

An efficient MSD protection and authentication scheme for automotive ICT based emergency call system

Nam-Uk Kim*, Tai-Myoung Chung*

*Department of Computer Engineering, School of Information and Communication Engineering,
Sungkyunkwan University, Suwon-si, Republic of Korea
nukim8275@gmail.com, tmchung@skku.edu

Abstract— An automotive ICT based emergency call system can automatically detect a vehicle accident, and send the information necessary for life-saving activity and accident handling in the form of an MSD(a minimum set of data) to emergency center. If network environment is based on TCP/IP, generally the easiest and safe application of security measures to MSD is to use TLS or DTLS. However there is a critical difference between emergency call operation environment and the other common operation environments, and this difference makes an important issue when it comes to applying TLS or DTLS to MSD delivering. Considering this issue, this paper proposes a secure communication protocol for MSD transmission in automotive ICT based emergency call system.

Keywords— e-Call, MSD, Security protocol, Message protection, Authentication

I. INTRODUCTION

In an automotive ICT based emergency call service, an ICT device in a vehicle detects car accident using various sensors, and automatically sends geographic location of the accident scene and other relevant data to emergency center, so that emergency relief agencies can quickly deal with the situation. The data sent from device, which is called MSD(a minimum set of data), to emergency center is highly recommended to be protected by security measures such as peer authentication, confidentiality and message authentication.

In Europe, e-Call system uses in-band modem for MSD transmission. In other words, the vehicle uses voice channel for MSD delivering for reliability[2]. However, in some countries like South Korea, using in-band modem for MSD transmission is impossible. Alternatively, MSD can be transmitted through typical TCP/IP based network environment in those countries. And if network environment is based on TCP/IP, generally the easiest and safe application of security measures to MSD is to use TLS or DTLS. However if TLS/DTLS is applied to MSD transmission, handshake for negotiating cryptographic security parameters between client and server has to be done right before MSD sending. It means that remarkable delay cannot be avoided until MSD starts from the device. Considering the accident information has to be sent quickly before the device is

destroyed, this feature of TLS/DTLS would be a major drawback. Considering this issue, this paper proposes a secure communication protocol for MSD transmission in automotive ICT based emergency call system.

The remainder of this paper is organized as follows. Section II briefly introduces automotive ICT based e-Call system. The main issue with adopting security measures to MSD transmission is presented in Section III. Section IV proposes a scheme for MSD protection and authentication. Finally, conclusions are drawn in Section V.

II. E-CALL SYSTEM MODEL

Automotive ICT based e-Call system's primitive goal is to automatically detect car accident using various sensors in a car, and send relevant information to e-Call center so that emergency relief agencies can quickens following process: recognizing vehicle accidents, getting detailed information of situation, and making a decision about what to do next.

An e-Call system has three components, which are accident emergency call device (AECD), e-Call center and emergency agency (EA), as figure 1 shows.

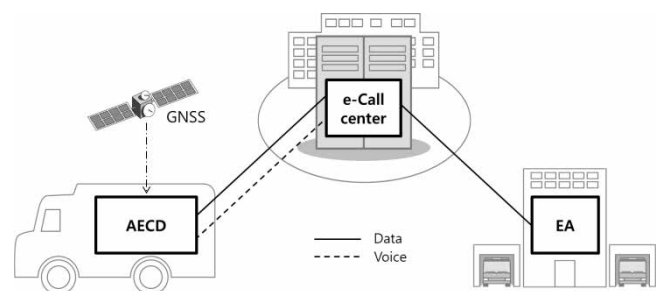


Figure 1. e-Call system architecture

An AECD collects data from various sensors and runs accident detection algorithm with the collected sensor data. If an AECD detects car accident, it calculates the exact location of the car using GNSS signal, and sends MSD to e-Call center. The device also provides voice call function for speaking with an e-Call center agent. A MSD is composed of timestamp, vehicle type, location of the vehicle, direction the vehicle is heading, call back number, etc. Final decision of whether it is

a valid situation for emergency is made in e-Call center, and it will deliver rescue request to EA if it is concluded to be real emergent situation.

If AECD detected an accident and AECD was not destroyed by the physical impact, following mechanism will processed without any problem.

