International Journal of Smart Home
Vol.8, No.1 (2014), pp.23-34
http://dx.doi.org/10.14257/ijsh.2014.8.1.04

# A Study on the Emergency Alert Service using a Coordinates Techniques One-Time PAD in an T-DMB Environment

Kil-Hun Lee[1], Moon-Seok Jun[1] and Hyeon-Hong Kim[2]

[1]*Department of Computer Science, Soongsil University, Sangdo-Dong, Dongjak-Gu,Seoul, 156-743, South Korea*
*{clarkent83, mjun, rlagusghd}@ssu.ac.kr*

***Abstract***

*This paper focuses on the research of the problem and the prevention of the catastrophy which the T-DMB Emergency Alert Message would cause by changing the contents paralyze the national communication channels during the transferring process. The T-DMB Emergency Alert which is used when the Disaster occur. Using the notice support message of that program. Protecting not just vicious attacks but forceful channel transfer rights and sending coded no-public certification information coordination method along with video. Since suing T-DMB Emergency Alert Message could give the right to transfer channels and could be moved to a different channel. So in this case all T-DMB receivers are the targets of the vicious Emergency Alert Broadcast. This paper compares the current Emergency Alert Broadcast Service which T-DMB Broadcast and the One-Time PAD based message alert which traditional service model provides. Suggested research content could be applied to all other Emergency Alert casts of digital broadcasts and national broadcasting system.*

***Keywords:*** *T-DMB, AEAS, One-Time PAD, OTP*

## 1. Introduction

Korea changed the broadcasting circumstance in whole country through T-DMB, satellite-based DMB, TV, and radio since 2002. T-DMB began to mobile broadcasting service on the world-first-metropolitan since December 2005, and it is essential requirement for market condition that become private and portable such as navigation. T-DMB has superior portability and mobility compare with technology, and taking advantage for low install cost and wide-coverage.

Also, when the concerning about the possibility of occurrence of local, national disaster and situation of disaster is exist, through disaster broadcasting service which is inherent in T-DMB their own lives and property can be protected by receive useful information immediately. Disaster broadcasting service is explaining of automatic

Disaster warning broadcasting service(T-DMB Automatic Emergency Alert Service: AEAS) of T-DMB, means the transmitting of information about disaster by using data channel of T-DMB without stopping of watching-broadcasting through the disaster cast, and the expediting of warning with the media device such as DMB to people of a certain unit disaster.

But if this great Emergency broadcasting service can cause national and individual dangerous security vulnerability when manipulate sent-received disaster information of data channel. Emergency Alert message can used through multi-media such as Terrestrial, Satellite, Cable, Internet for disaster warning business, and can service data and audio information through various route used on TV and radio. Also there is the possibility for massive damage

ISSN: 1975-4094 IJSH

when it abuse regardless of existing-broadcasted information, because the expedite broadcasting about necessary information to broadcasting licensee can be requested. The security plan that applying on automatic EAS broadcasting of T-DMB just regulated receiver that using by intention of broadcasting. Therefore in this situation, abusing disaster broadcasting service of malice attacker can cause national distrust and chaos of users who received message when the attacker seize and deterrent disaster prediction and warning message, or broadcasts fake message to the area with intention.

For the security method for prevent it, provide of automatic disaster warning broadcasting service which is secure for people through grafting One-Time PAD to data packet. In this paper, data transfer security method which applied One-Time PAD between area which EAS message is outputted to receiver from receiver and the area reaching to receiver through broadcasting/communication media from disaster warning transfer institution.

## 2. Background Research

### 2.1. T-DMB (Terrestrial-Digital Multimedia Broadcasting)

DMB is kind of broadcasting service that provides multimedia signal that changed to digital way such as sound, video to automobile-receiver and mobile. Through combining the concept of multimedia broadcasting to DAB (Digital Audio Broadcasting) which is existing radio technology, additional transmit of data information such as weather, news, location became possible, and the help for emergency is being possible through disaster warning broadcasting service.


