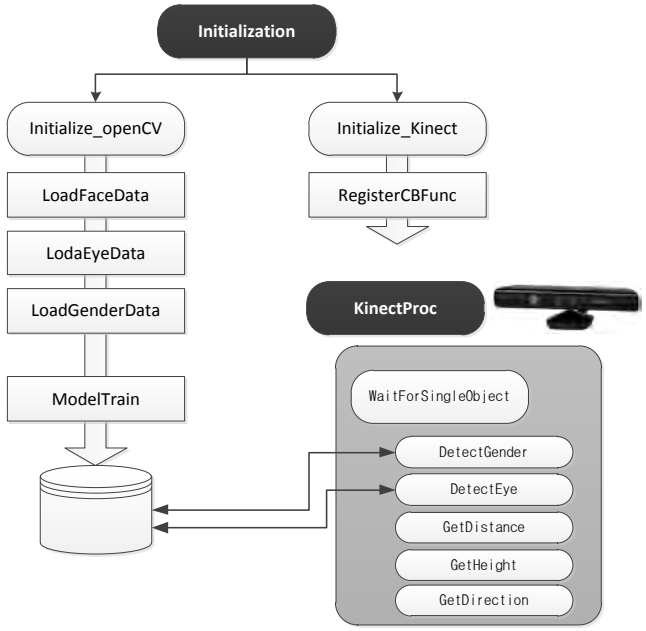


Figure 6. Example log message for measured audience metrics

When it comes to analyze gender and eye detection, it passes the vector data and images into model analyzer constructed within *openCV* library. The distance, height and direction data are coming from Kinect SDK. When the analysis is completed, it construct log message as shown in Figure 4, and sends it to remote log server using *WebSocket*.

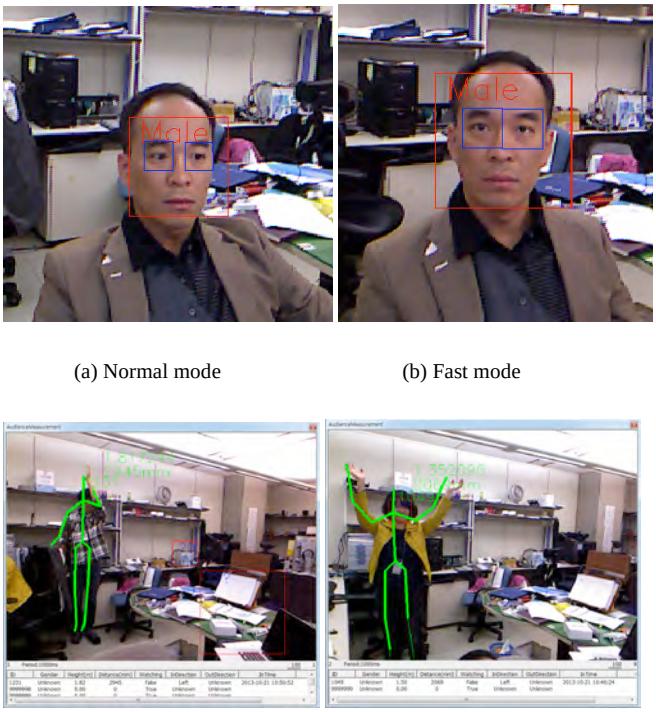
B. Acquisition mode of AM data

Since it takes time to analyse acquired image from camera depends on the size of crop area effects the performance, we have defined four level of analysis as shown in table 3.

TABLE 3. PARAMETERS AND IT'S VALUES FOR FACE DETECTION

Mode	Parameters	Value
Fastest	LogTick	50ms
	FaceDetectSize	180pixel
	EyeDetectSize	50pixel
Fast	LogTick	200ms
	FaceDetectSize	120pixel
	EyeDetectSize	30pixel
Normal	LogTick	500ms
	FaceDetectSize	80pixel
	EyeDetectSize	20pixel
Slow	LogTick	1000ms
	FaceDetectSize	30pixel
	EyeDetectSize	5pixel

In case of *fastest* mode, it generates a log every 50ms. Hence, it generates 200 messages in a second, but it has some limits on producing accurate data due to lack of time for analysis. When we used *slow* mode, it can extract most of metrics what we want. By the way, since Kinect SDK can support tracking of maximum four number of person simultaneously, metrics derived from Kinect is constrained. However, some metrics from *openCV*, such as number of person, gender and eye detection, are not limited since it just extracts those metrics by using image processing engine of *openCV* rather than using Kinect SDK. In this case, Kinect is just used as a source of image.



(a) Normal mode (b) Fast mode

(c) Height and distance detection using Kinect in *normal* mode

Figure 7. Extraction of audience metrics using AM client

Figure 6(a) shows a face detection using *normal* mode, and (b) shows in *fast* mode. The size of crop region in Figure 6(b) is slightly larger than Figure 6(a) as configured in table 3. The lower column of Figure(c) shows extracted metrics including gender, height, distance and eye detections.

C. Report of AM data

The AM information is delivered to AM server by using WebSocket with XML format like Figure 4. This report will be transformed into JSON format for storing into MongoDB.

VI. IMPLEMETATION OF WEB-BASED AUDIENCE MEASUREMENT PLATFORM

In this chapter, we describe procedures of web-based audience measurement platform briefly.

A. Audience measurement server operation

When AM server boots up, it establish RMI connection with controller server for retrieving preference information such

as port number that AM server should listen through step1~3. When it is ready, AM client sends report message to this server using WebSocket as shown in step 4. The AM server converts XML data into JSON format to insert mongoDB systems.

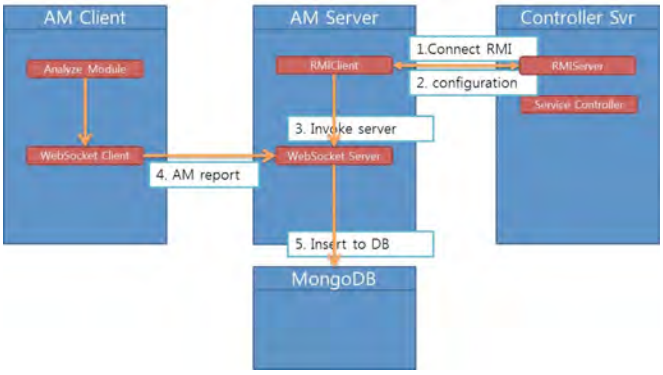


Figure 8. Procedures for audience measurement server

B. Analysis of advertisement effect procedures

When a customer or operator wants to take an analysis on the effect of advertisement, it is needed to specify period, output format, target terminals, attributes to be analyzed as shown in step 1 of Figure 9. When it submits the analysis profiles to controller server, it gives an order to pull data from *mongoDB* for specified criteria as shown in step 2. The result record will be stored into derby database for showing the result as a format of graph. When the analysis is completed, the platform notifies it to user for checking out the result.

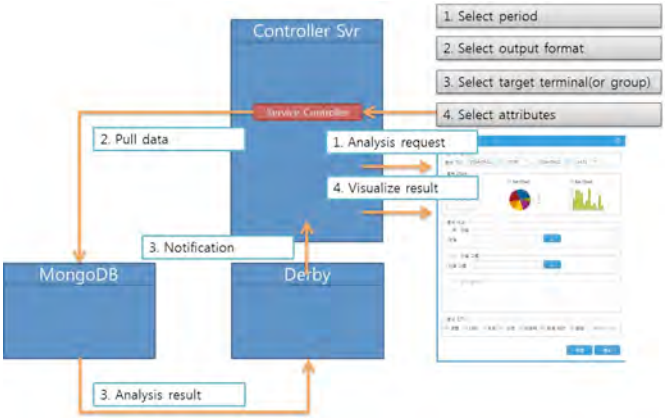


Figure 9. Procedures for measuring advertisement effect

The Figure 10 shows an interface of composing analysis request. As shown in the figure, it can express the result with three types of graph; line, bar and pie chart. It is possible to analize for one terminal, and it is also possible to do it for serveral terminals within a same group. These analysis can be used for installation strategy and setting up charing policy for an advertisement. It is also possible to make a advertisement plan based on the types of users and their behaviors on a specific terminal or terminal group.

This implementation supports of analysis on of gender, height, stayed duration and moving direction, and those attributes are gathered from *Kinect* devices.

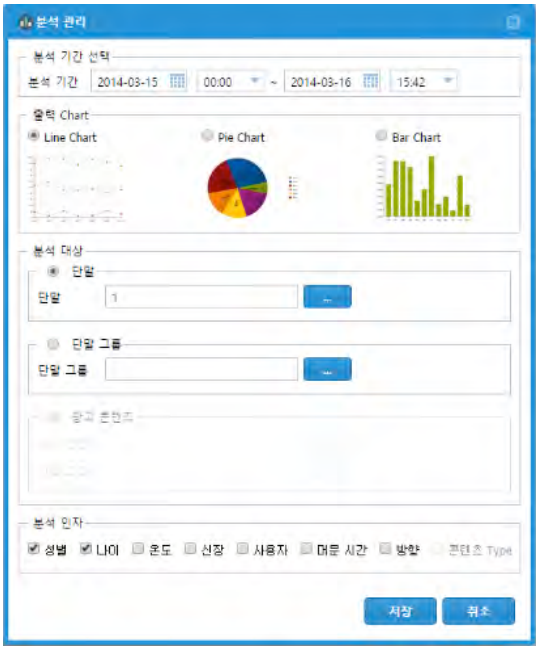


Figure 10. Web-based analysis of audience measurement data

Some attributes such as ages, temperature are not fully supported at this time, since those attributes are not gathered.

VII. CONCLUSIONS

In this paper, we have presented architectural model for web-based audience measurement platform for digital signage systems, and details regarding implementation of audience measurement functionalities collaborated with web technologies. By use of 3D camera, we can get more attributes of audience, such as distance, height, directions, etc. These metrics can be used for better marketing strategy with additional analysis on aggregated audience measurement data. For storing and analysing audience measurement information, we have used MongoDB, since there are lots of information would be stored. By use of this platform, it is possible to compose basic analysis on effect of advertisement by advertiser without any help of digital signage service provider by their own.

ACKNOWLEDGMENT

This research was supported by the ICT Standardization program of MSIP (The Ministry of Science, ICT & Future Planning).

REFERENCES

[1] Kinect , “http://www.microsoft.com/en-us/kinectforwindows/”
[2] OpenCV – Open Source Computer Vision, “http://opencv.org/”
[3] ITU-T Q14/SG16, H.DS-AM, “Audience Measurement for Digital Signage”, May, 2013
[4] H.780, “Digital signage: Service requirements and IPTV-based architecture”, ITU-T, 2012.06
[5] Digital Signage Expo 2013, “http://www.digitalsignageexpo.net/”
[6] Digital Signage Japan 2013, “http://www.f2ff.jp/dsj/2013/en/”
[7] Apache Tomcat, http://tomcat.apache.org/
[8] The WebSocket API, http://www.w3.org/TR/2011/WD-websockets-20110929/
[9] MongoDB, http://www.mongodb.org/
[10] W.Hyun, “Study on design and implementation of audience measurement functionalities for digital signage service using Kinect camera”, p597~600, ICACT 2014.

Wook Hyun is a research staff member with ETRI (Electronics and Telecommunications Research Institutes) since 2000. He has received M.S. degree in Information Communication Engineering from Chungnam National University, Korea in 2000. His research interests include VoIP, SIP, NGN, P2P, overlay networking and digital signage.

MiYoung Huh is a research staff member with ETRI (Electronics and Telecommunications Research Institutes) since 1990. She has received M.S. degree in Information Communication Engineering from Chung Nam National University, Korea in 2004. Her research interests include VoIP, SIP, IPTV, and Digital Signage.

Sung Hei Kim is a research staff member with ETRI (Electronics and Telecommunications Research Institutes) since 1991. She has received M.S. degree in Computer Science from Chung Nam National University, Korea in 1995. Her research interests include network management, NGN, service engineering, multicasting, P2P systems, and overlay networking.

ShinGak Kang received the BE and MSE in electronics engineering from Chungnam University, Korea, in 1984 and 1987, respectively and the Ph.D. degree in engineering from Chungnam University, Korea, in 1998. He is working for ETRI since 1984. Since 2008, he is a professor of the school of engineering, University of Science and Technology, Korea. His research interests include VoIP, IPTV, and future network.

Multipath Channel Characteristics for Propagation between Mobile Terminals in Urban Street Canyon Environments

Myung-Don KIM, Juyul LEE, Jinyi LIANG, Jinup KIM

Electronics and Telecommunications Research Institute (ETRI)

218, Gajeongno, Yuseong-gu, Daejeon, 305-700, Korea

mdkim@etri.re.kr, juyul@etri.re.kr, liangjinyi@etri.re.kr, jukim@etri.re.kr

***Abstract*—In this paper, we focus on multipath channel characteristics of low–height antenna links for mobile to mobile communications in urban street canyon environments. We present a wideband MIMO channel sounder and antennas used to measure multipath channel characteristics in the 3.7GHz frequency band and the result of calibration test to evaluate a system performance before field measurement. We carried out channel measurement campaigns in typical urban street canyon environments in Seoul, Korea. The root mean square (r.m.s.) delay spread and angular spread characteristics are analyzed with results of their distribution and cumulative density function (CDF) in line of sight (LoS) and non-LoS (NLoS) case respectively.**

***Keyword*—Mobile-to-Mobile, multipath characteristics, channel model, channel measurements, channel sounder**

I. INTRODUCTION

MOBILE-TO-MOBILE direct communications services, commonly known as D2D (device-to-device), are now being actively discussed in various standardization bodies, e.g., "ProSe" for the LTE-Advanced system [1]. Unlike typical rooftop cellular networks, both transmitters and receivers are generally found near street levels, since direct communication links are established between mobile terminals. Consequently, conventional propagation models are limited in their ability to predict specific channel environments and those characteristics for development of the direct communication system using a system or link level channel simulation.

Recently, new prediction methods and channel characteristics for propagation between mobile terminals based on field measurement in various outdoor environments are reported widely. Lu et al [2] developed simplified site-specific path loss formulas for street grids. They assumed that surrounding buildings are infinitely high so that "vertical plane" effects can be ignored. Considering reflection and diffraction along with the horizontal plane, they developed path loss formula based on two-ray models, which can account for up to two-turn NLoS links. M. Sasaki [3] proposed a new path loss model for propagation between terminals located below roof-top in residential environments. J. Lee et al [4] investigated the effects of surrounding building heights on path loss characteristics, especially in urban street grid environments in Korea. From the comparison results of the ITU-R propagation models such as ITU-R Recommendation P.1411 [5] and Report M.2135 [6], it is noted that conventional channel models are overestimated and the path loss characteristics can be affected by surrounding building heights. Furthermore, from the aspect of radio propagation between low-antenna terminals in high-rise environment, reflected waves at corners in horizontal plane seem to play a dominant role. Most of these researches are relevant to the path loss characteristics for mobile to mobile direct communications. However, when we consider direct communications between terminals using MIMO antennas, the study of multipath characteristics (i.e. delay spread, angular spread, etc.) is also very important.