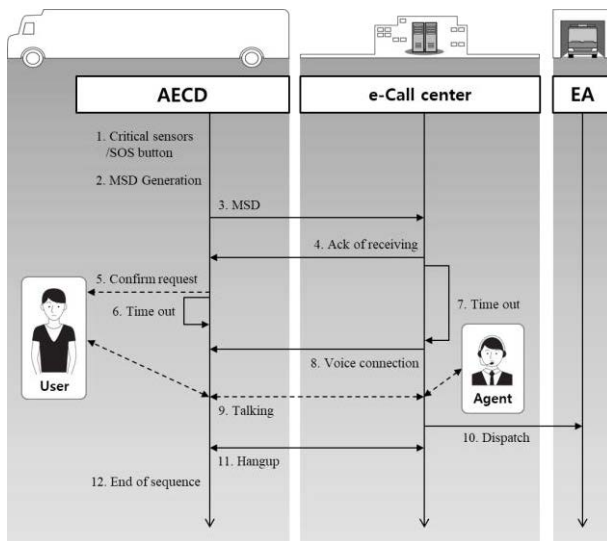


Figure 2. e-Call accident handling mechanism

- **step 1,2,3,4** : AECD detects an accident, generates MSD, and sends it to e-Call center . AECD confirms receipt by checking ack message.
- **step 5** : AECD informs a driver/passenger that the notification of accident has been delivered, and requests him/her to choose whether confirm or cancel the notification.
- **step 6, 7** : If a driver/passenger does not answer to the request before timeout, e-Call center assumes that there have been real accident. These steps are for the situation in which any person in the car is unavailable to answer due to aftermath of the accident.
- **step 8, 9** : e-Call center tries to call a driver/passenger. If he/she does not answer the call until timeout expires or asks for help, e-Call center concludes that people/a person in the car is in need of help, and e-Call center agent keeps the call open to get more detailed information of the situation.
- **step 10** : e-Call center agent request EA to dispatch the rescue team to the scene of the accident.
- **step 11, 12** : terminate all process

III. PROBLEM STATEMENT

As previous chapter mentioned, an MSD includes vehicle number, vehicle type, location of the vehicle, call back number (may be phone number), etc. It means that MSD carries personal information, though this information does not seem to be critical. However, it still contains risk factor in terms of security, so it is recommended to be protected.

The most critical security problem with MSD transfer is that when an MSD is manipulated maliciously, e-Call center

would get wrong information about the accident situation and it can lead to more serious personal injury or even death. If fake MSD can be generated and send, emergency agencies are likely to suffer headaches due to a new type of prank call. Therefore, application of security measures such as peer authentication, confidentiality and message authentication to MSD that is sent from AECD to e-Call center is highly recommended.

If network environment between AECD and e-Call center is based on TCP/IP, generally the easiest and safe application of security measures to MSD is to use TLS or DTLS. However there is a critical difference between e-Call operation environment and the other common operation environments, and this difference makes an important issue when it comes to applying TLS or DTLS to MSD delivering.

Think about that the AECD can be physically damaged with a high probability right after the accident has occurred. And unfortunately MSD generation and sending, which are the core function of AECD, might activated very often at the time of accident. Nevertheless, as long as the MSD can be transmitted before the AECD is damaged, emergency rescue can proceed without much problem, as you can see in figure 3

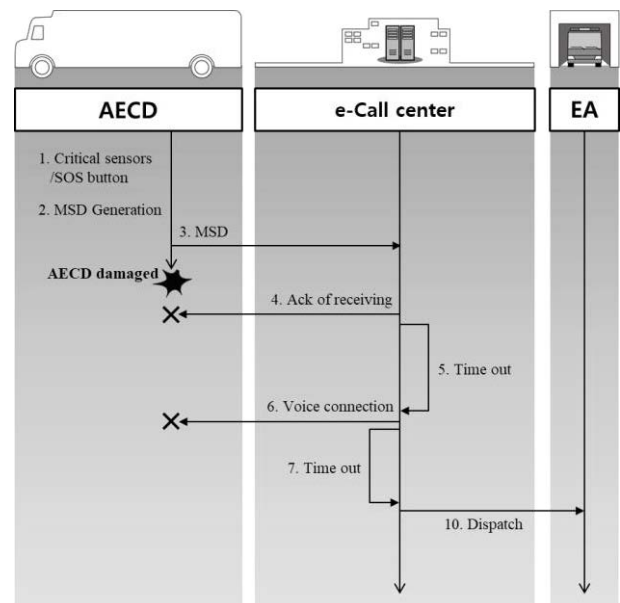


Figure 3. e-Call accident handling mechanism
(If AECD is damaged after MSD has been sent)

However, the longer the time between MSD generation and sending, the probability that AECD will be unavailable to send a MSD to e-Call center will increase(see figure 4).