**Figure 1. T-DMB (Source: DMB Allience)**

DMB classified to T-DMB and satellite DMB. T-DMB is multimedia broadcasting for receive transmit program on ground through using frequency, satellite DMB provides broadcasting service with satellite. Satellite DMB have disadvantage that receive is not actively available in building-densely populated area and it is available with pay. This paper studies about automatic disaster broadcasting service T-DMB that can use for free and having advantages about continual service while moving in metropolitan.

### 2.2. AEAS(Automatic Emergency Alert Service)

AEAS means T-DMB automatic disaster warning broadcasting service standard, and it is the kind of disaster information delivery service released for disaster forecast, warning and expedite broadcasting to whole people in country through using mobile, tablet, car navigation and other new media. It developed through 2 years in disaster broadcasting working group of

 

Korean information communicational technology association (TTA) DMB project group(PG801) since 2005, and published as information communication group standard, and conducted as 'DMB disaster warning data broadcasting' since August, 2010. The main contents of standard shows the detail of definition of service, requirement, and protocol stack, transmit specification and processing regulations and used code information.

The current method showing emergency message divided to two kind of way, outputting specific image and text to the center of the screen, and the bottom of the screen. However, encryption of emergency message transfer and output part does not occur at all. In each broadcasting station, service settings for T-DMB to formation of guarantee for just frequency band and transfer speed and the security is vulnerable. In this paper, One-Time PAD is added for the defense techniques for invasion attack to the part.

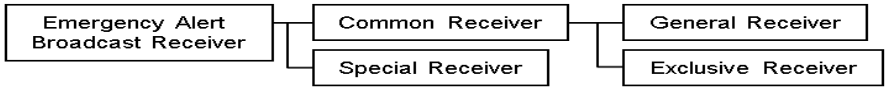


**Figure 2. Division of Emergency Alert Service Receiver**

Disaster warning broadcasting changes internal information according to the classification of receiver. The main study is about the general receiver. Disaster warning message is based on text and it can transfers multi-disaster form such as audio, still-image, video, data through sub channel at same time Information transmitted automatically through T-DMB network.

Disaster warning service time, duration, appoint time should be displayed on receiver and EAS Text should be able to transfer up to 180byte(bytes)(Korean 90 letter). Disaster message defines the class method and dividing method of disaster message. Looking for Protocol stack, the maximum length of disaster message is 416 bytes, however the method suggested in this paper requires the encryption have same length as the length of entire size of disaster message, 1024 bytes (1 Kbytes) message length should be ensured.

| Alert Priority | Contents | Display Contents |
|---|---|---|
| 00 | Unknown | |
| 01 | Normal | Text Information |
| 10 | Emergency | Text + Alarm |
| 11 | Greatly Emergency | Text + Alarm |

| Emergency Region Code | Contents |
|---|---|
| 000 | The Nation of Korea |
| 001 | Korea Government Designation |
| 010 | Administrative District Notation |
| 011~111 | Rfu |

**Figure 3. Warning Priority and Instances of Disaster Area Form**

In standard, there are the meaning and grammar for regulate on each field, they gives the roles due to the importance of warning. The meaning and displaying way of disasters code are changed due to the priorities, and appoint day and time are represented to each bit. Area code is quite important because it shows the code that means disaster area, so the massive chaos can caused when the area code is confused or abuse during use Emergency Alert message.

### 2.3. OTP(One-Time PAD)

One-Time PAD (Now-called OTP) is disposable password system that verifying user by different password every time. OTP examine the validity of disposable password according to the promised-rules between each other regardless of formation.

The frequency of occurrence of each text is all same and length of plaintext and length of secret key are composed by same n-random texts. For example, in the case of sending message 'HELLO', both transmitter and receiver pass encrypting/descrambling process

through using same module (random table). In this moment, the letter of each text message of pad changed to prepared number and calculates key and message.

Thus, sending the mass of the secret key securely is quite difficult. However when the secret key is created by using specific random table, the secret key becomes perfect password. It called stream password in other words. If generating pseudo random numbers with a small amount and creation of cryptographic secure secret key on every different time is possible, it will be very economic and effective encrypting/descrambling process. This paper suggests the method that creates Emergency Alert Service broadcasting message that PAD is applied.

