논문 2011-48TC-4-13

u-TSN에서의 안전한 차량 통신 시스템 구현

(Implementation of Secure Vehicular Communication System in u-TSN)

박 요 한*, 박 영 호**, 문 상 재***

(Yohan Park, Youngho Park, and Sangjae Moon)

요 약

u-TSN은 운전자들과 보행자들을 위하여 도로 안전과 교통 관리를 용이하게 하는 차세대 기술이다. u-TSN을 실제 환경에 사용하기 위해서는 개인의 정보와 통신상의 데이터를 위부 공격자로부터 안전하게 보호해야 한다. 상대적으로 무능한 공격자라도 u-TSN이 가질 수 있는 장점들을 방해하고 사용 불가능하게 만들 수 있다. 따라서 안전한 u-TSN을 구현하기 위해서는 악의적인 공격자의 공격들은 방어하는 것이 중요한 과제 중의 하나이다. 본 논문에서는 u-TSN 환경에서의 보안 시나리오를 소개하고 이를 IXP425 보드에 구현한다. 보안 모듈로 구현된 보안 시스템은 u-TSN 환경에서 안전하고 효율적인 통신을 제공한다.

Abstract

u-TSN is a promising technology facilitating road safety and traffic management for drivers and passengers. To deploy this technology in a real environment, personal information and communicated data should be protected against malicious adversaries. Even though such adversaries would appear relatively infrequently, in such cases, the benefits of u-TSN could be disrupted and disabled. Therefore, one of the ultimate goals in the design of secure u-TSN is to protect against attacks of malicious adversaries. In this paper, we present secure communication scenario for u-TSN and implement security protocols and algorithms that are the components of the scenario on an IXP425 board. The security systems, implemented as a security module, supports secure and efficient communication for the u-TSN.

Keywords : u-TSN, registration authentication, ECIES, AES-CCM, handover authentication

Ⅰ. Introduction

The concept of ITS (intelligent transportation system) has been actively researched, locally and abroad. CALM (communications access for land mobiles) and WAVE (wireless access in vehicular environment) are under study for use in vehicle communication[1].

Recently, studies of u-TSN (ubiquitous-transportation sensor network), a promising technology to facilitate road safety and traffic management for drivers and passengers, have been making progress locally. u-TSN can provide traffic flow control, vehicle safety control, and infotainment service[2]. For example, u-TSN helps to find facilities such as restaurants and gas stations, and broadcasts traffic-related messages about car accident and congestion[3~5]. Such information can help for drivers with knowledge of what is going on in their driving environment and allow them to take action to

* 정회원, *** 평생회원, 경북대학교 전자공학부
(Kyungpook National University)
** 정회원-교신저자, 경북대학교 산업전자전기공학부
(Kyungpook National University)
접수일자: 2010년12월20일, 수정완료일: 2011년4월14일

respond to abnormal situations early. We can have obtain the many advantages of safe, convenient and efficient driving when u-TSN is applied to our lives.

Despite these advantages, there are many challenges inherent in such systems from the aspects of security and privacy[6~7]. u-TSN inherits many of the known and unknown security weaknesses associated with wireless mobile networks, and could be subject to many security and privacy threats. Erroneous information occurring due to message modification and replay attack[8~9] with respect to the disseminated messages could cause traffic congestion and severe accident. Moreover, deceit can happen in toll collection systems and a driver's privacy also could be threatened by location tracking attacks. Therefore, it is critical to develop a suite of elaborate and carefully designed security mechanisms to achieve security and conditional privacy preservation.

In this paper, we present a secure communication scenario for u-TSN on the basis of IEEE Std. 1609.2. In addition, we study vehicle registration authentication protocol and Wang's handover authentication protocol. Then, we implement security protocols and algorithms on an IXP 425 board and test the system on the roads. The results show that communication in V2V (vehicle to vehicle) or V2I (vehicle to infrastructure) is protected against malicious adversaries. And the computational time of the implemented algorithms is permissible in a VANET environment. The rest of the paper is organized as follows. In Section Ⅱ, we present a secure communication scenario for u-TSN. Next we identify security protocols and algorithms in Section Ⅲ, followed by an implementation of security systems in Section Ⅳ. Finally, the paper is concluded in Section Ⅴ.