This paper investigates multipath channel characteristics for propagation between mobile terminals based on channel measurements in Seoul, Korea. Section II presents a wideband MIMO channel sounder used to measure multipath channel characteristics, and the result of calibration measurement to evaluate a system performance before field measurement. In Section III and Section IV, the field measurement campaign and analysis results of multipath characteristics such as delay spread and angular spread are described. Finally, to wrap up the work, conclusions are given in Section V.

Manuscript received September 8, 2014. This work was supported in part by the MSIP (Ministry of Science, ICT & Future Planning), Korea in the ICT R&D Program 2014, "Development of core technologies to improve spectral efficiency for mobile big-bang (14-000-01-002)". (Corresponding author: +82-42-860-6178; fax: +82-42-860-6732; e-mail: mdkim@etri.re.kr)

Myung-Don Kim is Principal Researcher with the Electronics and Telecommunications Research Institute, Daejeon, Korea (+82-42-860-6178; fax: +82-42-860-6732; e-mail: mdkim@etri.re.kr).

Juyul Lee is Senior Researcher with the Electronics and Telecommunications Research Institute, Daejeon, Korea (+82-42-860-5503; fax: +82-42-860-6789; e-mail: juyul@etri.re.kr).

Jinyi Liang is Researcher with the Electronics and Telecommunications Research Institute, Daejeon, Korea (+82-42-860-5289; fax: +82-42-860-6732; e-mail: liangjinyi@etri.re.kr).

Jinup Kim is Principal Researcher with the Electronics and Telecommunications Research Institute, Daejeon, Korea (+82-42-860-5423; fax: +82-42-860-6789; e-mail: jukim@etri.re.kr).

II. Measurement System and Calibration of System Performance Before Measurement

A. Wideband MIMO Channel Sounder

Measurement campaigns were conducted with the wideband MIMO channel sounder system developed at Electronics and Telecommunications Research Institute (ETRI), which can measure multipath characteristics in the 3.7 GHz frequency with 100 MHz bandwidth [7][8]. Table I represents a detailed specification of the channel sounder which can measure the channels received from multiple antenna elements and estimate multipath components with a time delay resolution of 10 ns.

TABLE I
Specification of Channel Sounder and Measurement Configurations

Items	Specifications
Frequency	3.7 GHz
Channel bandwidth	100 MHz
PN code length	2047 chips
Maximum Tx power	36 dBm
Multipath Resolution	10 ns (3m)
Frequency stability	10^{-11}
Number of Antenna elements	TX: 8 UCA, RX:8 UCA

For the measurement campaign, we installed a transmitter (TX) and a receiver (RX) channel sounder in separate vehicles respectively as shown in Fig. 1. A uniform circular array (UCA) antenna which has eight vertically polarized elements aligned circularly with a spacing of 0.5 λ is mounted on the rooftop of each vehicle with the height of 1.9 meters.

Fig. 1. Installation of channel sounder system and antennas (mounted on the rooftop of vehicle) for channel measurement campaign

B. System Calibration Measurement and Results

Before measurement campaign, we have conducted a system calibration measurement at ETRI playground (open space) with channel sounders (a transmitter and a receiver) and antenna arrays. For this measurement, full radiation patterns of all the elements of each array antenna were measured in the anechoic chamber in advance. The azimuth plane radiation pattern with two polarizations (vertically and horizontally from -180° to +180°) and the elevation plane (from -45° to +45°) have been obtained enabling the estimation of the spatial channel characteristics. Fig. 2 depicts a configuration of this test. The position of a transmitter (TX) was fixed, and a receiver (RX) was located at 9 m away. The UCA8 array antennas for both TX and RX were installed on the ground with a height of 1.5 m. We measured a channel from TX to RX, and changed the position of the RX and collected measured samples of total 8 points with different angles (θ = 0°, 45°, 90°, 135°, 180°, -45°, -90°, -135°).

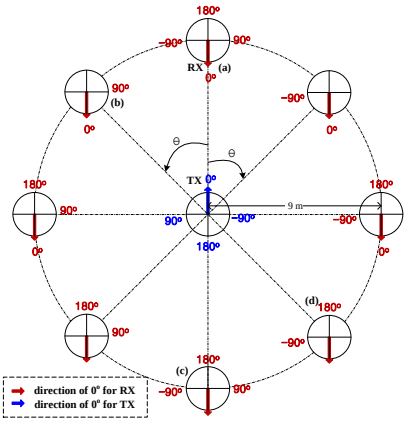


Fig. 2. Configuration of calibration measurement for channel sounders (TX-RX) and antennas

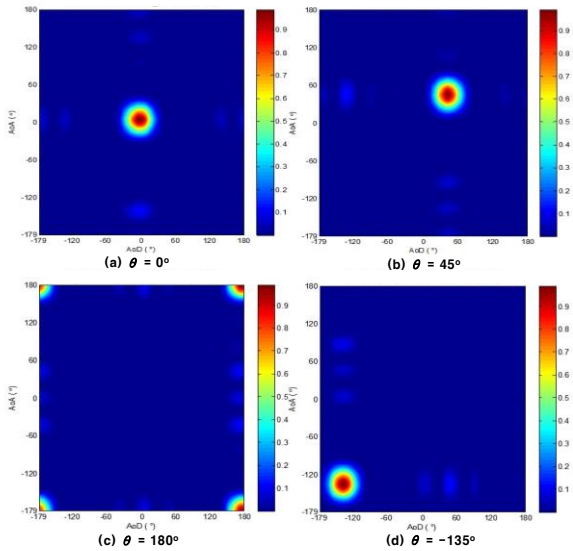


Fig. 3. Estimated result of AoA and AoD at the position of θ

In this paper, we observed the estimated results of an angle of departure (AoD) and an angle of arrival (AoA) by using a Barlett beam-forming method [9]. Fig. 3 shows estimated results of AoA and AoD at each point of θ. We can see that a dominant path component having the strongest channel power (red part) starts from each angle of 0°, 45°, 180° and -135° and correctly arrives at each angle of 0°, 45°, 180° and -135° in Fig. 3(a)-(d). From this measurement results, the performance of our channel sounders was evaluated, and we confirmed the ability to estimate time and spatial characteristics of multipath channels through field measurement campaign.

III. Measurement Campaign

To obtain multipath characteristics in urban street canyon environments, we conducted a measurement campaign at 3 sites which are carefully selected places among typical urban low-rise, high-rise, and very high-rise environments in Korea. All sites are composed of rectilinear flat street grids, but their average building heights are different, as specified in Table II.

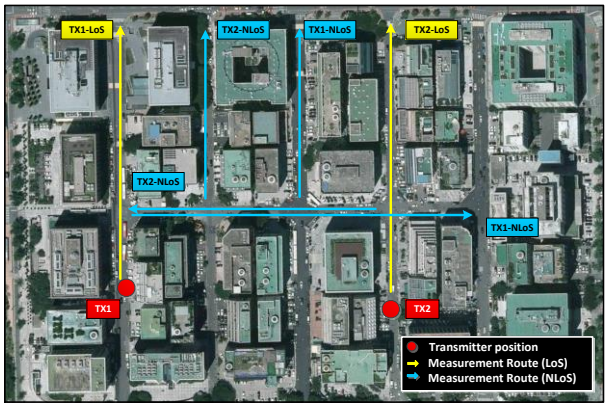
Fig. 4 shows the measurement routes and surrounding environment of each area. The measurement campaigns were performed along the planned routes in three different sites

respectively. Each site has two TX points i.e. TX1 and TX2, and all RX positions for LoS and NLoS scenario assigned along the road as shown in the map.

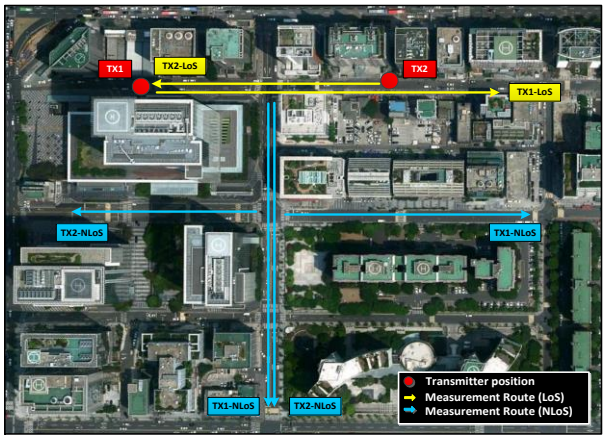
TABLE II
MEASUREMENT SITES AND ENVIRONMENTS

Sites	Class	Location	Feature
Site 1	Urban low-rise	Ilsan, Seoul	Low-rise buildings (3-5 story, 11-14m height) are located at both side of 2 lanes road (avg. 18 m wide)
Site 2	Urban high-rise	Yeouido, Seoul	A commercial area where high-rise buildings (10-15 story, 35-45m height) are located at both side of 2 lanes road (avg. 24 m wide)
Site 3	Urban very high-rise	Gangnam, Seoul	A downtown area with skyscrapers where very high-rise buildings (50-195m height) are located at both side of 2-4 lanes road (avg. 26 m wide)

(a) Site 1



(b) Site 2



(c) Site 3

Fig. 4. Measurement routes and environments of each site ((a) Site 1: Ilsan area, (b) Site 2: Yeouido area, (c) Site 3: Gangnam area)

The measurement campaigns were taken during daytime and outside of normal rush hours, when few people are on sidewalks and vehicle traffic running at about 30km/h. During measurement, we held the TX vehicle at a stationary position and moved the RX vehicle at a speed under 10 km/h along measurement routes. The RX channel sounder collected measured data including channel impulse responses and GPS information.

IV. MEASUREMENT RESULTS AND ANALYSIS

We analyzed multipath channel characteristics such as r.m.s delay spread and angular spread of arrival from measured results.

A. r.m.s delay spread

The r.m.s delay spread (DS) is the standard deviation value of the delay of multiple paths, and it is weighted proportional to the energy in the reflected waves. To obtain delay spread from measured data, we estimate the multipath components from power delay profile (PDP) from measured channel impulse responses (CIRs). CIRs can be obtained from the auto/cross-correlation function between an original PN sequence and a received signal as follows:

$$h_{mn}(\tau)=\frac{R_{xy}(\tau)}{R_{xx}(0)}=\frac{\mathcal{F}^{-1}(-X(f)^{*}\cdot Y(f))}{\sum_{i}|x(\tau_i)|^2} \quad (1)$$

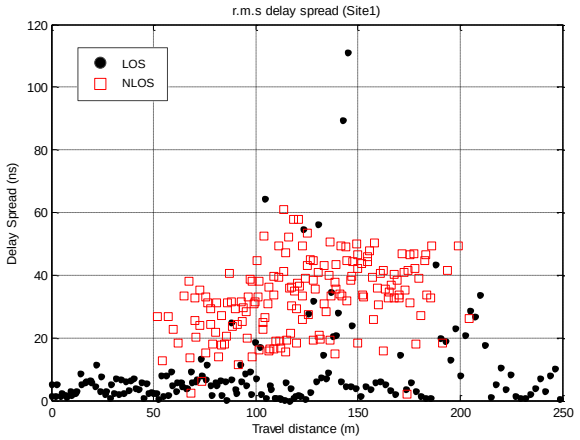
, where $Y(f)$ is a Fourier transform of the received signal $y(\tau)$, $x(\tau)$ is a sequence for transmission, R_{xx} means an auto-correlation to remove a system impairment [9], and $R_{xy}(\tau)$ means a cross-correlation of $x(\tau)$ and $y(\tau)$.

The power delay profile (PDP) can be calculated by:

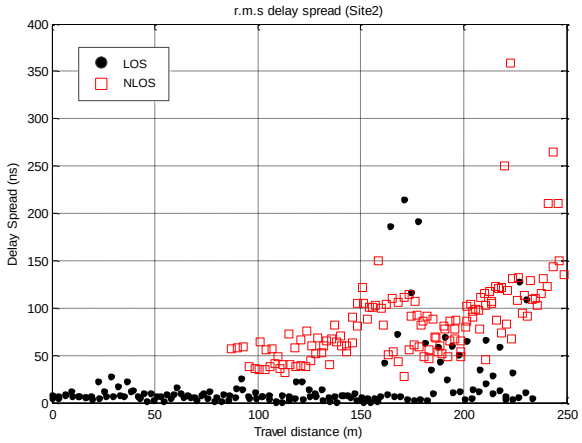
$$PDP(\tau)=\sum_{n=1}^{N}\sum_{m=1}^{M}|h_{mn}(\tau)|^2 \quad (2)$$

, where $h_{mn}(\tau)$ has an N × M matrix (n and m are the index of Rx and Tx antennas respectively). To extract multipath components, we set a threshold (20 dB below the peak level in this paper) considering the dynamic range of channel impulse responses [11], and then pick the multipath components $h(\tau_l)$ with a related delay τ_l, $l=1:L$. L is a total number of multipath components founded within threshold. Finally, delay spread can be calculated by the same method in [11].

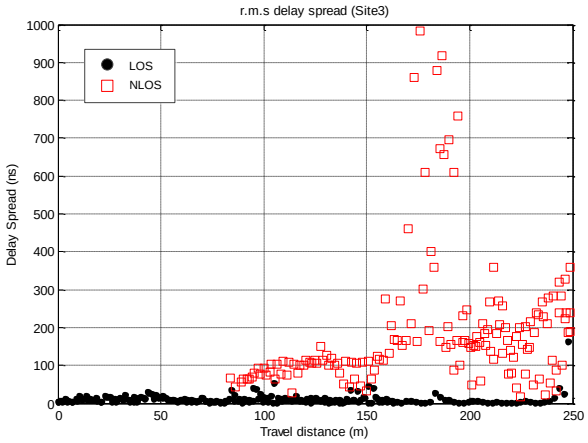
Fig. 5 shows the distribution of r.m.s. DS values corresponding to travel distance between the TX station and RX station for each scenario (LoS and NLoS) and environments (urban low-rise, urban high-rise and urban very high-rise). From the measurement results, we can see that distributed DS values of the NLoS are much larger than the LoS for all sites. Furthermore, in case of NLoS, we can observe that the DS values are gradually increased proportion to the distance. In addition, the cumulative distribution functions (CDF) of the delay spread for LoS and NLoS cases are plotted in Fig. 6.