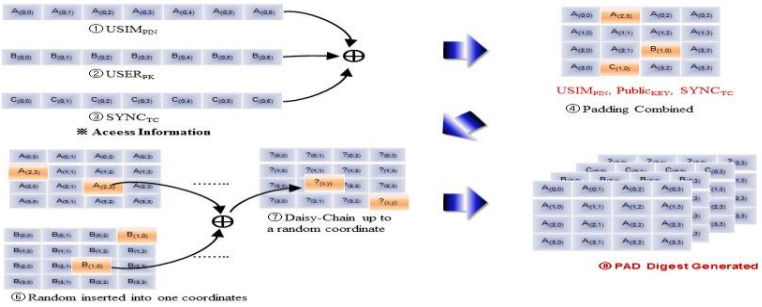


**Figure 4. Chain Structure of the OTP PAD**

## 3. Suggested Context

### 3.1. Abstract of Suggested System

Automatic disaster warning broadcasting service that suggested on this paper pass the process of data encryption of additional areas by random figure of OTP(One-Time PAD) algorithm. Encrypted data could not be opened until the verification of OTP is completed, and taking the process of normal disaster broadcasting service after confirms the information is secure.

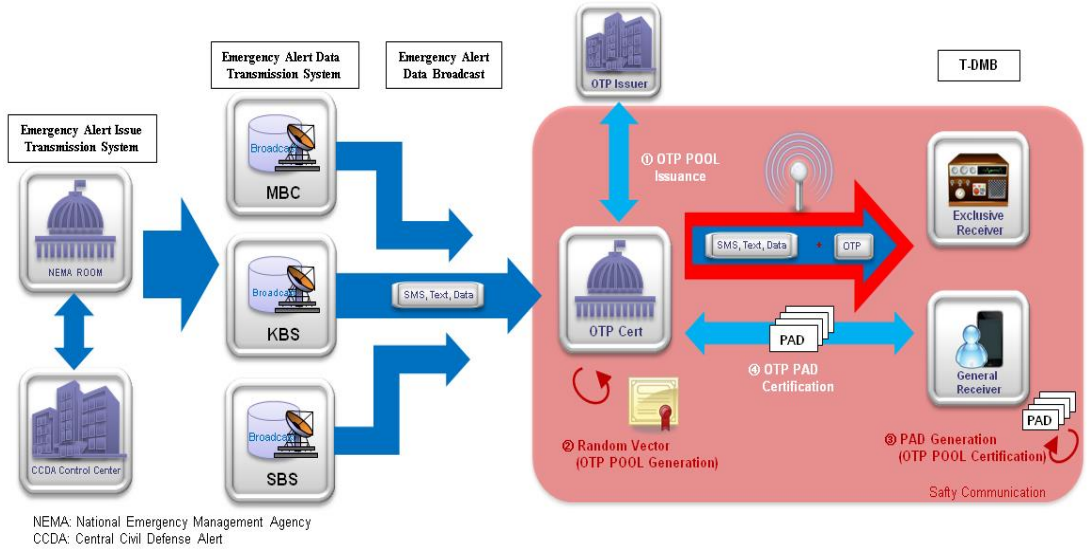


**Figure 5. Entire Structure of Suggested System**

Verified data transmitted to certain rate and the verification is maintained until additional verification is required. Information used for OTP uses terminal USIM and IMEI information and utilizes digest number which is temporary OTP POOL that applicable for any system.

Module form of digest verification creates secret key of different structure in circumstance of even any different data form and possesses strong immune properties for idle time and man-in-the-middle attack through applying suggested coordinates techniques. Entire structure of suggested system operates the process that outputting information after OTP verification with receiver through verified information of each area such as (Figure 5) below.

Moreover, it is assumed that the channel between national emergency management agency disaster situation room and broadcasting station is secure. The operating process of verification from generating of disaster warning on entire structure is like the picture below.

Step 1. When the warning is generated central Civil Defense warning control station, disaster warning of national emergency management agency disaster situation room appoints transmit system appoint warning.

Step 2. Appointed disaster warning passes the transfer preparing level through each broadcasting station and disaster warning data transmit system.

Step 3. Before the transferring, transfer each area-base station after applying random coordinate's encryption with base station information which will transfer to data through OTP verification institution. The base station information means the base station which is registered on each broadcasting systems.