Ⅱ. Secure Communication Scenario for u-TSN

Various security technologies are needed for each stage of the process of applying u-TSN in real

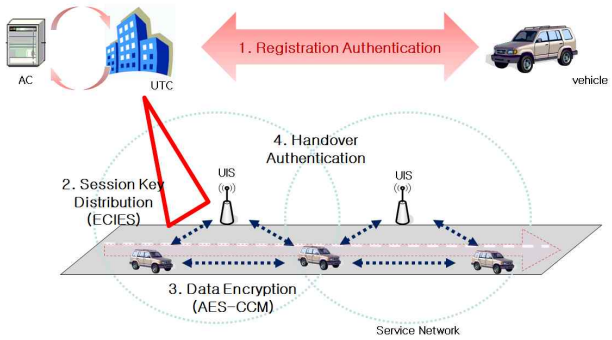


그림 1. u-TSN에서의 안전한 통신 시나리오
Fig. 1. Secure communication scenario in u-TSN.

environment. To provide secure communication u-TSN is considered to have several steps; authentication service, session key distribution, data encryption, and handover. Therefore, we have to design a secure communication scenario with care in order to provide security. The scenario is as follows.

First, vehicles register with a UTC (ubiquitous transportation center) with a registration authentication protocol. Then, vehicles receive the initial session key encrypted by the ECIES algorithm from the UTC. Vehicles can invoke V2V or V2I communication using the AES-CCM algorithm and this session key. The session key is updated by handover authentication protocol when vehicles move and change the UIS. This secure communication protocol is shown in Figure 1.

It is a big computational burden for the network to generate and distribute a session key using the ECIES algorithm for every new session (a session is defined as the communication between the vehicle and the UIS). To reduce the computational burden, we apply the handover authentication protocol. The handover authentication protocol can update the session key when vehicles contact a new UIS by moving to another service network. Thus, only one generation of a session key is sufficient for the new session. Therefore, we generate the initial session key using the ECIES algorithm and encrypt messages using the AES-CCM algorithm. Then, we update the session key efficiently using the handover authentication protocol.

Ⅲ. Security Protocols and Algorithms for u-TSN

In this section, we suggest components of each security system related to the security scenario proposed in the previous section.

1. Registration Authentication

The registration authentication is an essential requirement to support secure communication between vehicles and the UIS. We propose the following registration authentication protocol. This protocol provides authentication between the vehicle and the authentication center (AC), which is connected to the UTC. We assume that the v_i=$H[K_i]$ is shared in advance between the vehicle and the AC. The notation to be used in the registration authentication protocol is listed in Table 1.

The vehicle in u-TSN sends a request, VID and ti, to the UIS. The UIS receives this message and sends it to the UTC with $USIN$. The UTC sends VID and t_i to AC, and then checks the location of the vehicle, which sends the request using $UISN$ and decides to have the UIS reply. The AC computes N_i and $AUTH_C$ (1) using the session key generated in the AC and the data received from the UTC. The vehicle can receive the session key KS securely because N_i is computed as vi and timestamp t_i. Then AC sends N_i, RN and $AUTH_C$ to the UTC.

$$N_i = H[v_i \oplus t_i] \oplus K_S$$
$$AUTH_C = H_{K_S}[RN \| VID_i] \quad (1)$$

UTC stores $AUTH_C$ and forwards N_i and RN to the vehicle through the UIS located in the service area around the vehicle. The vehicle computes the session key KS and $AUTH_i$ (2), and then sends $AUTH_i$ to the UTC through the UIS. The UTC verifies that $AUTH_C$ and $AUTH_i$ are the same. Then UTC only registers the vehicle in the case of correct verification.

표 1. 기호들.
Table 1. Notations.

t_i	timestamp
RN	random number
VID_i	identity of vehicle i
$UISN$	identification number of UIS
K_i	private key of vehicle i
K_S	session key