In TLS/DTLS based MSD transport environment, both sides of communication must establish a security session before delivering MSD. The security session is established by handshake protocol, which takes at least 2 RTT (Round Trip Time) + α (α includes the time it takes to perform a cryptographic operation on each side). Therefore, the handshake procedure causes a remarkable delay in MSD sending, so AECD might be destroyed during handshake procedure depending on the situation. Considering this issue,

this paper proposes a secure communication protocol for MSD transmission in e-Call system.

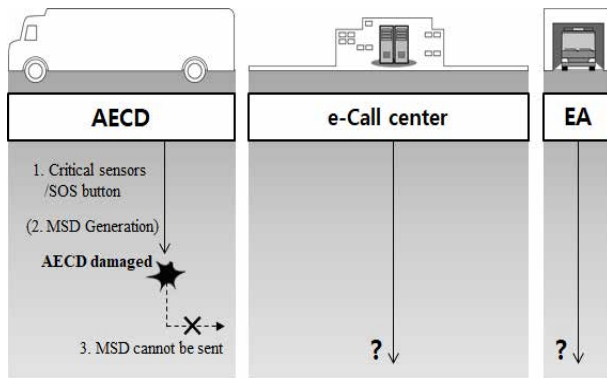


Figure 4. e-Call accident handling mechanism (If AECD is damaged before MSD has been sent)

IV. PROPOSED MSD PROTECTION AND AUTHENTICATION SCHEME

This section proposes an efficient MSD protection and authentication scheme for automotive ICT based emergency call system.

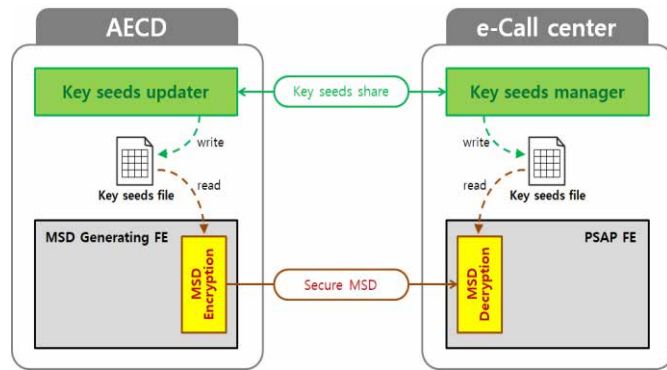


Figure 5. Proposed MSD protection and authentication scheme

The secure e-Call communication protocol has following features.

- A key seeds sharing protocol is activated at the time that is not related to MSD transmission, as a distinct process, once at fixed period.
- All cryptographic security parameters are negotiated during key seeds sharing process.
- If AECD detects an accident, MSD is protected using shared security parameters and sent to e-Call center.

Through a key seeds sharing process, an AECD and a e-Call center securely share a 2-dimensional random number array. For example, suppose a 4x4 random number array like figure 7 is shared between two nodes.

n bytes			
$R_{0,0}$	$R_{0,1}$	$R_{0,2}$	$R_{0,3}$
$R_{1,0}$	$R_{1,1}$	$R_{1,2}$	$R_{1,3}$
$R_{2,0}$	$R_{2,1}$	$R_{2,2}$	$R_{2,3}$
$R_{3,0}$	$R_{3,1}$	$R_{3,2}$	$R_{3,3}$

Figure 6. 4 × 4 random number array example

For a predefined period, symmetric keys are derived from this array and used for MSD encryption/decryption. They also used for message authentication. As shown in figure 7, the mechanism for generating a symmetric encryption/decryption key from the array is very simple.

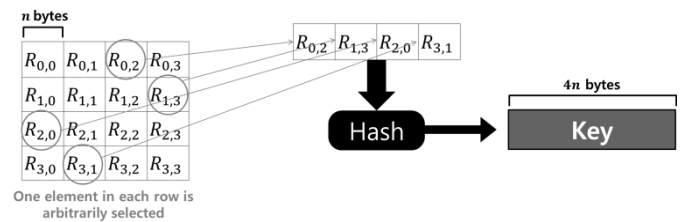


Figure 7. Generating a symmetric encryption/decryption key

A. Key seed sharing mechanism

The overview of key seeds sharing mechanism is described in figure 8. This mechanism is performed when AECD is first turned on or when the expiration date of key seeds has passed.