Step 4. After the first verification in base station of each area, transfer encryption data to each area's terminal which is for their own.

Step 5. Received terminal creates OTP PAD with base station information to confirm base station information on first verification.

Step 6. Pass confirm process through transferring created OTP PAD to OTP verification institution, and operate disaster warning data broadcasting according to whether it is out of order or not.

According to 6levels of process above, automatic disaster warning broadcasting service through OTP verification of PAD formation is completed and malice transfer area information which is not registered for transfer area is deterrence through first verification. Issue and verification protocol

### 3.2. Issue and Verification Protocol

Suggesting issue and verification protocol show the process of disaster warning data broadcasting after T-DMB-passed OTP through disaster warning data transmit system in verification disaster warning appoint transmit system.

Spoofing and sniffing are the representative example for the route that middle-in-attack can generate in base station. Base station information that first verification and terminal information that and second verification are verified without division, so the entire protocol is written for only once. Also, verification number of terminal information is replaced to IMEI number through this process. (Figure 6) is the detail protocol about issue and verification, and the explanation for each level is like below.

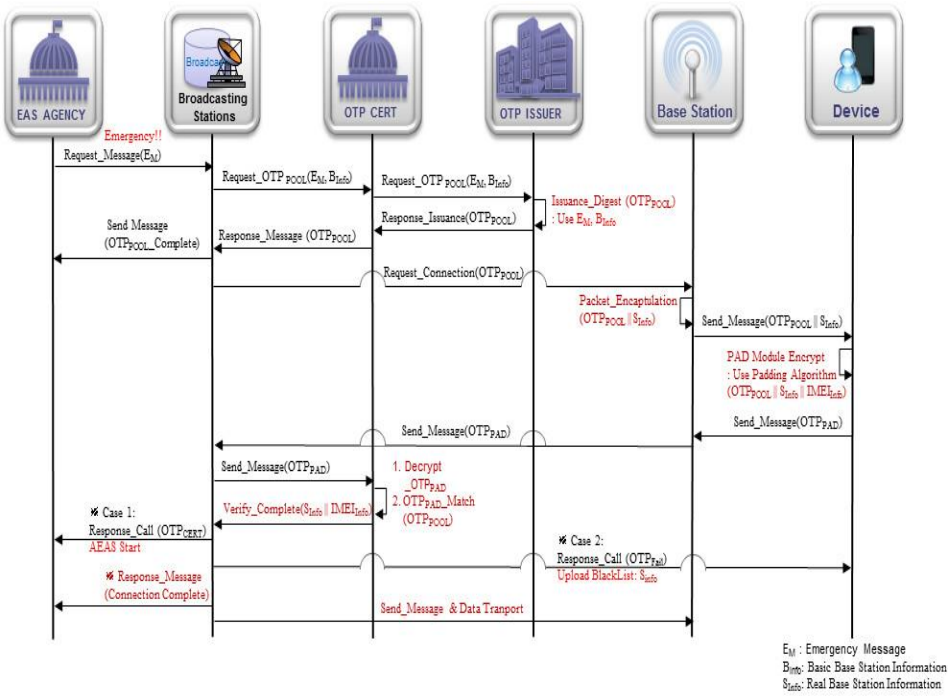


**Figure 6. Issue and Certification Protocol**

Step 1. Transmit signal of generate of disaster situation to each broadcasting system through receiving civil defense warning in national emergency management agency disaster situation room.

Step 2. In each broadcasting stations which are Disaster warning data transmit system, the verification is required to OTP verification institution by transferring OTP issue information which possessed as the pre-level before secure data communication is completed. (Assuming holding OTP issue information is secure)

Step 3. OTP-verification-requested OTP verification institution requests OTP POOL issue to OTP issue institution.

Step 4. Issue OTP POOL after confirms OTP issue information (base station information hold by broadcasting station and appointed disaster warning message).

Step 5. OTP POOL including verification information is received to each broadcasting station from OTP verification institution.

Step 6. Broadcasting station transmits message that broadcasting is prepared to national emergency management agency disaster situation room.

Step 7. Disaster warning data transmit system transmits message of requesting connection to base station which disaster broadcasting will be connected.