(a) Site 1



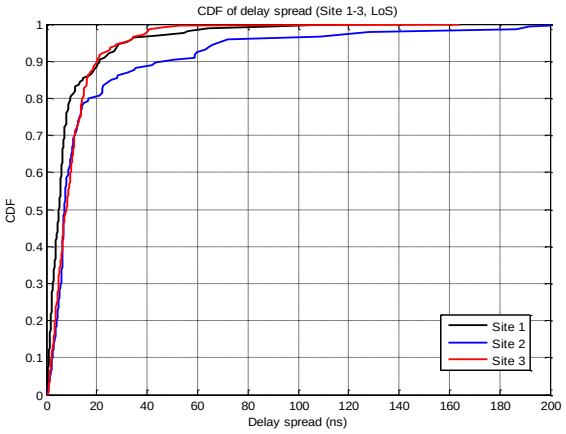
(b) Site 2



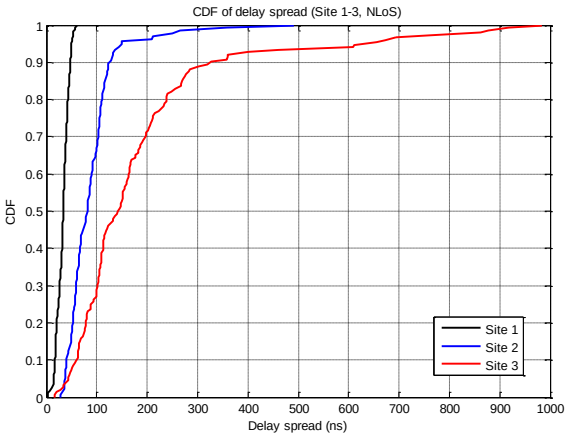
(c) Site 3

Fig. 5. Measurement results of r.m.s. delay spread corresponding to Tx-Rx distance ((a) Site 1: urban low-rise environment, (b) Site 2: urban high-rise environment, (c) Site 3: urban very high-rise environment)

We summarize the measured r.m.s. delay spread for the different cases with cumulative probability of 10%, 50% and 95% as shown in Table III. When we compared median values (50% of CDF) of r.m.s. delay spread in Table III, Site 3 (urban very high-rise environment) has the largest value, Site 2 (urban high-rise environment) has a medium, and Site 1 (urban low-rise environment) has the smallest value. From this result, we can understand that the higher buildings around the TX or the RX station, the more multipath components can be generated.



(a) LoS cases



(b) NLoS cases

Fig. 6. CDF of delay spread for LoS and NLoS scenarios (site 1 to 3)

TABLE III
MEASUREMENT RESULTS OF R.M.S DELAY SPREAD

Sites	Class	Scenario	r.m.s. delay spread (ns)		
			10%	50%	95%
Site 1	Urban low-rise	LoS	0.9	5	31.9
		NLoS	16.7	33.1	50
Site 2	Urban high-rise	LoS	2.2	7.1	69
		NLoS	40.5	81.3	149.4
Site 3	Urban very high-rise	LoS	2	8.1	31
		NLoS	58	142	610.5

B. *r.m.s angular spread*

The r.m.s. angular spread is the power-weighted standard deviation of the direction of arrival and departure, and it is given by the second moment of the power angular profile [11]. We calculate the power azimuth spectrum (PAS) corresponding to the only founded multipath components. The PAS calculation function is based on Bartlett beam-forming theory [9], which is written as follows:

$$PAS_i(\varphi_{\mathrm{AOA}}) = \left|\Omega_{\mathrm{RX}}(\varphi_{\mathrm{AOA}}) \cdot h_{mn}(\tau_{\mathrm{i}})\right|^2 \quad (3)$$

, where Ω_{RX} is a radiation pattern of RX antennas (360 x N matrix), and φ_{AOA} is an angle of arrival.

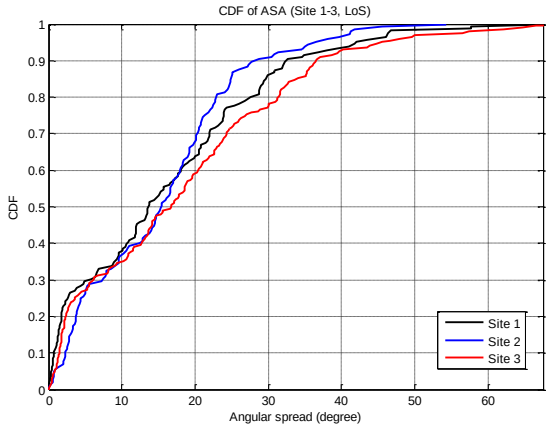
Then, to overcome the limitation of angular resolution for estimation of direction of arrival using a small number of antenna elements [12], we find the peak angle φ_l from the

result of PAS as below:

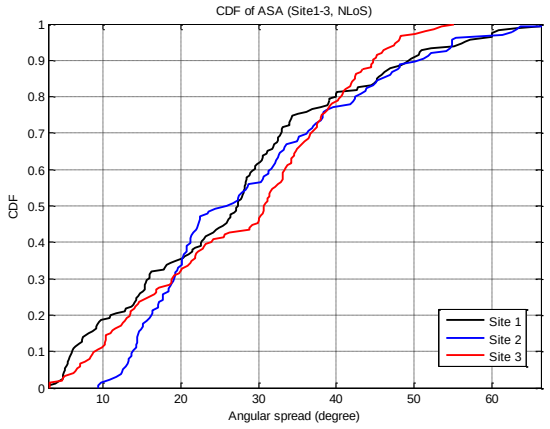
$$\varphi_l = arg\max_{\varphi}\{\mathrm{PAS}_l(\varphi_{\mathrm{AOA}})\} \quad (4)$$

After all, we obtained the r.m.s. angular spread of arrival from extracted coefficients such as arrival angle φ_l and related power for each multipath components.

Fig. 7 depicts the CDF curves of the angular spread of arrival (ASA) for LoS and NLoS case, respectively. When we observed the distribution of ASA values, they are not increased or decreased depending on the distance, but the case of NLoS is highly distributed than the LoS for all environments.



(a) LoS cases



(b) NLoS cases

Fig. 7. CDF of angular spread of arrival for LoS and NLoS scenarios

TABLE IV
MEASUREMENT RESULTS OF R.M.S ANGULAR SPREAD

Sites	Class	Scenario	r.m.s. angular spread (degree)		
			10%	50%	95%
Site 1	Urban low-rise	LoS	0.7	13.6	42
		NLoS	6.1	27.3	56.6
Site 2	Urban high-rise	LoS	2.3	15.4	36.5
		NLoS	13.9	25.9	54.9
Site 3	Urban very high-rise	LoS	1.5	16.7	45.6
		NLoS	8.7	30.7	47.5

Table IV summarizes the measured results of r.m.s. angular spread with the probability of 10%, 50% and 95% for the different environments and scenarios. We can observe that the median values (50% of CDF) of r.m.s. angular spread in NLoS cases are higher than the LoS cases for all environments. Furthermore, the height of surrounding building seems to affect the angular spread characteristics at 50%, but not much at other probabilities.

V. CONCLUSION

In this paper, we investigated the multipath channel characteristics between mobile terminals with low-height antennas considering for mobile-to-mobile communication scenarios. We carried out channel measurement campaigns in the 3.7GHz frequency band in three different urban street canyon environments. In our measured results, r.m.s delay spread values of the NLoS case are much larger than the LoS for all sites. Furthermore, especially in case of NLoS, we can observe that the DS values are gradually increased proportion to the distance. On the other hand, r.m.s. angular spread values are not looked increase or decrease depending on the distance in those circumstances. The ASA values in case of NLoS are highly distributed than LoS case for all environments. The height of surrounding building, in particular at 50% of CDF, seems to slightly affect the angular spread characteristics. This issue should be further studied on the basis of more measurement data. The statistical angular characteristics of departure (ASD) are expected to similar with those of arrival based on reciprocity if two mobile terminals are located at the same environment and scenario.

REFERENCES

[1] 3GPP TR 22.803, Feasibility study for Proximity Services (ProSe), Mar. 2013.
[2] J. S. Lu, H. L. Bertoni, C. Chrysanthou, and J. Boksiner, “Simplified path gain model for mobile-to-mobile communications in an urban high-rise environment,” in Proc. IEEE Sarnoff Symp., Princeton, NJ, Apr. 2010.
[3] Motoharu Sasaki, Wataru Yamada, Naoki Kita, Takatoshi Sugiyama, “Path Loss Model with Low Antenna Height for Microwave Bands in Residential Areas”, IEICE Transactions 96-B(7), pp1930-1944, 2013
[4] J. Lee, H. K. Chung and M. D. Kim, "Building Height Effects on Path Loss for Low Antenna Links in Urban Street Grid Environments", IEEE Asia Pacific Wireless Communication Symposium, Aug. 2013.
[5] Rec. ITU-R P.1411, Propagation data and prediction methods for the planning of short-range outdoor radiocommunication systems and radio local area networks in the frequency range 300 MHz to 100 GHz, Feb. 2012.
[6] Rep. ITU-R M.2135-1, Guidelines for evaluation of radio interface technologies for IMT-Advanced, Dec. 2009.
[7] J.-J. Park, M.-D. Kim, H.-K. Kwon, H.-K. Chung, X. Yin, and Y. Fu, “Measurement-Based Stochastic Cross-Correlation Models of a Multilink Channel in Cooperative Communication Environments,” ETRI Journal, vol. 34, pp. 858–868, Dec. 2012.
[8] M. D. Kim, J. J. Park, H. K. Kwon, and H. K. Chung, “Performance Evaluation of Wideband MIMO Relay Channel Sounder for 3.7 GHz,” IEEE Asia Pacific Wireless Communication Symposium, Aug. 2011.
[9] M. Barlett, “Smoothing periodograms from time series with continuous spectra,” Nature (London), vol. 161, no. 8, pp. 686–687, 1948.
[10] H. Chung, et al., “MIMO channel sounder implementation and effects of sounder impairment on statistics of multipath delay spread,” Proc. IEEE VTC, vol. 1, pp. 349–353, Sep. 2005.
[11] Rec. ITU-R P.1407, "Multipath propagation and parameterization of its characteristics", Oct. 2009.
[12] Gerd Sommerkorn, et.al. "Performance Evaluation of Real Antenna Arrays for High-Resolution DoA Estimation in Channel Sounding", COST 273 TD(03)196, Sept. 2003.

Myung-Don Kim (BS'93–MS'95) is a Principal Researcher in the Advanced Communications Research Laboratory at Electronics and Telecommunications Research Institute (ETRI). He joined ETRI, Daejeon, Rep. of Korea, in 1995, and he worked on the development of mobile test-beds for CDMA, IMT-2000 and WCDMA systems. Since 2006, he has been involved in the development of wideband MIMO channel measuring system, measurement and channel estimation of MIMO channels. His research interests include MIMO, channel measurement and channel modeling for next generation mobile communications

Juyul Lee (BS'96-MS'98-PhD'10) is a Senior Researcher in the Advanced Communications Research Laboratory at Electronics and Telecommunications Research Institute (ETRI) since 2000. Prior joining with ETRI, he was a Research Engineer with the Agency for Defense Development (ADD) from 1998 to 2000. His research spans the fields of information theory and wireless communications, with special interests in multiple-antenna/multiple-user/multi-cell resource allocations, device-to-device communications, and wireless propagation channel measurements and modeling.

Jinyi Liang (BS'04–MS'13) is a Researcher in the Advanced Communications Research Laboratory at Electronics and Telecommunications Research Institute (ETRI). He is Chinese and joined ETRI, Daejeon, Rep. of Korea, in July 2013, and he's working on the project 'Wireless Channel and Frequency Characterization based on Field Measurements for Broadband Mobile Hot-Spot Applications'. His research interests include MIMO, channel measurement and channel modeling for next generation mobile communications.

Jinup Kim (BS'85-MS'87-PhD'96) has been with Electronics and Telecommunication Research Institute since 1987. And also he has been a professor of University of Science and Technology in the field of Wireless communications since 2005. He has researched in the field of the wireless communication system. He is recently interested in the Digital RF, channel modeling, Software Defined Radio and Cognitive Radio technologies, etc.

A TOR-Based Anonymous Communication Approach to Secure Smart Home Appliances

Nguyen Phong HOANG, Davar PISHVA

Institute of Information & Communications Technology, APU

(Ritsumeikan Asia Pacific University), Japan

hoang.phong.37e@st.kyoto-u.ac.jp, dpishva@apu.ac.jp, **Fax: +81 977 78 1001, Tel: +81 977 78 1000**

***Abstract*— Digital information has become a social infrastructure and with the expansion of the Internet, network infrastructure has become an indispensable part of social life and industrial activity for mankind. The idea of using existing electronics in smart home appliances and connecting them to the Internet is a new dimension along which technologies continue to grow, and in recent years mankind has witnessed an upsurge of usage of devices such as smart phone, smart television, home health-care device, smart LED light bulbs system, etc. Their build-in internet-controlled function has made them quite attractive to many segments of consumers and smart phone has become a common gadget for social networking. There are, however, serious challenges which need to be addressed as these tiny devices are designed for specific functions and lack processing capacity required for most security software. This research explores how these internet-enabled smart devices can be turned into very dangerous spots for distributed attacks purposes by cybercriminals for various ill intensions in a pinpointed manner. It then introduces a new approach to deal with such problems by taking advantage of the anonymous communication of the Onion Router (hereafter: TOR). It compares pros and cons of using anonymous communication scheme and justifies it be an efficient countermeasure to most attack scenarios.**

***Keyword*—Smart Appliances, the Internet of Things, Security, Anonymous Communication, the Onion Router (TOR)**

I. INTRODUCTION

NOWADAYS, thanks to the impressive achievement of material science especially in semiconductor materials and nanomaterials, all the electronic devices are getting smaller in size, and microprocessors can be found in most appliances. Such developments have been leading mankind to a new era of technology, the era of the "Internet of Things" (hereafter: IoT), where all the appliances are getting tiny and controllable via the Internet, thus enabling people to enjoy network based services, such as Video on Demand (VOD), Music on Demand (MOD), remote update, e-commerce, remote control, and other similar services. Furthermore, researchers around the world have come up with an abundance of resourceful ideas on how to effectively use microprocessors and Internet in other everyday household appliances. 'Smart' has become the new buzzword that we have kept on hearing in recent years, for example, in 'smart' homes, 'smart' kitchens, 'smart' ovens, 'smart' refrigerators, etc. [1]. Table 1 indicates functional classification of smart home appliances. There is also a tremendous business potential for them because of foreseen future demand by elderly people, where the number of people over the age of 65 is expected to double to 70 million by 2030 [2]. According to a study conducted by International Data Corporation, 212 billion "things" will be installed based on IoT with an estimated market value of $8.9 trillion in 2020 [3]. Those "things" will be nothing special but daily used appliances ranging from watch, light bulb to smart television, refrigerator and so on.

TABLE I
FUNCTIONAL CLASSIFICATION OF SMART HOME APPLIANCES

No	Function	Example of Product or Usage
1	Content Retrieval	Broadband TV, Microwave Oven, HDD Recorder (for TV program, etc)
2	Content Storage/Usage	HDD Recorder (for TV program, etc), MP3 Player
3	Communication/ Messaging	VoIP , IP-TV Phone, All kinds of Emails System, Healthcare System
4	Remote Surveillance	Security Camera, Gas/Fire Sensors, Refrigerator, Lighting Fixture, Door Lock
5	Remote Control	Air Conditioner, Lighting Fixture, TV, TV Program Recording
6	Remote Maintenance	Firmware Update, Trouble Report
7	Instrument Linkage	Networked AV Equipments
8	Networked Game	Family Type Game Machine

Connecting smart home appliances to the Internet, however, makes us vulnerable to malicious attacks. An intruder can steal private information such as contact info, shopping or eating preferences, lifestyle and relaxation habits, or credit card information used to pay for such services. They can also use smart appliances as launching pads to carry out malicious attacks into other systems. Table 2 shows a list of common attacks that can be carried out through smart home appliance and the next section discusses some specific attack cases.

TABLE II
A LIST OF COMMON ATTACKS

No	Common Threat	Example of an Attack
1	User Impersonation	Impersonation using password
2	Device	Impersonation of a device using its faulty

Manuscript received on September 9, 2014. This work is a follow up of a presentation done at the 16th International Conference on Advanced Communication Technology which received Outstanding Paper Award.