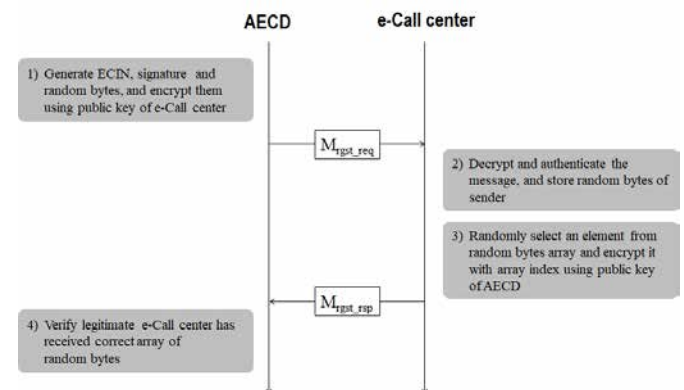


Figure 8. Key seeds sharing mechanism overview

DIN = Device Identification Number	H	Hash function
VIN = Vehicle Identification Number	PRNG	Pseudo random number generator
CBN = Call Back Number	HMAC	HMAC function
ECIN = E-Call Identification Number	E_{asym}	Asymmetric encryption
PR_C = Private key of client (AECD)	D_{asym}	Asymmetric decryption
PR_S = Private key of server (e-Call center)	E_{sym}	symmetric encryption
PU_S = Public key of server (e-Call center)	D_{sym}	symmetric decryption
$S_C(x)$ = Client(AECD)'s signature for x		

Figure 9. List of abbreviations and symbols

1) [AECD] generates ECIN, signature and random bytes and encrypts them using public key of e-Call center : First of all, ECIN is generated using device identification number, vehicle identification number and call back number. ECIN can be thought of as an identifier for AECD. A signature value of ECIN is generated by encrypting with PR_C . This signature value will guarantee that the message is transmitted by legitimate AECD device. A 2-dimensional random number array (R_{array}) is also created using cryptographically secure pseudo random number generator (PRNG). After all, ECIN, signature of ECIN and R_{array} are encrypted with PU_S and sent to e-Call center. Using PU_S for encryption guarantees that only the node that holding the PR_S corresponding to the PU_S can decrypt the received message.

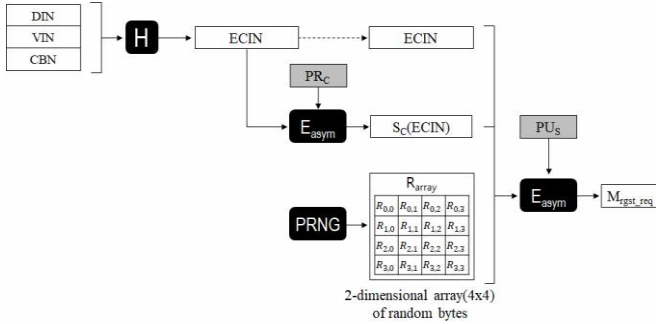


Figure 10. Key seeds sharing mechanism – 1)

2) [e-Call center] decrypts and authenticates the message, and store random bytes of sender : The e-Call center decrypts the received message M_{rgst_req} with PR_S . Then signature of ECIN, one of the data decrypted from received message, is checked using PU_C . If this signature is verified to be valid, decrypted ECIN and R_{array} are paired and stored in keystore directory.

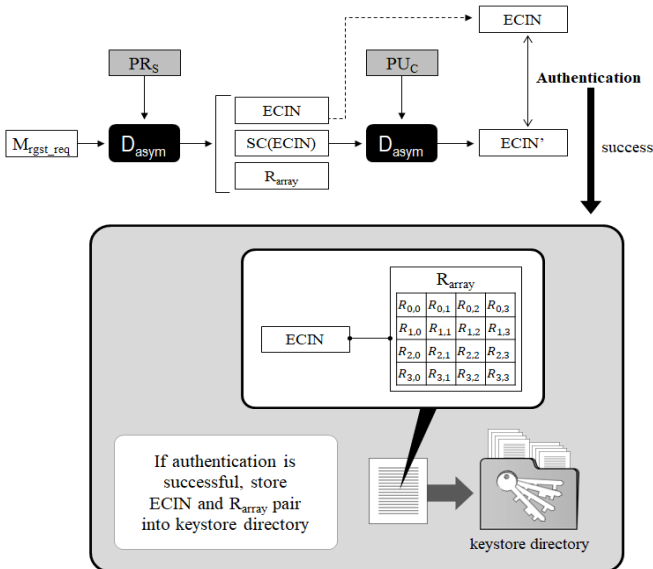


Figure 11. Key seeds sharing mechanism – 2)