Step 8. In each base station, the message that disaster situation is generated is transmitted to terminal located on each area through encapsulate base station information to OTP POOL.

Step 9. In terminal, create One-Time PAD (now-called OTP PAD) which using base station information, terminal IMEI, OTP POOL through operating verification module.

Step 10. Created OTP PAD transferred to OTP verification institution through base station and disaster warning data transmit system (broadcasting station).

 

Step 11. OTP PAD descrambled through module in OTP verification institution, and OTP POOL information is verified, and broadcasting station base station information and terminal information are verified.

Step 12. In disaster warning data broadcasting station which confirmed each information, when after determine that the information have no problems, provide disaster warning service to the route. However when determine it is malice route, stop disaster broadcasting on the area and post base station on black list.

Step 13. Begin disaster warning broadcasting service after announce to national emergency management agency disaster situation room that the route for start broadcast is secured.

### 3.3. Coordinates Techniques One-Time PAD

Through looking for protocol stack for the Disaster warning service, there is the frame structure creates on each class. In this section, enhanced transfer security method is suggested through packet form having coordinate structure due to the feature of One-Time PAD encrypting same capacity as the general disaster warning message.

Looking for Disaster message class, it give existed padding number through OTP message which is the same length as existing disaster message and adding message which the encryption is applied existing Padding. So, entire length of disaster message should be 1024 bytes (1 Kbytes), and using of disaster message without the information of encryption way used in module.

However there is the worry for decrease of efficiency due to the two-times increasing of suggested protocol stack increases two times, continual DMB communication can achieved through memory of terminal after first verification on each area.

OTP module used on terminal and OTP verification institution have same secret key structure, and the information usable in OTPPOOL includes disaster appointer, disaster appoint institution, warning priorities, disaster area formation, number of disaster area, disaster generate time, OTP publication time, Administration Building code, disaster warning data(text, audio, video, *etc.*).

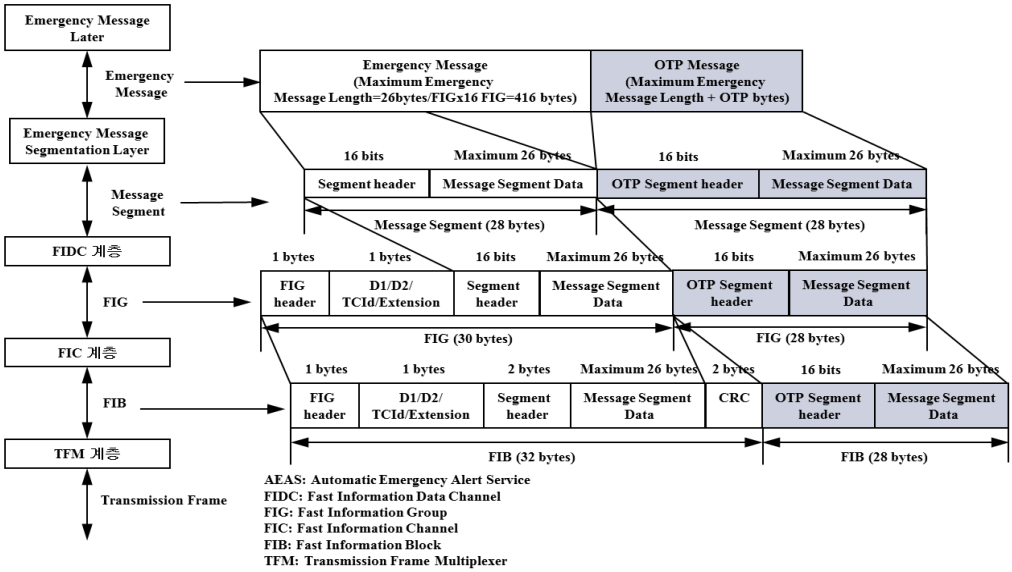


**Figure 7. Suggested Protocol Stack and Frame**

When it transferred, it creates OTP coordinate information random number according to information list by combination of information between transmitter and receiver in each module. Information of coordinate should be smaller than disaster warning message, OTP information should applied increasingly as the data size of divided class. Through the referring of stack information used in Module, the reduction of the coordinates of the random number method size is possible.