Nguyen Phong HOANG is a graduate student at the Graduate School of Informatics at Kyoto University Japan (hoang.phong.37e@ st.kyoto-u.ac.jp).

Davar Pishva is a professor in ICT at Ritsumeikan Asia Pacific University (APU) Japan (corresponding author: +81-977-78-1000, fax: +81-977-78-1001, e-mail:dpishva@apu.ac.jp).

	Impersonation	certificate
3	Service Interruption	Distributed Denial of Service (DDOS)
4	Data Alteration	Data alteration of transmitted or stored data
5	Worm/Virus Infection	Infiltration and/or damaging of a computer system
6	Phishing/Pharming	Impersonation of users' destination
7	Data Wiretapping	Information leakage through wiretapping
8	Firmware Alteration	Replacing of firmware at will
9	OS/Software Vulnerability	Launching of worms and attacks using such vulnerabilities

II. Typical Attack Cases On Smart Appliances

In a previous research, the authors showed how the nature of Internet Protocol could accidentally put its user's identity into high risk of being revealed due to the existence of private information behind the IP address in the packet header, which can be easily extracted and observed by various IP tracer and deep packet inspection tools [4]. In addition, the use of sniffing tools such as Wireshark or other network monitoring applications, though not new, turn out to be very efficient for attacking IoT networks too. Table 3 shows threat likelihood level of a given smart home appliance type for a particular attack and the rest of the section briefly discusses some of the classical techniques that have recently been employed to carry some of these attacks on the smart home appliance system not only to steal personal information but also abuse the devices and make them serve cyber criminals' numerous illegal purposes.

TABLE III
THREAT LIKELIHOOD LEVEL OF A GIVEN SMART HOME APPLIANCE

No.	Common Threat / Function	1. User Impersonation	2. Device Impersonation	3. Service Interruption	4. Data Alteration	5. Worm/Virus Infection	6. Phishing/Pharming	7. Data Wiretapping	8. Firmware Alteration	9. OS/Software Vulnerability
1.	Content Retrieval	H	H	M	L	M	L	L	-	L
2.	Content Storage/Usage	-	-	L	L	M	-	L	-	L
3.	Communication /Messaging	H	H	M	L	M	M	L	-	L
4.	Remote Surveillance	H	H	L	L	L	L	L	-	L
5.	Remote Control	H	H	H	H	L	L	L	-	L
6.	Remote Maintenance	H	H	H	M	L	L	L	L	L
7.	Instrument Linkage	M	M	M	L	L	L	L	-	L
8.	Networked Game	H	H	H	M	M	L	L	-	L

A. Man-In-The-Middle Attack

In March 2014, a Vulnerability Research Firm named ReVuln, published a video which describes how to employ man-in-the-middle attack to penetrate into the Philips Smart Television through the wireless network that the device connects to. Consequently, the cyber criminal could steal the cookies from the built-in web browser of the television and generate a session hijacking attack to gain access to victim's personal pages [5].

After observing the attack video, one can easily say that TV's configuration for connecting to wireless network through a default hard-coded password is not appropriate. Though it may be convenient for the users, it is quite dangerous if the cyber criminal is also within the range of wireless router. It could even cause more serious aftermath since remote control TV application can easily be downloaded from the Internet. Through such application the hacker could obtain the TV's configuration files and control the TV if he knew the IP address of the television.

B. Denial-of-Service (DOS) Attack

DOS attack is not a new technique and the main attacking mechanism is that a huge amount of packets are generated and sent simultaneously to a targeted appliance. As a consequence, the appliance is either brought down causing permanent crash, or reset to factory setting automatically and making it lose its configuration, stored data and applications.

This kind of attack has recently been reported (August 2014) [6]. A hacker named, Hemanth Joseph, shared on his blog a very simple way to carry a DOS attack on a Pebble Smart Watch. The attacker just needs to know the victim's phone number, Facebook ID, or any other way to interact with the Watch's IP address. Considering that the watch has a function of showing messages received from Facebook, tablet or phone on its screen without character limitation, the attacker can keep on sending many lengthy messages so as to cause a DOS attack on the watch. As a consequence, the Smart Watch could be brought down, reset to factory setting, and lose all of its data as shown in Fig. 1:

Fig. 1. After DOS attack, the Watch's screen is full of white straight lines, all data and applications are erased because of reset to factory setting [6].

In addition to the IoT network of home appliances, cyber criminals can also easily penetrate into internet-based-control public appliances. A study published in August 2014 by security researchers from the University of Michigan demonstrates how a series of vital security vulnerabilities in traffic light systems in the US could allow adversaries to quite easily take control of the whole network of at least 100 traffic signals from a single point of access [7].

By carefully examining the above cases, the authors found that the main reason behind such vulnerability was because those appliances make use of unencrypted wireless radio signals thus simply monitored and compromised by cybercriminals.

C. Thingbot

Thingbot is derived from the word botnet which itself is a combination of the words "robot" and "network". In a similar manner, thingbot is comprised of the words "thing" and "robot".

In order to create a huge botnet network, many computers are compromised and abused by malware to launch cyber attacks without awareness of internet users. In a very similar manner, botnet composed of smart home appliances and

other devices in IoT network, can be infected and easily turned into slaves by the attackers because of lack of proper security. After knowing the real IP addresses of such compromised devices, it becomes easy for the hacker to generate cyber attacks such as spamming, or executing Distributed Denial of Service (DDOS) by manipulating them via standards-based network protocols such as Internet Relay Chat (IRC) and Hypertext Transfer Protocol (HTTP) [8].

Although no serious DDOS attack originating from IoT network has been reported as of this moment, it is predictable that DDOS attack scheme from IoT will be on its upward trend in a near future as mentioned in a warning press from Kaspersky blog [9]. Just to do a small calculation as a reference, let us assume that only 0.01% of the IoT network is compromised by 2020. This will make around 20 million appliances vulnerable to cyber attacks. Even granting that most of the IoT will only transmit relatively small amounts of data, considering their enormous size, the DDOS attack will be severe enough and should have no difficulty in bringing down a server, or any single host. Moreover, unlike DOS attack which is generated in a pinpointed manner from a single computer or server to flood a target, DDOS attack is an integrated effect of a huge number of compromised devices. Once it occurs, blocking becomes extremely difficult since each compromised element has its own unique IP address.

D. Some Specific Attack Cases in Japan

A DVD/HDD video recorder in Japan, which implemented a proxy server and was accessible without authentication under its default configuration, was used as an open proxy server base for spamming [10], as shown in Fig. 2. In another incident, a music player, which was infected with a virus in the factory, corrupted its user's computer upon connection [11]. In an example of privacy violation, a poorly implemented 'referer' feature in a cellular phone constantly transmitted previously accessed page information even when the page was reached via direct addressing (i.e., non-hyperlink access). The browser flaw caused private information, which may had been required to access a previous page (e.g., user name, password), to be revealed to the next link. It also revealed the user's favorite sites by transmitting information on a previously accessed page [12].

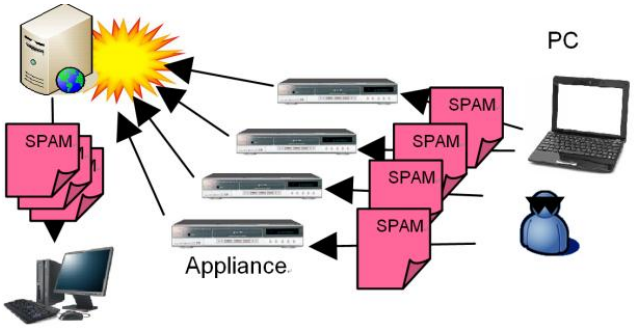


Fig. 2. A spamming incident

III. Security Implementation Challenges

Continuous growth of diverse smart home appliances and development of numerous networking technologies make management of home network security and their associated

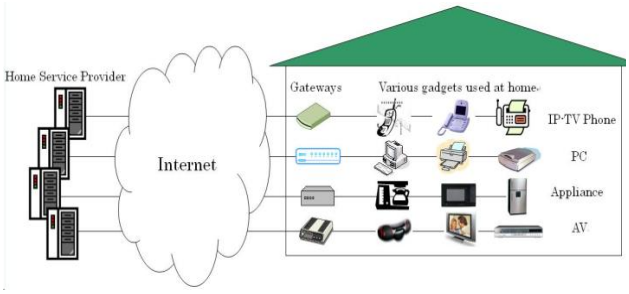


Fig. 3. A heterogeneous home network and its service Providers

services complex to both users and service providers, as can be seen from Fig. 3.

Implementing security on these devices also presents more challenges than traditional computer security due to the limited resources (e.g., toy CPUs that cannot handle computationally expensive cryptographic computations and battery power that prohibits long-lasting or high-peak computations). Furthermore, because security of a network depends on its weakest link, security of networked smart home appliances would rely on the security of its most primitive home appliance e.g., a coffee maker or a toaster. The problem is further aggravated by the fact that home appliance users cannot be considered as "skilled" administrators, but are instead technology-unaware people in many cases.

In order to cope up with such security challenges, the corresponding author in a previous work proposed the idea of handling them through network operator. The recommendation was to engage a network operator to build dedicated but nonproprietary home gateways and become the preferred trusted third party and motivate internet-enabled smart appliance manufacturers to develop device drivers and application software that can run on such universal home gateways to control and operate the appliances. This idea is schematically shown in Fig. 4, where a universal home gateway, managed by a network operator, functions as an entry point to the networked appliances. In this architecture, all transactions with the smart appliances, whether local or remote, are done via universal home gateways. [13][14].

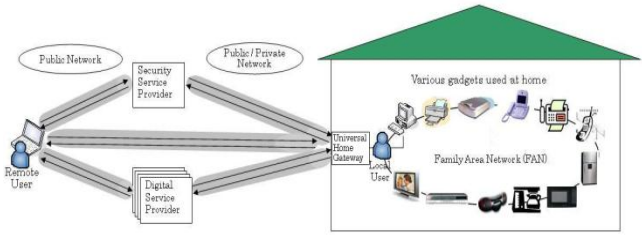


Fig. 4. Smart home appliance security via network operator

Unfortunately, however, as of today no such universal home gateway has yet been manufactured, without which it becomes impossible for a network operator to take the role of trusted third party.

IV. Motivation Behind The Study

In a recent previous work on anonymous communication and its application to social networking, the authors conducted some experiments to test the confidentiality level and anonymity level of several anonymous tools such as

Incognito Mode in Chrome browser, proxy server, virtual private network (VPN), and TOR. In conclusion, the study was able to point out some significant pros and cons in each particular anonymity tool. Additionally, the authors recognized that TOR is indeed the strongest anonymous tool compared with other tools [4]. This is mainly because "Tor Browser Bundle" operates as an internet browser which anonymizes all internet surfing activities that pass through and sends them to the TOR network. After concluding that TOR is a powerful tool for protecting internet user's privacy from being compromised by most contemporary attack techniques and learning about a new-style of attack; reported by Proofpoint, an innovative security-as-a-service vendor, in January 2014, the authors realized that smart appliances' security have not yet been realized via network operator and TOR may play an effective role in this endeavor.

The Proofpoint's report was about cyber attack involving commonly used smart home appliances and in its press release, the company stated: "The attack that Proofpoint observed and profiled occurred between December 23, 2013 and January 6, 2014, and featured waves of malicious email, typically sent in bursts of 100,000, three times per day, targeting Enterprises and individuals worldwide. More than 25 percent of the volume was sent by things that were not conventional laptops, desktop computers or mobile devices; instead, the emails were sent by daily consumer gadgets such as compromised home-networking routers, connected multi-media centers, televisions and at least one refrigerator. No more than 10 emails were initiated from any single IP address, making the attack difficult to block based on location" [15]. Thus, this study is motivated by the aforementioned scenario and our relevant previous work. In this paper, the authors will demonstrate how TOR can help remedy the recent security problems in smart home appliance system.

V. TOR – A New Approach To Secure Smart Home Appliances

Taking into consideration all of the aforementioned cyber attack cases aimed at smart appliances, it is apparent that the attack techniques are not new. However, what have been changed are the attack targets, which are the smart home appliances and devices in IoT network. In most cases, the attackers make complete use of the nature of Internet Protocol to have the access to those appliances; and oftentimes, the devices do not have full-functional display or screen so it is really hard for the victims to even detect that they are being attacked and abused internally. Furthermore, different from human-controlled computers, most of smart appliances (such as *LED light bulbs smart system, smart refrigerators and smart meters*) can easily be accessed due to their 24 hours around-the-clock availability on the Internet. Last but not least, because each appliance is designed to serve only a specific purpose, marketability factors such as low cost, portability, tinier size, etc. make built-in full cryptography capability infeasible in most of such appliances.

While the previously proposed concept of universal home gateways and involvement of network operators in security challenges of such appliances is not achieved, it is going to be difficult for producers to produce economically feasible, safe and tiny smart appliances. This is because for instance, an LED in smart light bulb systems would become unaffordable to buy if cryptography process and sufficient memory for encrypting information were built into each single bulb. Hence, it is certainly not the right approach to equip all smart appliances with built-in security function against cyber attacks in the same manner that has been done on personal computers and web servers.

An intermediate solution, which is proposed in this paper, is to make use of TOR and this section will demonstrate how to utilize TOR to make the IoT network more robust and secure against most of the contemporary cyber attacks.

A. Some Important Properties of TOR

Before moving into detailed technical demonstrations, it is necessary to briefly introduce some important properties of TOR. In the previous research we already described its internal working mechanism and showed that it is indeed an ideal anonymous communication tool which employs asymmetric cryptography, takes advantage of public-key encryption and transmits data from a source to a destination through a randomly selected route of multiple nodes [4]. Raw data having its destination IP address encrypted and re-encrypted with public key of the selected nodes, something which resembles an onion ring where in each layer is a re-encrypted version of an encrypted data by the public key of the node. In the transmission process, each node decrypts a layer of the encryption to extract the next layer's IP address, an operation resembling an onion-peeling-off process. The final node decrypts the last layer of the encryption and sends the original data to its real destination without revealing or even knowing its original sender [16].

In this paper, we would like to expand the research into a deeper level of TOR and employ its subproject, The Amnesic Incognito Live System (Hereafter: Tails); a live operating system, Debian-based Linux distribution which can run on almost any CPU based gadget like DVD, USB stick, or SD card [17].

Usually ordinary internet users often use TOR as an internet browser and the Tor Browser Bundle is one of its most well-known subprojects. While the Tor Browser Bundle operates as an anonymous browser where only those surfing activities done within the browser are anonymized, Tails acts as a complete stand-alone operating system causing not only net surfing activities in the browser but also all of the networking activities running within other applications and operating system be anonymized by forcing them to pass through TOR network before going out to the public internet environment. Through this mechanism, the data transmission process gets firmly secured because of the multilayer asymmetric cryptography feature of TOR. As the process also encrypts the destination IP address, real IP address of the device also gets hidden from the adversaries. Thus we have taken advantage of these two features of Tails operating system and investigated its potential for addressing the security problems of the IoT network.