3) [e-Call center] Randomly selects an element from random bytes array and encrypts it with array index using public key of AECD : As an acknowledgement, an $R_{x,y}$ is randomly selected from R_{array} and sent to AECD with index values. These are encrypted with PU_C before transmitted to AECD.

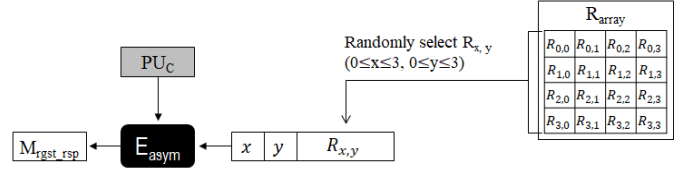


Figure 12. Key seeds sharing mechanism – 3)

4) [AECD] verifies that legitimate e-Call center has received correct array of random bytes : AECD decrypts received message with PR_C and check that the element in the x^{th} row and y^{th} column of the random number array matches the received $R_{x,y}$.

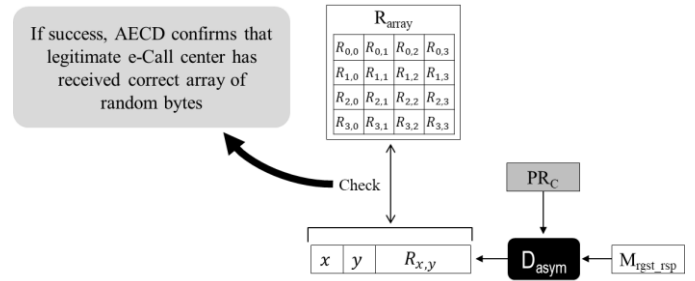


Figure 13. Key seeds sharing mechanism – 4)

B. Secure MSD transmission mechanism

The secured MSD is transmitted from AECD to e-Call center without handshake process, to reduce delay.

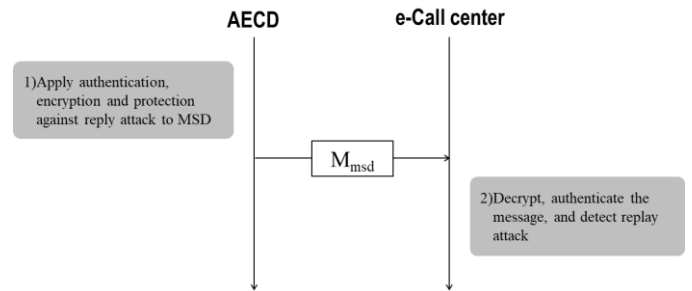


Figure 14. Secure MSD transmission mechanism overview

1) [AECD] applies authentication, encryption and protection against reply attack to MSD : Selecting one element per row in R_{array} arbitrarily and hashing them, encryption key K_{enc} and HMAC key K_{hmac} are generated. These key generation processes can be completed in advance. In this case, M_{msd} can be created omitting the key generation process at the time of accident. M_{enc} is generated by encrypting MSD and timestamp with K_{enc} , and M_{hmac} is a

HMAC of ECIN + MSD + Timestamp, in which the HMAC key is K_{hmac} . The format of M_{msd} is as follows :

- ECIN|j|k|m|n|M_{enc}|M_{hmac}

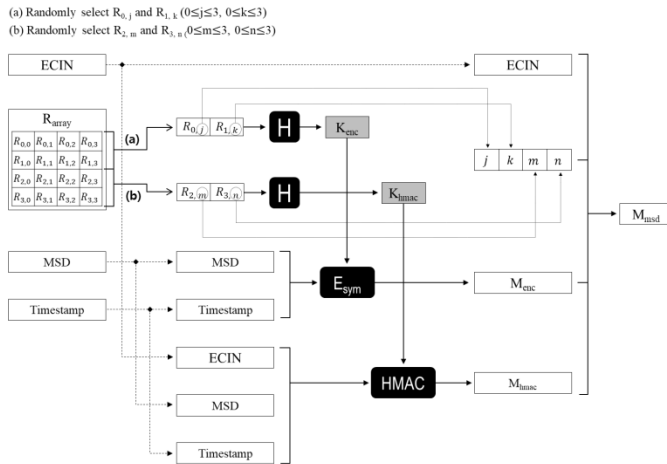


Figure 15. Secure MSD transmission mechanism – 1)