## 4. Performance Evaluation

### 4.1. Implementation of Environmental

**Table 1. System Development Settings**

| Category | | Contents |
|---|---|---|
| Server | OS | Windows7 Home Premium K SP1 (x64) |
| | H/W | Intel® Core™ i5-3317U CPU @ 1.70GHz RAM 8.00GB |
| | Development Tool | Visual_Studio_2010_Premium |
| | Algorithm | AES |
| Client | OS | MS-Windows_Phone_SDK_7.1 (Mango) |
| | H/W | Nokia_Lumia_710 |
| | Algorithm | AES |

This paper write design of suggested disaster warning broadcasting service and result of realization and efficiency evaluation [Table 1] shows realization circumstance operating realized application. And realized operating screen can showed through windows mobile application.

OTP information number realized in this paper shows the send and receive information continually, but does not show the actual usage. (For convenient, emulator screen of Windows Phone 7.1 Mango replaces realization of T-DMB function, because the Korean version is not applied.)

### 4.2. Implementing Screen

To provide Emergency Alert Service broadcasting during ordinary watching T-DMB, message below being outputted on screen and the process for verify the disaster broadcasting message it started. Due to the completion to mobile-communicative company of the registration for using device existing DMB service, the process is proceed without additional log-in or sign-up. Receiver cannot use Emergency Alert broadcasting until the verification is completed. However the process is to prevent man-in-the-middle attack or forgery, so it proceeds essentially.

Looking for the screen, there is the situation of short signal lost in message process when verification is loading. When verification being unavailable by malice attacker or problem for connect process is determined, the output OTP verification and message are lost like the first screen.

 

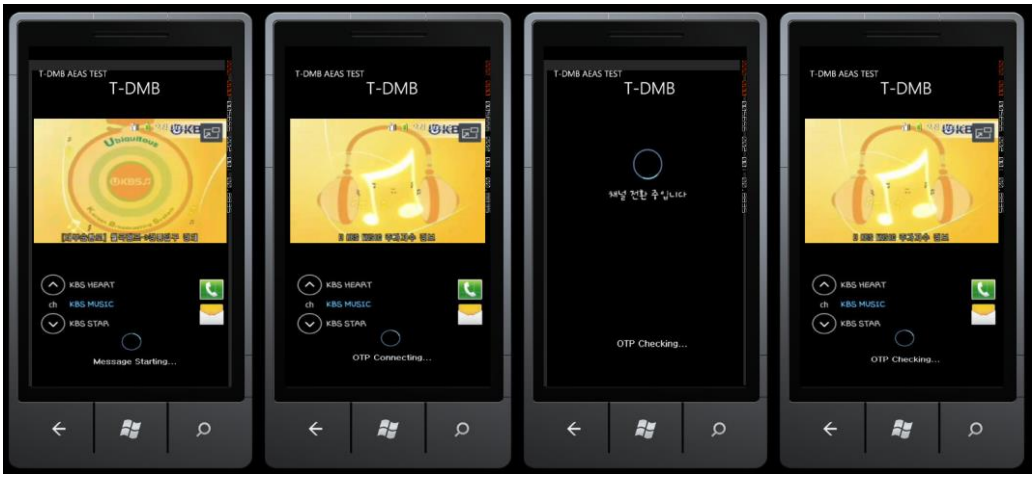


**Figure 8. Receive-Waiting before OTP Verification and Verification Process Screen**

After the completion message is outputted above connection-completed DMB screen. Emergency Alert Service broadcasting message is outputted base station verification which is first verification starts Emergency Alert Service broadcasting after completion of verification to receiver holding OTP to receiver cannot cognize it and disaster and warning information about their local information is received.

For the confirmation of Location information, the device which the verification had completed determines whether the Emergency Alert Service is counterfeited or not through verifying and comparing of transferred OTP random number and random table of OTP module.