B. Test Platform Configuration and Monitoring Process

In this section we describe how to configure TOR to secure smart home appliance system. The main idea is to set up Tails to be the central control gateway thus forcing all the transmitted data packets of smart home appliances to pass

through before going out to the public internet environment. Since no universal home gateway has yet been produced, we made use of existing devices and software to create a new system and used it to conduct the experiment as illustrated in Fig. 5:

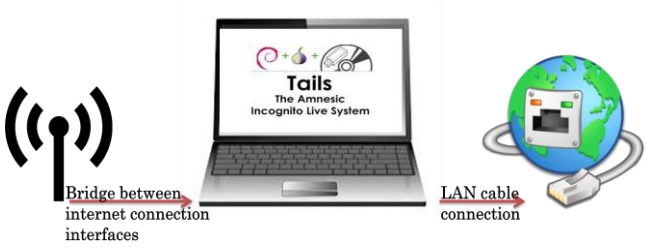


Fig. 5. Setting up a TOR network for smart home appliances

Our experimental system consisted of a laptop with WiFi internet connection interface, local area network (LAN) cable connection interface and a Tails-contained storage device (such as DVD, USB stick, or SD card). Initially we loaded Tails into the laptop, configured the LAN cable to be its main interface to the Internet and reserved WiFi interface as an Access Point for smart home appliances. The LAN and WiFi interfaces were then bridged to each other so that the Internet connection from LAN cable is shared with WiFi interface to form the Access Point. All the smart home appliances were then configured to connect through this Access Point instead of directly connecting to the Internet.

This way, because of the built-in anonymity feature of Tails, all the networking activities passing via laptop's WiFi Access Point are anonymized and multilayer-encrypted by public-key cryptography before being sent through the TOR nodes network to their real destinations. Fig. 6 shows the operating mechanism of this process.

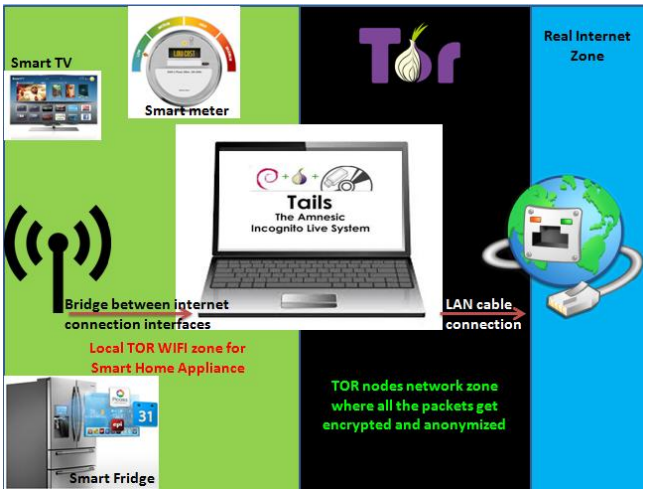


Fig. 6. The overview of TOR WiFi network for smart home appliances

Once the Internet connection is available, Tails immediately send a request to TOR directory server node to obtain the list of other nodes in TOR network and establish a sufficient amount of circuits for routing data through the TOR network anonymously. It is easy to monitor how Tails forms the available TOR nodes to create circuits by means of a built-in tool called *TOR network map*. Fig. 7 shows a series of random routing paths that Tails forms to transmit data through the TOR network.

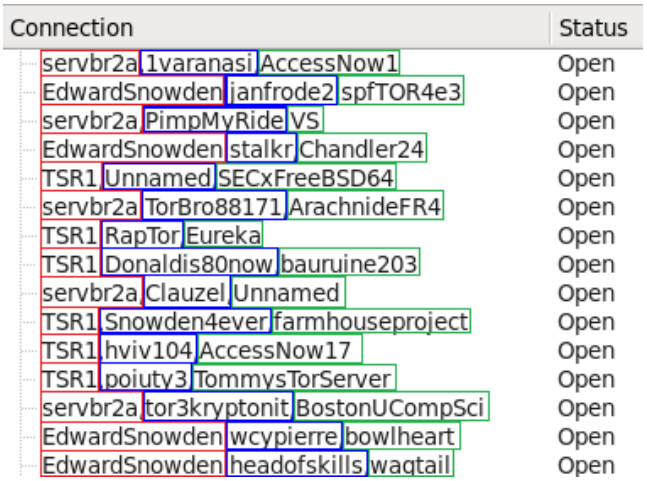


Fig. 7. A list of TOR circuits obtained from TOR network map tool

The data transmission process is done anonymously through distributed TOR nodes system operated by a huge number of volunteers around the world. As indicated in Fig. 7, each circuit has 3 nodes called entry, intermediate and exit which are highlighted in red, blue and green respectively. The entry nodes (in this case: *servbr2a*, *EdwardSnowden*, *TSR1*) are rarely changed. Tails sometimes reuses the same set of entry nodes in a working session, while the intermediate and exit nodes keep changing from circuit to circuit. This is because the entry node is the first node where the connection gets into the TOR network. As it is vital to make the connection steady and robust as much as possible, TOR directory nodes often have longer uptime than other voluntary nodes (in this case: the directory node *servbr2a* has 118-day uptime). In order to provide more thorough details, we collected information about all the nodes shown in Fig. 7, the results of which are indicated in Fig. 8.

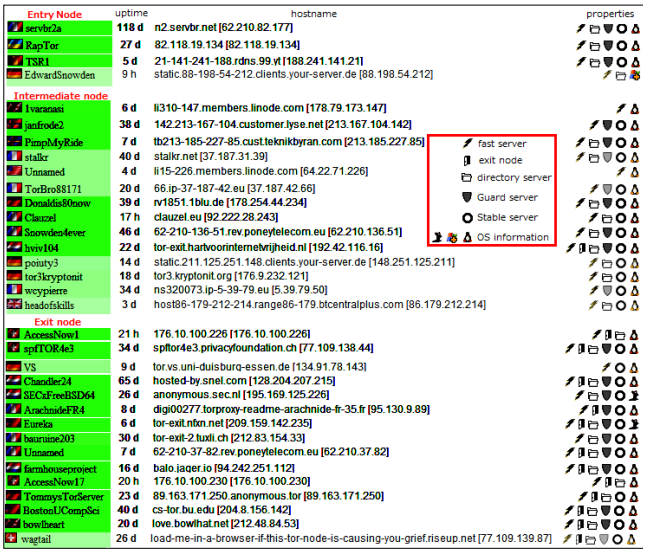


Fig. 8. List of TOR nodes in a random working session of Tails with their detailed information (country, uptime, IP address, sever type and Operating System information)

TOR nodes of Fig. 8 are obtained from the TOR-network monitoring website named http://www.torstatus.blutmagie.de, which contains detailed information of the available TOR nodes. In a similar manner, Tails user can check through which node the data packets will be transmitted and decide to either let the data pass through a

particular route or not. For instance, by examining the uptime and properties of the entry node *EdwardSnowden*, an experienced Tails user may not want his/her data pass through that node. This is because its uptime is not long; it is not a Guard and Stable node, hence, vulnerable to compromise because the data could be dropped during transmission process and result in leaking the identity information of Tails users. To prevent data transmission through such an unwanted circuit, the user just needs to right click on it from *connection window*, choose *Delete circuit*, and then Tails will remove it from the list.

Another noteworthy feature of this Tails is that all data are sent and received in a distributed manner, a particular case of which is shown in Fig. 9.

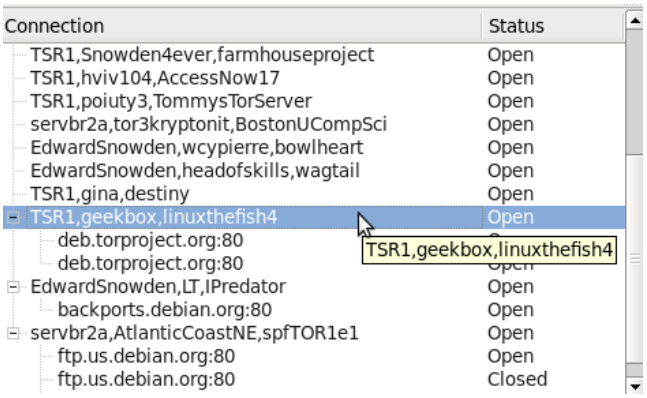


Fig. 9. Data Transmission is done in distributed manner by means of dispersed voluntary TOR nodes around the world

For example, in the same working session of Tails, we executed *sudo apt-get update* in *root terminal* to run an update task for the Debian operating system. Although it is a single task in which the system communicates with Debian database servers to update newest functions for Tails, the task gets divided into many subtasks and communicates with Debian servers through separate streams as described technically in Tor proposal 171 [18]. The update task shown on Fig. 9 is done in distributed manner through the following 3 separate circuits:

1. *TSR1, geekbox, linuxthefish*
2. *EdwardSnowden, LT, IPredator*
3. *servbr2a, Atlantic CoastNE, spfTOR1e1*

As a result, there is no way for any single node in the circuits, including the LAN admin or Debian servers' admin nodes to have all the information about transmission route, original IP address of TOR user, and the raw data. This means that each component in the system can only know a part of the whole transmission process. Thanks to this unique working mechanism of Tails, altering transmission route frequently in about every 10 minutes and providing maximal anonymity for Tails user. Therefore, if functionality of the system shown in Fig. 5 is constructed as a Tails-embedded router, it is certainly going to be a promising solution for securing smart home appliance system.

Last but not least, *MAC address spoofing* feature is also an indispensable feature of Tails. Although MAC address is not sent over the Internet and only used within the local network, there is a risk of an internal attack from an adversary who is also in the same network. Tails also fakes MAC address of the system, laptop in our example, so as to protect the system from internal attack and prevent local network admin or other users in the same LAN to monitor Tails-installed device from within.

To verify the *MAC address spoofing* feature, we used a network tool called Fing [19] and monitored the LAN to where Tails-based laptop was connected. As shown in Fig. 10, devices without Tails-installed operating system could be easily traced thus revealing their names, real interfaces and MAC addresses; while Tails-installed laptop changed its MAC address every time the machine got connected again to the local network and did not leak its name, thus made monitoring hard as indicated in the highlighted red section of Fig 10.

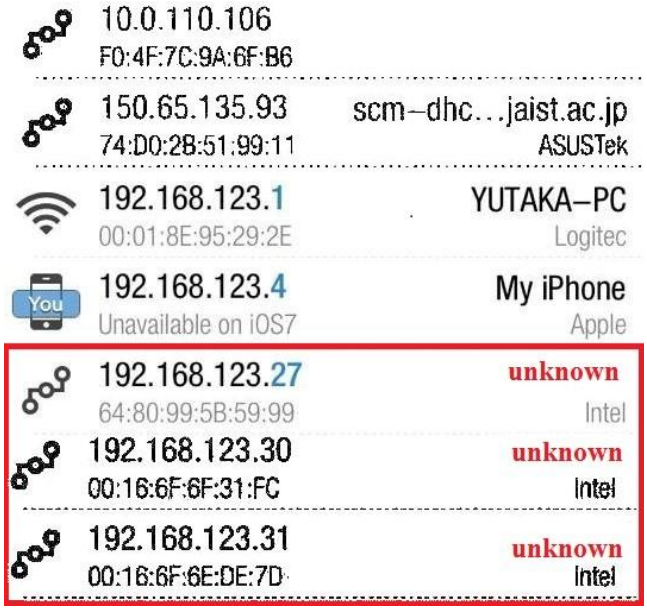


Fig. 10. MAC address spoofing feature of Tails

C. Testing with Multimedia Transmission

In this section we demonstrates feasibility of transmitting multimedia data over the TOR-based network using Sony BRAVIA smart television (hereafter: the smart TV) as a typical testing object, shown in Fig. 11:

Fig. 11. Testing object - Smart Sony BRAVIA television

The smart TV was intentionally selected for the experiment since it is integrated with many applications and can be considered as a typical representative of other smart appliances as well. Apart from the function of a traditional television, the smart TV has also many other multimedia applications and internet-based services such as high

definition (hereafter: HD) movies from the Internet, online music, net surfing, social networking and so on as shown in Fig. 11.

Considering that TOR only supports the Transmission Control Protocol (hereafter: TCP), as stated in TOR project documentation [16], we had to first examine which protocol is mainly used in the smart TV to communicate with the Internet and ensure proper rerouting of its data stream through the TOR network. To monitor the data transmission process of the smart TV, we used a network monitoring tool, called Microsoft Network Monitor, to tap to the connection channel between the smart TV and the Internet. We then run all the essential applications, ranging from Youtube, Sony online HD movies service to gaming applications, at the TV side and Fig. 12 shows captured result at the network monitoring tool side.

Source	Destination	Protocol	Description
r5.sn-xgmnpoxuopp-ogue.googlevideo.com	192.168.123.28	TCP	TCP:[Continuation to #15198]Flags=.....
r5.sn-xgmnpoxuopp-ogue.googlevideo.com	192.168.123.28	TCP	TCP:[Continuation to #15198]Flags=.....
192.168.123.28	r5.sn-xgmnpoxuopp-ogue.googlevideo.com	TCP	TCP:Flags=...A...., SrcPort=40156, Ds...
192.168.123.28	r5.sn-xgmnpoxuopp-ogue.googlevideo.com	TCP	TCP:Flags=...A...., SrcPort=40156, Ds...
192.168.123.28	bivl.np.ac.playstation.net	TCP	TCP:Flags=.....S., SrcPort=43382, Ds...
ssm1.internet.sony.tv	192.168.123.28	TCP	TCP:Flags=...A...F, SrcPort=HTTPS(443...
192.168.123.28	ssm1.internet.sony.tv	TCP	TCP:Flags=...A...., SrcPort=47781, Ds...
ssm1.internet.sony.tv	192.168.123.28	TCP	TCP:Flags=...A...F, SrcPort=HTTPS(443...
bivl.np.ac.playstation.net	192.168.123.28	TCP	TCP:Flags=...A..S., SrcPort=HTTPS(443...
192.168.123.28	bivl.np.ac.playstation.net	TCP	TCP:Flags=...A...., SrcPort=43382, Ds...
23.32.241.24	192.168.123.28	TCP	TCP:Flags=...A...F, SrcPort=HTTP(80),...
tv.app.bs.sony.jp	192.168.123.28	TCP	TCP:Flags=...A...F, SrcPort=HTTP(80),...
23.32.241.24	192.168.123.28	TCP	TCP:Flags=...A...F, SrcPort=HTTP(80),...
tv.app.bs.sony.jp	192.168.123.28	TCP	TCP:Flags=...A...F, SrcPort=HTTP(80),...
23.32.241.24	192.168.123.28	TCP	TCP:Flags=...A...F, SrcPort=HTTP(80),...
applicast.jp.sonystyle.com	192.168.123.28	TCP	TCP:Flags=...A...F, SrcPort=HTTP(80),...
192.168.123.28	23.32.241.24	TCP	TCP:Flags=...A...., SrcPort=40495, Ds...
192.168.123.28	23.32.241.24	TCP	TCP:Flags=...A...., SrcPort=40496, Ds...
192.168.123.28	23.32.241.24	TCP	TCP:Flags=...A...., SrcPort=40497, Ds...
192.168.123.28	tv.app.bs.sony.jp	TCP	TCP:Flags=...A...., SrcPort=59071, Ds...
192.168.123.28	23.32.241.24	TCP	TCP:Flags=...A...., SrcPort=40498, Ds...
192.168.123.28	tv.app.bs.sony.jp	TCP	TCP:Flags=...A...., SrcPort=59072, Ds...
192.168.123.28	23.32.241.24	TCP	TCP:Flags=...A...., SrcPort=40499, Ds...
192.168.123.28	applicast.jp.sonystyle.com	TCP	TCP:Flags=...A...., SrcPort=58565, Ds...