2) [e-Call center] decrypts, authenticates the message, and detects replay attack : The e-call center can find the keystore file that contains the a random number array of sender, using the ECIN included in the received message. K_{enc} and K_{hmac} are derived from the array and index values in M_{msdc} message, using hash function. MSD and timestamp are decrypted with K_{enc} , and the timestamp is used for detecting redirection attack by comparing it with current timestamp. MSD and timestamp decrypted, ECIN value and K_{hmac} are used for message authentication. If HMAC of them (M'_{hmac}) and received HMAC (M_{hmac}) are the same, message authentication succeeds.

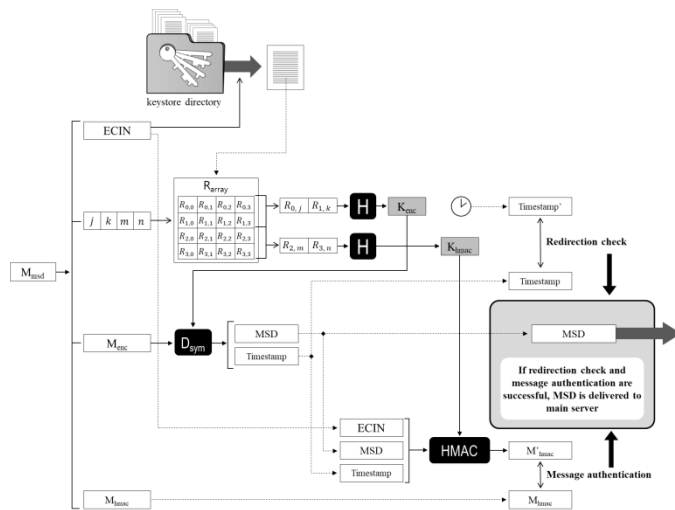


Figure 16. Secure MSD transmission mechanism – 2)

V. CONCLUSION

This proposes an efficient MSD protection and authentication scheme for automotive ICT based emergency call system. In this protocol, cryptographic security

parameters are negotiated through key seeds sharing protocol, which is activated at the time that is not related to MSD transmission, as a distinct process, once at fixed period. Therefore, when AECD detects an accident, MSD can be sent without additional preliminary handshake. If R_{array} is $2n \times 2n$ array, $2n^n$ different encryption keys and $2n^n$ different HMAC keys can be generated. Thus if you want to increase the key seeds sharing period, you can increase n value of $2n \times 2n R_{array}$. In the future, security analysis and comparative analysis of proposed scheme will be given.

ACKNOWLEDGMENT

This work was partly supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIT) (No.R0113-15-0002, Automotive ICT based e-Call standardization and after-market device development) and MIST(Ministry of Science and ICT), Korea, under the National Program for Excellence in SW supervised by the IITP(Institute for Information & communications Technology Promotion) (No.2015-0-00914).

REFERENCES

- [1] HeERO website. [Online]. Available: <http://www.heero-pilot.eu/view/en/ecall.html>
- [2] M. Niculescu, F. Ropot and M. Minea "Analysis of the Requirements for the Communication Link used in the Transmission of e-CALL Messages," in 16th Conference on Automatic Control, Modelling and Simulation ACMOS'14, Brasov, Romania, 2014.



Nam-Uk Kim is currently a Ph.D. student at Sungkyunkwan University, Suwon, Korea. He received his B.E. and M.E. degrees in Computer engineering from Sungkyunkwan University in 2009 and 2012, respectively.



Tai-Myoung Chung is a professor at the Department of Software, Sungkyunkwan University, Suwon, Korea. He received his M.E. in computer engineering from University of Illinois Chicago and his Ph.D. from Purdue University. His research interests are in information security, network, information management, and protocols of the next-generation networks such as active networks, grid networks, and mobile network.