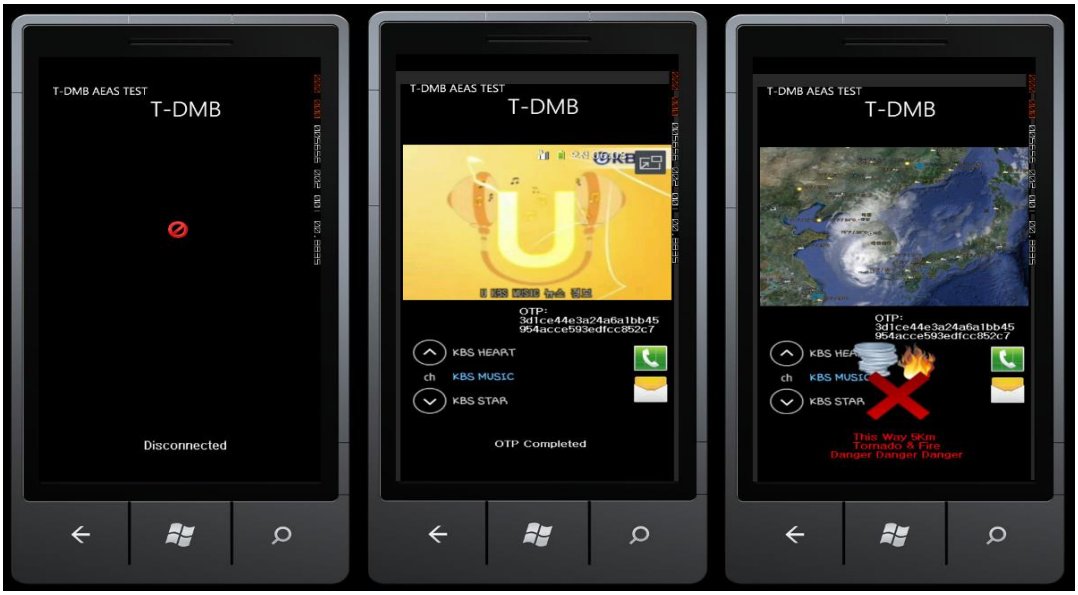


**Figure 9. Failure Screen of OTP Verification and Operation screen EAS Broadcast**

Through looking for existing Emergency Alert Broadcasting Service, when disaster is generated the measure for outputting of specific screen, sound, and text is adopted.

The security is certain enhanced compare to existing disaster broadcasting service through using OTP which applying the coordinate technique that making data to random number for protect the output such as Hurricane, fire, earthquake, national emergency.

### 4.3. Security Verification to Implementation Result

| Security Requirements | | Existing System | **Suggested System** |
|---|---|---|---|
| 3 | ID / Password Attacks | SAFETY | SAFETY |
| | Phishing / Pharming | UNSAFE | SAFETY |
| | Message Counterfeiting | UNSAFE | SAFETY |
| | Sniffing / Spoofing | UNSAFE | SAFETY |
| 2 | Replay authentication Information | UNSAFE | SAFETY |
| | Generating Authentication Information Leakage | UNSAFE | SAFETY |
| | Man-in-the-Middle Attacks | UNSAFE | SAFETY |
| | Session Hijacking | UNSAFE | SAFETY |
| | Trade Deny | UNSAFE | SAFETY |
| 1 | Physical Attacks | UNSAFE (Only Device) | SAFETY (Device + One-Time PAD) |

**Figure 10. The Difference between Existing Method and Suggested Method**

Through the verifying and comparing of efficiency and security of Existing Emergency Alert broadcasting service, suggested systems security is superior certainly. However, existing verification system has faster verification speed than OTP verification system on data transfer rate in verification process for service connection.

This Figure is the graph about the security of existing system and suggested system. To verify the security of apply technology, security threat of sniffing, spoofing, prevent of deny, illegal AP, man-in-middle attack are applied.

Looking for proven results, security of recent OTP verification way is good, but there is the poor part in generating. However, under the assumption that there is no physical vulnerability by default, the conclusion of secure was drawn through the security validation.

## 5. Conclusion

If One-Time PAD technology that these coordinate technique is applied used in disaster warning broadcasting service of T-DMB system, the result will be derived that poor operating existing system speed and efficiency. However, suggest way is very secure from takeover due to the man-in-the-middle attack, modulation, fake attack, by the verification through OTP random number with module.