Fig. 12. Data stream between Sony BRAVIA smart television and multimedia resources

As can be seen in the captured result, most of applications communicate with the Internet via TCP. In this particular case, Youtube communicates with *r5.sn-xgmnpoxuopp-ogue.googlevideo.com* to load videos via TCP; or other Sony-based services like online HD movies, gaming applications communicate with Sony's service-providing servers such as *bivl.np.ac.playstation.net*, *ssm1.internet.sony.tv*, *applicast.jp.sonystyle.jp*, and *tv.app.bs.sony.jp* using TCP. It is evident that such TCP-based data streams can be routed through the TOR network in order to make the connection more secure. Though the Internet connection speed may theoretically get slower and adversely affect quality of the services when routed through the TOR network since it has to pass through 3 TOR nodes before reaching the final destination, the experiment showed that all the above mentioned applications and Sony-based services still works smoothly over the TOR network. Despite the fact that buffering speed of HD movies and videos from Youtube was not as fast as the normal and direct connection environment, the videos from Youtube server still loaded with an acceptable speed and caused no interruption in between.

D. Testing with Voice-over-Internet Protocol Applications

This section examines potential of using the TOR-based network for voice over IP application like Skype. Unlike Youtube videos and HD movies which are TCP-based applications, Skype which is a voice over IP service and instant messaging client software developed by Microsoft, operates based on The User Datagram Protocol (hereafter: UDP). It is one of the vital applications in the application suite of the smart TV, but has to operate in a real-time manner. In other words, the transmitted data packets have really short time-to-live and need to hit their final destination before the time-to-live is over. Hence, applications like Skype, LINE and Viber conventionally operate based on the UDP.

Our initial attempt to launch Skype via TOR network in the same manner as other TCP-based applications over the Internet having a regular speed failed mainly because of the short time-to-live duration of UDP packets. In order to prove that TOR-based network could also work with voice over IP application, we conducted the next phase of our experiment at Japan Advanced Institute of Science and Technology (hereafter: JAIST) where the Internet connection speed is 10 Gbit/s, one of the highest in Japan [20]. Fig. 13 shows the setup of our experiment where at one side, we connected the smart TV to the Internet via the Tails-installed laptop and at the other side; a regular Windows equipped with Skype was connected to JAIST network. At both side, Microsoft Network Monitor was used to tap to the transmission channels.

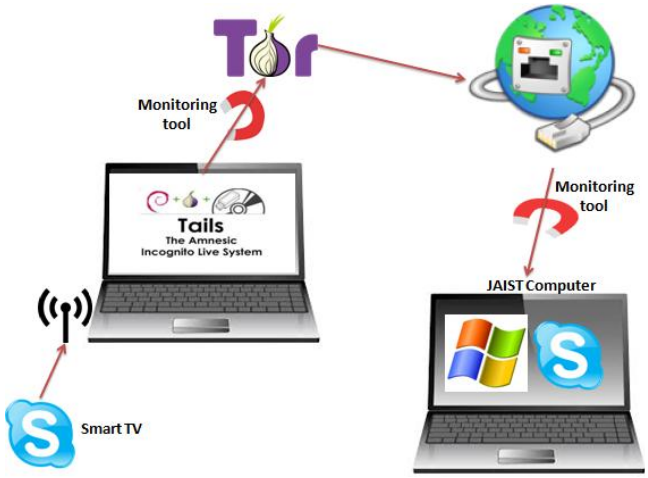


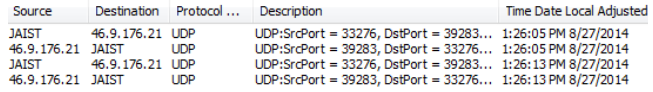
Fig. 13. Testing VoIP over TOR network

We then made a call from the Skype account in the smart TV to the Skype account in the JAIST computer while monitoring the transmission process at both sides by two separate network monitoring tools. This time, the Tails-installed laptop instead of dropping out the UDP connection, encrypted and encapsulated all the UPD packets of Skype into TCP packets and sent them through the TOR network as shown in the captured screen of its monitoring tool in Fig. 14, where *192.168.123.27* is the local IP address of the Tails-installed laptop, and *62.210.137.27*, *188.138.1.229* and *94.23.105.27* are the IP addresses of the entry TOR nodes at that time.

Source	Destination	Protocol	Description	Time Date Local Adjusted
62.210.137.230	192.168.123.27	TCP	TCP:Flags=...A...., SrcP...	1:26:04 PM 8/27/2014
192.168.123.27	62.210.137.230	TLS	TLS:TLS Rec Layer-1 SS...	1:26:04 PM 8/27/2014
62.210.137.230	192.168.123.27	TLS	TLS:TLS Rec Layer-1 SS...	1:26:04 PM 8/27/2014
192.168.123.27	62.210.137.230	TCP	TCP:Flags=...A...., SrcP...	1:26:04 PM 8/27/2014
188.138.1.229	192.168.123.27	TCP	TCP:Flags=...A...., SrcP...	1:26:04 PM 8/27/2014
192.168.123.27	188.138.1.229	TCP	TCP:[Continuation to #...	1:26:04 PM 8/27/2014
188.138.1.229	192.168.123.27	TLS	TLS:TLS Rec Layer-1 SS...	1:26:04 PM 8/27/2014
188.138.1.229	192.168.123.27	TCP	TCP:Flags=...A...., SrcP...	1:26:04 PM 8/27/2014
94.23.105.27	192.168.123.27	TLS	TLS:TLS Rec Layer-1 SS...	1:26:04 PM 8/27/2014
192.168.123.27	94.23.105.27	TLS	TLS:TLS Rec Layer-1 SS...	1:26:04 PM 8/27/2014
62.210.137.230	192.168.123.27	TCP	TCP:Flags=...A...., SrcP...	1:26:04 PM 8/27/2014
192.168.123.27	188.138.1.229	TCP	TCP:Flags=...A...., SrcP...	1:26:04 PM 8/27/2014
192.168.123.27	62.210.137.230	TLS	TLS:TLS Rec Layer-1 SS...	1:26:04 PM 8/27/2014
62.210.137.230	192.168.123.27	TLS	TLS:TLS Rec Layer-1 SS...	1:26:04 PM 8/27/2014
192.168.123.27	62.210.137.230	TCP	TCP:Flags=...A...., SrcP...	1:26:04 PM 8/27/2014
188.138.1.229	192.168.123.27	TCP	TCP:Flags=...A...., SrcP...	1:26:05 PM 8/27/2014
192.168.123.27	188.138.1.229	TLS	TLS:TLS Rec Layer-1 SS...	1:26:05 PM 8/27/2014
94.23.105.27	192.168.123.27	TLS	TLS:TLS Rec Layer-1 SS...	1:26:05 PM 8/27/2014
192.168.123.27	94.23.105.27	TLS	TLS:TLS Rec Layer-1 SS...	1:26:05 PM 8/27/2014
188.138.1.229	192.168.123.27	TLS	TLS:TLS Rec Layer-1 SS...	1:26:05 PM 8/27/2014

Fig. 14. Tails-installed PC encapsulates UPD packet inside TCP packet

At the exit node of the TOR, the TCP packets got decrypted thus disclosing the original UDP packets and sending them to the final destination. Consequently, at JAIST computer side the incoming Skype UDP packets created a ring sound of the incoming call and established a channel for voice conversation as shown in the captured screen of its monitoring tool in Fig. 15.



Source	Destination	Protocol ...	Description	Time Date Local Adjusted
JAIST	46.9.176.21	UDP	UDP:SrcPort = 33276, DstPort = 39283...	1:26:05 PM 8/27/2014
46.9.176.21	JAIST	UDP	UDP:SrcPort = 39283, DstPort = 33276...	1:26:05 PM 8/27/2014
JAIST	46.9.176.21	UDP	UDP:SrcPort = 33276, DstPort = 39283...	1:26:13 PM 8/27/2014
46.9.176.21	JAIST	UDP	UDP:SrcPort = 39283, DstPort = 33276...	1:26:13 PM 8/27/2014

Fig. 15. Incoming UDP Skype packets after being decrypted and dispatched from TOR exit node (in this case, TOR exit node IP address is 46.9.176.21).

However, by the time the Skype account at the JAIST computer side clicked *answer*, the channel only survived for a few seconds and without being able to transmit any voice it got dropped. By analyzing the monitoring results of both sides, it is not difficult to show the cause of the drop out shortly after the ring. As shown in Fig. 14, the TCP packets are sent out at the time the call was made (from 1:26:04). However, at the JAIST computer, the UDP packets were received interruptedly at 1:26:5 and at 1:26:13. It is therefore clear that connection delay and short time-to-live duration of UDP packets is the main cause, something which could be eventually offset by the expected increase in the Internet connection speed in the next coming years through the evolution of optical fiber technology.

To further investigate the potential of TOR-based network for with voice over IP applications, we also tested it with other voice over IP applications like LINE and Viber and observed the same phenomenon and have no doubt that UDP-based smart home appliances could also operate smoothly in TOR environment in the near future.

VI. Conclusion

Since the Internet of Things is still at the early stage of its development, smart home appliance producers need more time and effort in order to produce cost-effective and safe products. Until then, however, being aware of cyber attacks aimed at smart home appliances and its numerous risks, having an alternate solution to remedy the potential problems is quite important.

In this paper we first showed numerous vulnerabilities that smart home appliance users are facing and how networking monitoring tool and regular DDOS attack technique can easily be used to attack the IoT network and simultaneously abuse them for illicit purposes. We then proposed the implementation of TOR-based anonymous communication into the IoT network as an effective alternative way to help smart home appliance users protect their privacy and make the smart home appliance system more secure from aforementioned cyber attacks. Our results show that Tails having many security features such as multilayer encryption, data transmission in distributed manner over a huge amount of voluntary nodes around the world, and MAC address spoofing, is indeed a suitable approach to solve recent security problems in TCP-based smart home appliances.

Future work along this research which is already being carried out by the authors is to utilize the TinyOS programming language and simplify The Amnesic Incognito Live System so as to create a Tails-embedded router that can act as the central control gateway to support and secure the smart home appliance system. The idea is to come up with a practical version of the universal home gateway while waiting for the development of its ideal version and involvement of network operators in the security challenges of smart home appliances. Practical realization of "*VoIP over TOR*" is another area which needs further investigation while waiting for further increase in the Internet connection speed through the evolution of optical fiber technology.

Acknowledgment

Firstly, Nguyen Phong HOANG would like to sincerely thank his supervisor, Professor Davar PISHVA (Dean of College of Asia Pacific Studies at APU), for his dedicated help and support during the last 2 years. Without such help and academic advice this research could not have been accomplished. Next, we would like express our deepest gratitude to Professor Atsuko Miyaji from the School of Information Science, Japan Advanced Institute of Science and Technology (JAIST). Through an Academic Exchange Program which exists between APU and JAIST, Mr. Nguyen Phong HOANG was able to enjoy her state-of-the-art scientific laboratory and precious advice while conducting some experiments for this work.

References

[1] Herper, Matthew. *Emerging Technologies: 'Smart' Kitchens A Long Way Off*, Forbes, Feb. 2003.

[2] Staff. *Wired News: Caregiver Tech Slowly Evolves*, Associated Press, September 2003.

[3] Carrie MacGillivray, Vernon Turner, Denise Lund, *Worldwide Internet of Things (IoT) 2013–2020 Forecast: Billions of Things, Trillions of Dollars.* International Data Corporation, 2014. Available: http://www.idc.com/getdoc.jsp?containerId=243661

[4] Hoang Nguyen Phong, and Davar Pishva. "Anonymous communication and its importance in social networking." *the 16th International Conference on Advanced Communication Technology (ICACT 2014)*, pp. 34-39 (February 2014)

[5] *Having fun via WIFI with Philips Smart TV. Revuln, 2014. Available: http://vimeo.com*/90138302

[6] Hemanth Joseph, *Dosing Pebble Smart Watch And Thus Deleting All Data Remotely*, August 2014 [Online]. Available: http://www.whitehatpages.com/2014/08/dosing-pebble-smartwatch-and-thus.html

[7] Ghena, B., Beyer, W., Hillaker, A., Pevarnek, J., & Halderman, J. A. "Green lights forever: analyzing the security of traffic infrastructure." *In Proceedings of the 8th USENIX conference on Offensive Technologies* (pp. 7-7). USENIX Association. (2014, August).

[8] Ramneek Puri, *SANS Institute InfoSec Reading Room*. SANS Institute, August 2003. Available: http://www.sans.org/reading-room/whitepapers/malicious/bots-botnet-overview-1299

[9] Brian Donohue, *Beware The Thingbot!* Kaspersky Lab, January 2014. Available: https://blog.kaspersky.com/beware-the-thingbot/

[10] Katagi, Kizu. *Vulnerability of Toshiba's RD Series HDD-DVD Recorder 'Stepping-stone' for Danger*, Internet Watch, October 2004 (In Japanese) http://internet.watch.impress.co.jp/cda/news/2004/10/06/4882.html.

[11] Press Release, *A Report to Customers on the Issue of 'Creative Zen Neeon' Digital Audio Player and its Response*, Creative, September 2004 (In Japanese) Available: http://jp.creative.com/corporate/pressroom/releases/welcome.asp?pid=12181.

[12] AU Announcement, *EZweb Browser's Home Page URL Transmittal on AU and TU-KA Mobile Phones*, KDDI News, December 2005 (In Japanese) Available: http://www.au.kddi.com/news/topics/au_topics_index20051209.html.
[13] D. Pishva, K. Takeda, *A Product Based Security Model for Smart Home Appliances*, 40th Annual IEEE International Carnahan Conferences on Security Technology, pp. 234-242 (2006).
[14] D. Pishva, K. Takeda, *A Product Based Security Model for Smart Home Appliances*, IEEE Aerospace and Electronics System Magazine, Vol.23, No.10, pp. 32-41 (October, 2008).
[15] *Proofpoint Uncovers Internet of Things (IoT) Cyberattack*. Proofpoint Inc., Sunnyvale California, 2014.
[16] "*The solution: a distributed, anonymous network*", Tor: Overview. TOR project. Available: https://www.torproject.org/about/overview.html.en#thesolution
[17] Koen Vervloesem, *the Amnesic Incognito Live System: A live CD for anonymity*. Linux Info from the Source, April 2011. Available: https://lwn.net/Articles/440279/
[18] Robert Hogan, Jacob Appelbaum, Damon McCoy, Nick Mathewson, *Separate streams across circuits by connection metadata*. The Tor Project, October 2008. Available: https://gitweb.torproject.org/torspec.git/blob/HEAD:/proposals/171-separate-streams.txt
[19] *Fing, the ultimate network toolkit*. Overlook Soft. Available: http://www.overlooksoft.com/features
[20] *Information Environment, Information Environment (Information Society Research Center) - Campus Network*. Japan Advanced Institute of Science and Technology. Available: http://www.jaist.ac.jp/is/keyword/research/info.html

Nguyen Phong HOANG was born in Tien Giang Province, Vietnam in 1992. He received his undergraduate degree in Business Administration majoring in Information & Communications technology (ICT) from Ritsumeikan Asia Pacific University (APU), Japan. He is presently pursuing his graduate studies at the Graduate School of Informatics at Kyoto University in Japan. He has received numerous scholarship and awards; APU Tuition Reduction Scholarship from 2010-2014, JASSO (Japan Student Services Organization) Scholarship from 2011-2012, and TOYOTA Tsusho Scholarship from 2013-2014. His research interests include information security, privacy and anonymous communication. He hopes to advance his research on TOR (The Onion Router), one of the most robust anonymous tools, during his graduate studies. He participated in the 16th International Conference on Advanced Communication Technology and received Outstanding Paper Award from the Conference. He has been an IEEE member since 2013.

Davar Pishva is a professor in ICT at the College of Asia Pacific Studies, Ritsumeikan Asia Pacific University (APU) Japan and presently serves as the Dean of both College and Graduate School of Asia Pacific Studies. In teaching, he has been focusing on information security, technology management, VBA for modelers, structured decision making and carries out his lectures in an applied manner. In research, his current interests include biometrics; e-learning, environmentally sound and ICT enhanced technologies. Dr. Pishva received his PhD degree in System Engineering from Mie University, Japan. He is Secretary General of IAAPS (International Association for Asia Pacific Studies), Senior Member of IEEE, and a member of IEICE (Institute of Electronics Information & Communication Engineers), IAAPS and University & College Management Association.

Smart Device Based Power Generation Facility Management System in Smart Grid

Young-Jae Lee*, Eung-Kon Kim*

**Department of Computer Science, Sunchon National University,*
255 Jungang-ro, Suncheon, Jellanam-do, Republic Of Korea

leeyoungjae@sunchon.ac.kr, kek@sunchon.ac.kr
Corresponding Author: Eung-Kon Kim

***Abstract*— As energy consumption is gradually increased due to rapid development of industrialization, the whole world including our country is faced with an issue of lack of back-up power, exhaustion of fossil energy and global warming. Under this background, as a method of maximizing energy efficiency by preventing global warming and reduction of greenhouse gas emission, smart grid that converged existing power network with IT technology receives concentrative attention as a growth engine of next generation [1-3]. Currently, maintenance of domestic solar power plant management is provided at the center through remote monitoring by using measuring sensor being installed at power plant and as regular check-up or repair being performed at site is progressed by site management personnel by directly moving power generation facility, there is a difference in time and accuracy depending on ability of site management personnel. In this paper, a system of managing smart grid power generation facility by internet of things (IOT) technology is suggested. Maintenance of suggested system for its regular check-up and failure is allowed by site manager conveniently and by using facility recognition based technology instead of existing QR code, its direct application is allowed without additional equipment to smart grid power generation facility being operated at present and by developing power generation facility recognition service using markerless based facility recognition technology, it may be expanded to a technology of recognizing other smart grid power generation facility in the future.**

***Keyword*—Smart Grid, Power plant facility management, Smart Phone, Location Based Service**

I. INTRODUCTION

As energy consumption is gradually increased due to rapid development of industrialization, the whole world including our country is faced with an issue of lack of back-up power, exhaustion of fossil energy and global warming. Under this background, as a method of maximizing energy efficiency by prevention of global warming and reduction of greenhouse gas emission, smart grid that converged existing power network with IT technology receives concentrative attention as a growth engine of next generation [1-3].

Smart grid power generation facilities are under operation by it being spread in various places from small-scaled power generation being installed in general housing, building, parking lot and public facilities to large-scale power generation system being composed in a grid form and these facilities require sustained management and check-up and in case of occurrence of problem such as facility malfunction, power failure or damage, rapid and exact check-up and repair are required to be performed at the site.

However, at present, management of solar energy power generation facilities is performed at the center through remote monitoring by using measuring sensor being installed at the power generation facility and as regular check-up or repair at site is progressed by site management personnel by directly moving power generation facility, there is a difference of time and accuracy depending on ability of site management personnel.

In addition, in case of solar energy power generation facility or wind power generation facility, as it has diversified products, standards and forms, there are a lot of difficulties for exact check-up and in case of small-scaled power generation facility, in view of its features, as maintenance cost is high and a lot of cost is required once a failure is taken place, prevention of failure in advance is required through regular check-up and operational check-up.

Recently, due to popularization of smart phone, a study on industrial application by using smart phone is under way and as smart phone is mounted with wireless internet communication module (3G, 4G, Wifi, etc.), GPS sensor, electromagnetic sensor, image sensor, diversified information provision by using facility recognition technology is enabled [4].

In this paper, a system of managing smart grid power generation facilities by using power generation facility recognition based technology is suggested. Suggested system recognizes smart grid power generation facility image in real time by using image sensor and GPS sensor and it provides site manager with detailed information, hardware drawing, sensor data, facility history of power generation facility.

In addition, it provides location information of facilities so that site manager could identify other surrounding facilities conveniently. When utilizing suggested system, site manage

Manuscript received June 23, 2014. This work was supported in part by This research was financially supported by the Ministry of Education (MOE) and National Research Foundation of Korea(NRF) through the Human Resource Training Project for Regional Innovation (No. 2013H1B8A2032217).

Young-Jae Lee, was with Sunchon National University, 255 Jungang-ro, Suncheon, Jellanam-do, Republic of Korea (e-mail: skyit89@nate.com)

Prof. Eung-Kon Kim, was with Sunchon National University, 255 Jungang-ro, Suncheon, Jellanam-do, Republic of Korea(corresponding author to provide phone: +82-61-750-3627; fax: +82-61-750-7999; e-mail: kek@sunchon.ac.kr).

could perform regular check-up and maintenance of repair conveniently and by using facility recognition based technology instead of existing QR code, its direct application is allowed without addition equipment to smart grid power generation facility being operated at present and by development of power generation facility recognition based technology using markerless based facility recognition technology, it may be expanded to a technology of recognizing other smart grid power generation facility in the future.

II. Related Works

A. Cimphony (Open Grid System)

Cimphony is data management and analysis application of multiple platform smart grid power generation system having OSGI modular system and Eclipse based user interface. Cimphony module provides an independent service such as geographic information visualization by using data editing, OCL based verification, model based conversion, distributed data and KML.

This system is able to support new standard and data model without change of framework by using model-driven architecture, open standard such as CIM (Common Information Model) and smart grid facility monitoring and management function through data visualization from IPad and IPhone [5].

B. Field Force Data Visualization App with Augmented Reality

This is augmented reality based smart grid site monitoring application that was promoted in renewable energy and smart grid research institute EPRI being composed of consortium including a lot of universities and enterprises.

This system is a conception model of light-weighted, mobile access platform that integrated diversified back office systems and this is a project in which user visualized smart grid facility information in actual world by augmenting it using GIS sensor and electromagnetic sensor built in tablet PC.

As a mobile application program for data control and visualization aiming at supporting site workers, it provides information of site details, location and manual, sensor provided to site staffs and cheaper platform built in power source by utilizing mobile system.

In addition, application user may reserve request for work in real time.

This project is a kind of demonstration project that proves strong power of CIM(Common Information Model) in a conceptual way under actual application environment and it has characteristics of having efficiency of visualizing CIM data, stability of site workers, low cost mobile data platform and CIM base utilizing actual data and system, light-weight and mobile data platform [6].

C. Integrating geographical information and augmented reality techniques for mobile escape guidelines on nuclear accident sites

As a study on integrating augmented reality that provides counterfactual information service for escape and location guidance at the time of nuclear accident, it not only provides guidance of escape route by using augmented reality but also visualizes current nuclear power plant condition in geographical map.

This system supports site workers escape from nuclear accident site in real time by identifying current location after capturing surrounding image by using camera built in user's own working system and visualizing escape route in a map [7].

However, it has a disadvantage that high quality map is required, time of loading escape route is long and people at nuclear accident site may consume a lot of time while waiting for this map.

III. Facility Recognition Based Mobile Power Plant Management System

A. System Configuration

In this paper, power generation facility management system that enables convenient and exact management is suggested in a way that site workers recognize smart grid power generation facilities by using power generation facility recognition technology, transmit it to server through wireless communication such as 3G, WiFi and then provide information of current condition, past history, design drawing by matching it with data stored in server.

Power generation management system may be mainly divided into two parts including smart grid power generation facility management server system for providing site workers with formation relevant to current condition, check-up and management history and design of power generation facility and smart application that recognizes and manages power generation facility by using power generation recognition as shown on Fig. 1.

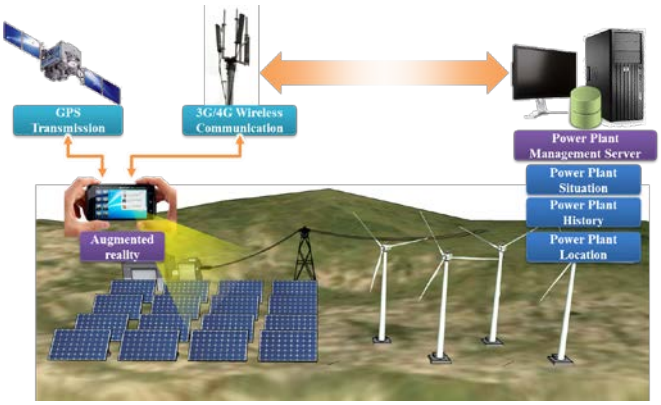


Fig. 1. System layout

B. Power generation facility recognition and registration using power generation facility recognition

Location and image information of power generation facility in power generation facility management server are registered by recognizing power generation facility after using image being shot in screen view of site worker's smart phone and information for power generation facility requested by site worker is provided.

Recognition and registration process of smart grid power

generation facility is as shown on Fig.2.

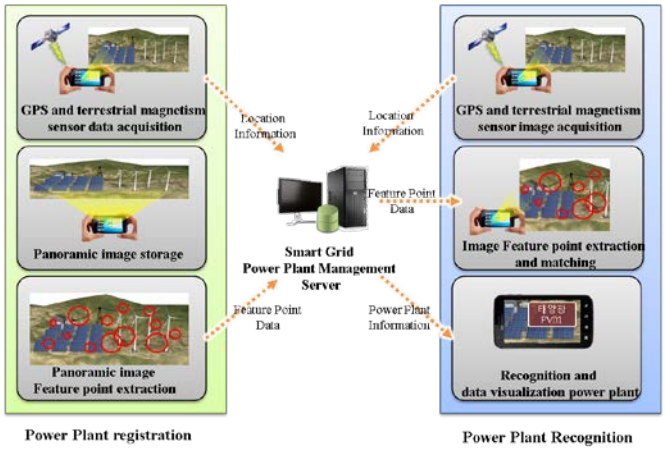
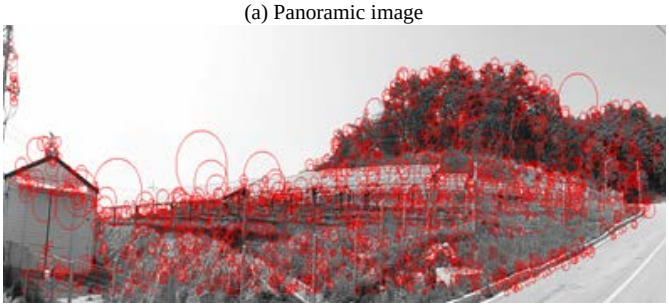


Fig. 2. Recognition and registration process of power generation facility

Registration and recognition process of smart grid power generation facility is that site worker approaches power generation facility within distance of 10cm and makes camera direct at power generation facility and at this time GPS sensor and electromagnetic data are read and at angle of app. 5^{o} to the right/left, power generation facility is shot as panoramic image.

By transmitting GPS sensor, electromagnetic sensor and feature point data to server after extracting feature point of photographed panoramic image as shown on Fig. 3, power generation facility is registered in server data base.

(a) Panoramic image

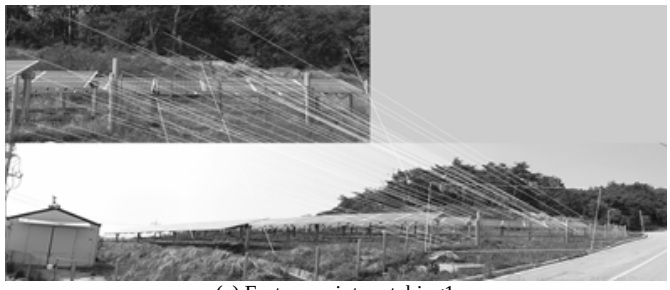


(b) Feature point extraction by using SURF algorithm

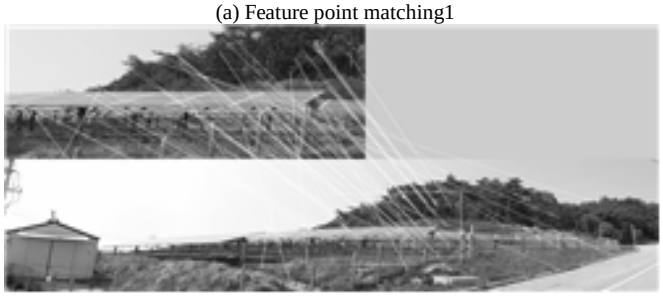
Fig. 3. Recognition and registration process of power generation facility

In a process of recognizing power generation facility by site manager, power generation recognition of worker is requested through the same method as power generation facility registration process.

And then server searches data most similar to facility requested by worker among GPS stored in real time and electromagnetic sensor data and when a result is obtained by matching feature point of panoramic image of searched facility with feature point data transmitted by worker as shown on Fig. 4, information of relevant power generation facility is transmitted to worker but if its matching failed, unrecognizable message is transmitted.



(a) Feature point matching1



(b) Feature point matching2

Fig. 4. Feature point matching test and facility recognition

In this paper, feature point was extracted by using SURF (Speeded Up Robust Features) algorithm so that fast performance ability and feature points that are not changed to rotational change and scale conversion could be found in feature points of panoramic image being transmitted from server and images being obtained from smart phone camera and camera and object would be recognized as identical object even though its angle and distance are different at the time of shooting smart grid power generation facility[8].

C. Power generation facility management server

Smart grid power generation facility management system provides information of current condition, check-up, management history and design drawing of power generation facility based on mobile web application server (WAS: Web application server) in order to ensure convenient interface with smart phone.

Smart grid power generation facility management server system is as shown on Fig. 5.

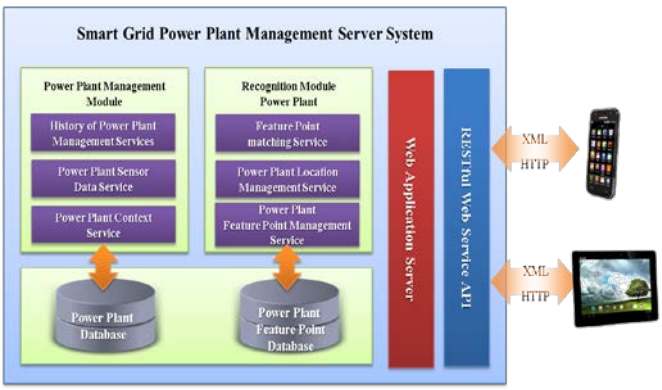


Fig. 5. Power generation facility management server system

Diversified smart phone and tablet PC are supported by

providing an independent interface to platform by utilizing Rest API and a complete interface of smart application is possible by providing power generation facility management service through Rest API.