If EAS broadcasting is abused it is clear that a tremendous impact will be load. In these days, security techniques that applied on Emergency Alert broadcasting Service are not applied. The method that suggested in this paper taking the advantage to support secure communication and deterrent the disadvantages that receiver can get damage without checking whether it is counterfeit or not. Thus, the better OTP security defense techniques

 

can be adopted in future, through Emergency Alert Service broadcasting, provide of fast service to user will be possible while reducing the risk of national loss.

## References

[1] M.-S. Baek, Y.-H. Lee, G. Kim and S.-R. Park, "Development of T-DMB Emergency broadcasting system and trial service with the legacy receivers", Consumer Electronics, IEEE Transactions, vol. 59, no. 1, **(2013)** February, pp. 38-44.
[2] P. Calduwel Newton and L. Arockiam, "A Quality of Service Performance Evaluation Strategy for Delay Classes in General Packet Radio Service", IJAST, vol. 50, **(2013)** January, pp. 91-98.
[3] K. Lee and M. Jun, "A Design of Coordinates Techniques One-Time PAD for a Secure Transmission with Key in PKI Environment", Soongsil University, **(2012)**.
[4] S.-G. Kwon, S.-H. Lee, E.-J. Lee and K.-R. Kwon, "T-DMB Receiver Model for Emergency Alert Service", ICCSA Part IV, LNCS 7336, **(2012)**, pp. 434-443.
[5] I.-K. Lee and Y.-O. Park, "Study on Coexistence between Long Term Evolution and Digital Broadcasting services", IJAST, vol. 38, **(2012)** January, pp. 75-92.
[6] Y.-H. Lee, G. Kim and S.-R. Park, "An efficient emergency broadcasting signal multiplexing method for supporting the legacy T-DMB receivers in break-in system", Consumer Electronics IEEE Transactions on vol. 57, no. 5, **(2011)** November, pp. 1550-1555.
[7] J. Park, J. Chung and H. Kang, "Design of disaster alerting information disseminator", NISS, 5th International Conference on New Trends, vol. 1, **(2011)**.
[8] S.-G. Kwon, H. Jun and S.-H. Lee, "TII based T-DMB location AEAS receiver model", Multimedia and Expo, IEEE International Conference on ICME, **(2009)** June, pp. 1286-1289.
[9] A. Kumar and D. Akopian, "A secure wireless mobile-to-server link", Multimedia on Mobile Devices SPIE vol. 7256, pp. 14-22, **(2009)** January.
[10] Q. Y. Dai, R. Y. Zhong, M. L. Wang, X. D. Liu and Q. Liu, "RFID-enable Real-time Multi-experiment Training Center Management System", IJAST, vol. 7, **(2009)**, pp. 27-48.
[11] Z. Xin and W. Xiao-dong, "Design and Implementation of Hybrid Broadcast Authentication Protocols in Wireless Sensor Networks", IJAST, vol. 2, **(2009)** January, pp. 63-70.
[12] L. K. Moore, "The Emergency Alert System(EAS) and All-Hazard Warning", **(2009)** June 26.
[13] S. Jong Choi, "Analysis of Emergency Alert Services and Systems", Convergence Information Technology, **(2007)**.

## Authors

**Kilhun Lee** received his B.S. degree in Information Communication Science from Seoil University, Seoul, Korea in 2009, and his M.S. degree in Computer Science from Soongsil University, Seoul, Korea in 2012. He is a researching in Ph.D. course of Soongsil University since 2013. His research interests Secure communication and Information security and Mobile Security and Multimedia Security.

**Moonseok Jun** received his B.S. degree in Computer Science from Soongsil University, Seoul, Korea in 1981, and his M.S. and Ph.D. degree in Computer Science from University of Maryland, Maryland, United States, in 1986 and 1989, respectively. He has been lecturing Computer Science in Soongsil University since 1991. His research interests information security and PKI and cryptography.

**HyeonHong Kim** received his S.I. degree in Computer Science from Seoil University, Seoul, Korea in 2009, and his M.S. degree in Computer Science from Soongsil University, Seoul, Korea in 2013. He is a researching in Ph.D. cource of Soongsil University since 2013. His research interests secure communication and Network security and information security.