Management server system of power generation facility is composed of power generation history, sensor data, matching power generation facility data base of its management module that provides situation information service with feature points, location management of power generation facility and feature point data base of power generation facility recognition module that provides its feature point management service.

As shown on Table 1, smart grid power generation management server mainly provides functions of log-in, history, recognition management of power generation facility, environment setting and log-in.

TABLE I
SMART GRID POWER GENERATION MANAGEMENT SERVER MAINLY PROVIDES FUNCTIONS

No	Div	Function	Description
1	Log-in	User log-in	Function of user authentication
2		Password change	Function of changing user ID and password
3	Power generation facility history management	Inquiry of power generation facility information	Detailed information inquiry of power generation facility
4		Addition of power generation facility history	Addition of power generation facility history
5	Power generation facility recognition management module	Power generation facility recognition information storage	Feature point data storage of GPS, electromagnetic sensor data and panoramic image of power generation facility
6		Power generation facility recognition information inquiry	Feature point data inquiry of GPS, electromagnetic sensor data and panoramic image of power generation facility
7		Deletion of power generation information	Function of deleting registered power generation facility information
8	Environment setting	Server setting	Setting of server network and access
9		User setting	Setting of power generation facility manager account and authority
10	Log function	Power generation facility recognition module management log	Storage/inquiry of log record for a function of registration/inquiry/deletion being performed in power generation facility recognition management module
11		Power generation facility history management log	Storage/inquiry of log record for inquiry/addition of facility history being performed in power generation facility history management module

D. Guidance service of location-based smart grid power generation facility

Guidance service of location-based smart grid power generation facility is a service of guiding location of power generation facility so that worker may perform inspection for surrounding power generation facility based on location information obtained through mobile communication network or GPS as shown on Fig. 6 and by guiding location of smart grid power generation facility that is distributed widely, site worker could perform next inspection rapidly.

Location guidance service of power generation facility first reads latitude/altitude coordinates from GPS sensor of smart phone, transmits it to power generation facility management server and power generation management server obtains lineal distance (Euclid distance) with power generation facility location stored in server based on transmitted coordinates and guides location by transmitting location of power generation facilities to site manager through a stage of transmitting ID, GPS coordinates of power generation facility within radius of 5km.

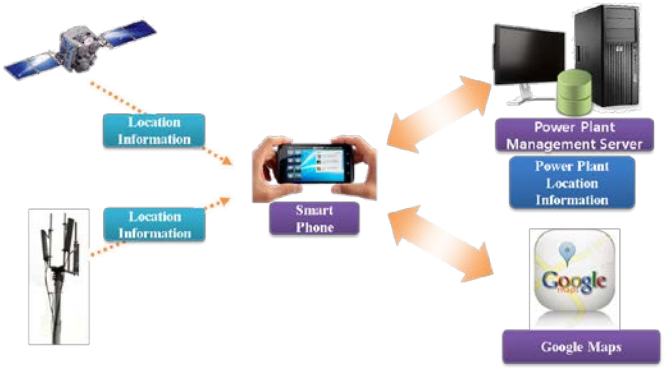


Fig. 6. Guidance service of location-based smart grid power generation facility

E. Smart phone application for smart grid power generation facility management

Major function of smart phone application using power generation facility recognition technology is to recognize power generation facility through smart phone image at site using power generation facility recognition technique and identify location information including its latitude/altitude being interfaced with Google map.

In addition, it may monitor current measurement information of facility such as voltage, current, active, reactive power, provide its detailed information for model name, manufacturer, hard ware layout and manage history of power generation facility.

Intuitive and convenient use is allowed by providing history management, current condition and HW related detailed information in a way of recognizing power generation facility through camera view of smart phone.

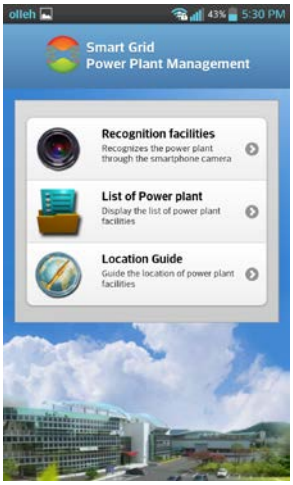
Smart phone application supports both android smart phone being utilized most widely and IPhone and its application was implemented in a hybrid mode using PhoneGap in order to ensure application to smart phone of diversified platforms based on development of just one time.

In addition, user interface of mobile application was composed by using HTML5 and JQuery Mobile and control module of GPS sensor and camera were developed by utilizing PhoneGap library and JavaScript.

Screen of the result of implementing smart phone for smart grid power generation facility management being suggested in this paper is as follows.

Fig. 7 is a screen of log-in implementation that certifies user by transmitting manager ID and password to server after receiving it at site and main menu implementation.

(a) Log-in



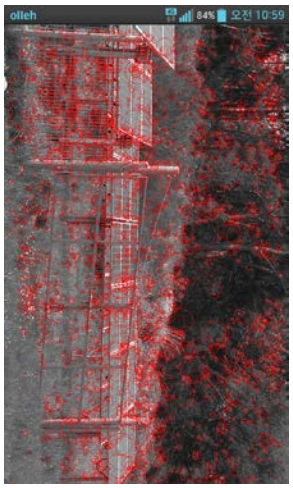
(b) Main menu

Fig. 7. User log-in and main menu

Main menu is composed of three menus including facility recognition that recognizes power generation facility through camera, power generation list that may inquire overall power generation facility and its location guidance and when touching relevant menu, each function is performed.

Power plant recognition transmits data to server after extracting feature points through SURF algorithm followed by photographing panoramic image by using GPS and image sensor of smart phone as shown on Fig. 8.

(a) Facility image 1

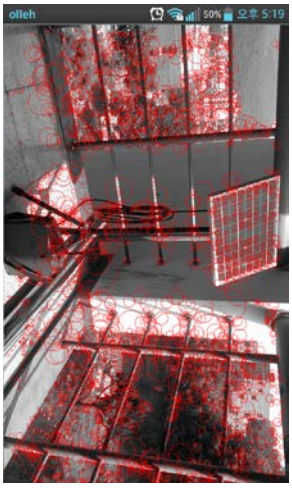


(b) Feature point extraction1

(c) Facility image 2

(d) Feature point extraction2

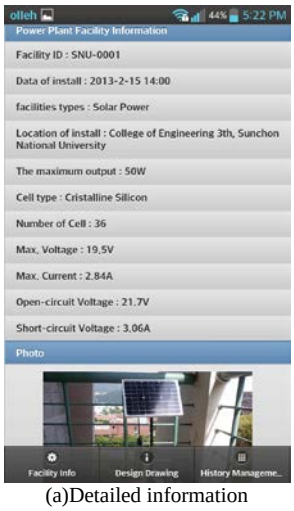
(e) Facility image 3



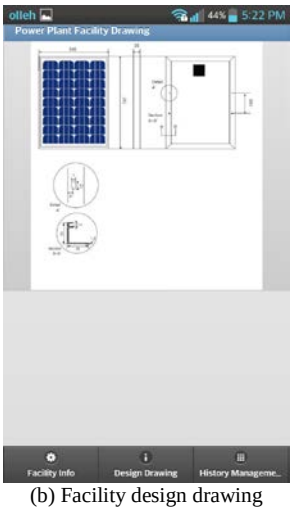
(f) Feature point extraction 3

Fig. 8. Facility recognition

In server, by matching transmitted data with stored data, coincided power plant is found out and as shown on Fig. 9, detailed information, design drawing and management history information of power plant are provided to workers through wireless communication.



(a)Detailed information

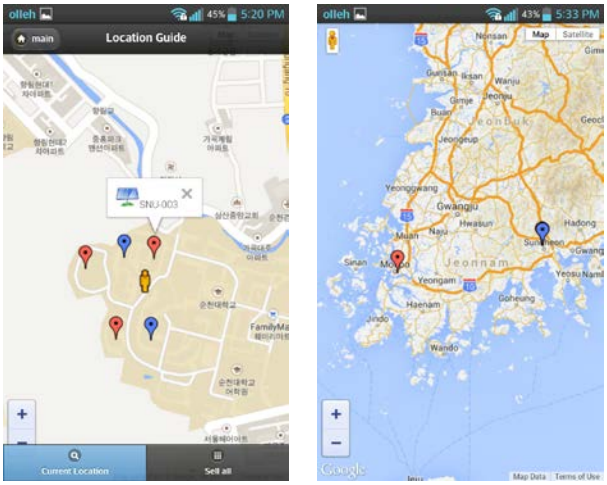


(b) Facility design drawing

(c) Facility management history

Fig. 9. Facility information

Site manager could receive information of current location and overall location of power generation facility as shown on Fig. 10.



(a)Current location guidance of site manager (b)Total location information

Fig. 10. Location guidance service of facility

When implementing location guidance service of power generation facility, it is guided through visualized Google map and when selecting marker of visualized power generation facility, type and information of relevant power generation facility are outputted.

marker being visualized in Google map indicates current location of site manager, marker indicates location of wind power generation facility and marker indicates location of power generation facility, respectively.

IV. EXPERIMENTS

Experiments were composed to test whether the proposed system recognizes power generation facilities and provides its status and detailed information.

The test-bed consists of a small solar panel, an inverter, a battery, a gateway, a power generation facility management server like Figure 11.

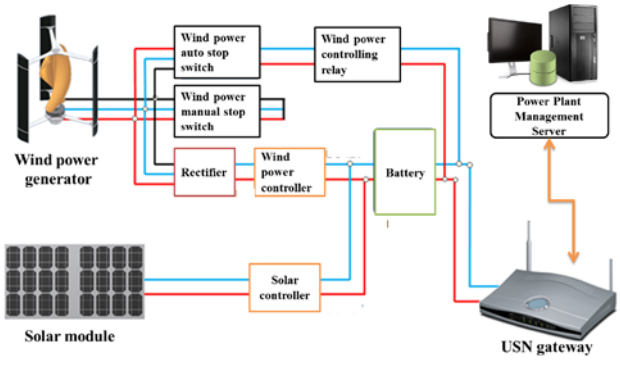


Fig. 11. Diagram of Test-bed

A test was conducted whether it would be possible to check the current status, measurement information, details and temporal data of the power generation facility module using a smart phone.

In addition, the results of a test on recognition rate and recognition time of the power generation facility by angle are like the following Table 2.

TABLE II
FACILITY RECOGNITION TEST

Evaluation item	Front	30°Side	45°Side
Recognition rate (%)	100	92	78
Recognition time (ms)	452	456	470

The power generation facility recognition rate of the proposed system was 100%, 92% and 78%, respectively in front, side angles 30° and 45° like Table 2. The recognition time was 452ms, 456ms and 470ms, respectively in front, side angles 30° and 45°.

It turned out that in spite of a little difference by angle, it recognized the power generation facility accurately, overall.

V. CONCLUSION

In this paper, facility recognition based mobile smart grid facility system by which site manager recognizes smart facilities by using GPS sensor and image sensor of smart phone or tablet PC and diversified information including detailed information, HW drawing, sensor data, management history of facility and location guidance are provided to site manager was suggested.

By having developed smart application based on hybrid architecture, it is expected that simultaneous support to almost all the smart phone platforms would be allowed based on its development of just one time and intuitive and convenience use would be possible by recognizing power generation facility through camera view of smart phone and providing its information to site manager.

In addition, as site manager is able to receive detailed information of facility at site, efficient maintenance for regular check-up and failure could be performed conveniently, overall operation cost could be reduced and furthermore, by using facility recognition technology instead of existing QR code, its direct application is possible without any need of adding equipment to smart grid facility currently under operation.

Owing to development of facility recognition service through markerless based facility recognition technology, it is expected that it may be expanded to technology recognizing T/R facility of smart grid and other facilities in the future and its cheaper construction would be possible as well.

ACKNOWLEDGMENT

"This research was financially supported by the Ministry of Education (MOE) and National Research Foundation of Korea(NRF) through the Human Resource Training Project for Regional Innovation (No. 2013H1B8A2032217).".

REFERENCES

[1] V. C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, and G.P. Hancke, "Smart Grid Technologies: Communication Technologies and Standards," IEEE Transactions on Industrial Informatics, vol. 7, no.4, pp. 529-539, Nov. 2011

[2] Zhong Fan, Parag Kulkarni, Sedat Gormus, Costas Efthymiou, "Smart Grid Communications: Overview of Research Challenges, Solutions, and Standardization Activities", IEEE Communications Surveys & Tutorials, Vol. 15, No. 1, pp. 21-37, 2013

[3] Nejad, M.F, Saberian, A.M, Hizam, H. Radzi, M.A.M, "Application of Smart Power Grid in Developing Countries", Power Engineering and

Optimization Conference (PEOCO) 2013 IEEE 7th International, pp. 427 – 431, 2013
[4] Kanghun Jeong; Hyeonjoon Moon, "Object Detection Using FAST Corner Detector Based on Smartphone Platforms," Computers, Networks, Systems and Industrial Engineering (CNSI), 2011 First ACIS/JNU International Conference on , pp.111~115, May 2011.
[5] Cimphony is a product of Open Grid Systems Ltd. Glasgow, UK
[6] McMorran, A. W., Rudd, S. E., Simmins, J.J., McCollough, N., Shand, C. M., "Field force data visualization: Developing an open mobile platform for integrated data access," Power and Energy Society General Meeting, 2012 IEEE, pp.1~5, July 2012
[7] Ming-Kuan Tsai, Yung-Ching Lee, Chung-Hsin Lu, Mei-Hsin Chen, Tien-Yin Chou, Nie-Jia Yau"Integrating geographical information and augmented reality techniques for mobile escape guidelines on nuclear accident sites", Journal of Environmental Radioactivity, Vol. 109, pp. 36~44, 2012
[8] H. Bay, T. Tuytelaars, L. V. Gool, "SURF: Speeded Up Robust Features," in Proceedings of the European Conference on Computer Vision, 2006.

.

Young-Jae Lee
Young-Jae Lee received the B.S., M.S degree from Korea Sunchon National University, Korea, in 2012, 2014 She is currently a Ph.D. student in computer science at the Sunchon National University, Korea, Her current research interests include augmented reality, image processing, computer graphics.

Eung-kon Kim(Corresponding Author)
Eung-kon Kim received the B.S. degree from Chosun University, Gwangju,, Korea, in 1980, his M.S degree from department of electronics, Hanyang University, Seoul, Korea, in 1987, his Ph.D. degree from Chosun University, Gwangju, Korea, in 1992. His current research interests are computer vision, virtual/augmented reality, image processing, and computer graphics. Currently he is a professor in department of computer engineering, Sunchon National University, Korea

Volume 3 Issue 5, Sep. 2014, ISSN: 2288-0003

ICACT-TACT JOURNAL

Global IT Research Institute

1713 Obelisk, 216 Seohyunno, Bundang-gu, Sungnam Kyunggi-do, Republic of Korea 463-824

Business Licence Number : 220-82-07506, Contact: secretariat@icact.org Tel: +82-70-4146-4991