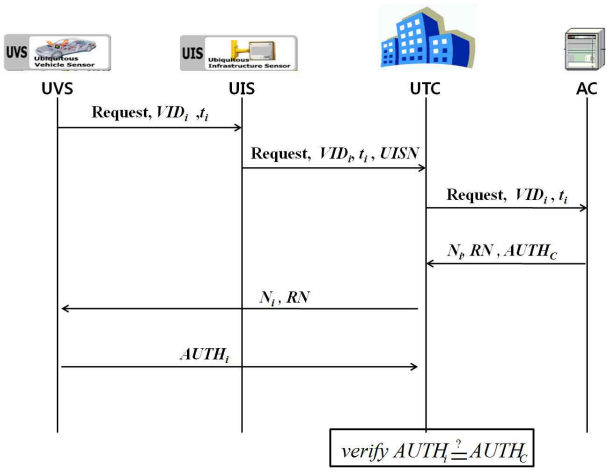


그림 2. u-TSN에서의 등록 인증 프로토콜
Fig. 2. Registration authentication protocol in u-TSN.

$$N_i \oplus H[v_i \oplus t_i] = K_S$$
$$AUTH_i = H_{K_S}[RN \| VID_i] \quad (2)$$

This protocol is secure because the session key is made up of the shared value vi, so the adversary cannot generate $AUTH_i$, and finally fails in the registration authentication. Figure 2, below, illustrates the protocol specifically.

2. Session key Distribution

In each session, UTC generates new session keys and forwards them to vehicles in the u-TSN. IEEE Std 1602.2 recommends ECIES (elliptic curve integrated encryption scheme) to perform session key encryption process securely. ECIES is a public key cryptosystem based on elliptic curve[9]. The strong point of ECIES compared to conventional public key cryptosystem is that it provides a similar security level even though it uses a short key. This advantage is suitable for a wireless mobile environment that suffers from insufficient

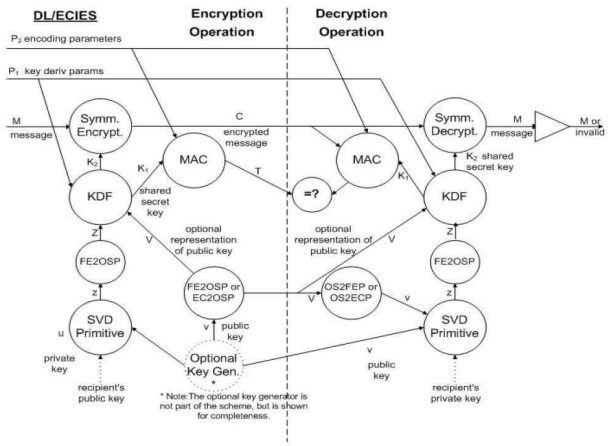


그림 3. ECIES 암호/복호 과정
Fig. 3. ECIES encryption/decryption process.

computation and transmission ability. IEEE Std 1363a-2004 shows the encryption and decryption processes as follow[10].

The encrypted messages consist of (V,C,T). V is the public key of the sender, used to encrypt the session key, C is the encrypted value of the private key using V, and T indicates the message authentication code. In Figure 3, the key that is used for deriving the key for the private key decryption and for generating the MAC authentication is generated using V and the KDF (key derivation function). The encrypted private key C and the T generated by MAC are sent to the receiver. The receiver, which generates keys for private key decryption and to prove that MAC is using KDF with shared information, finally performs the private key decryption and the MAC authentication.

3. Data Encryption/Decryption

IEEE Std 1609.2 recommends a standard data encryption algorithm, AES-CCM, for data encryption in ITS. AES-CCM is one of the AES algorithms using CCM (counter with CBC-MAC)[9]. AES, published by NIST in 2001, is the most common method to use the block encryption algorithm[11]. CCM is a combination of counter and CBC-MAC. Counter is normally used to verify the integrity of a message by generating the MAC of the message[12].

In the AES-CCM mode, the sender and the receiver perform encryption and decryption sequentially, as shown in Figure 4.

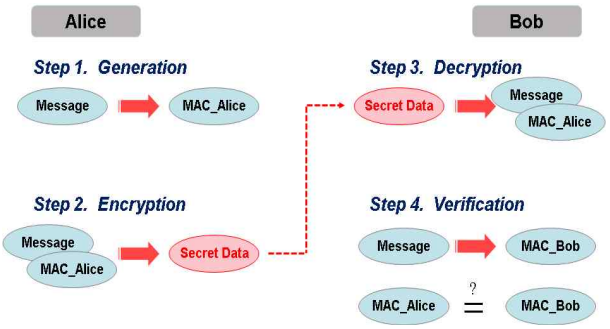


그림 4. AES-CCM 암호/복호 과정
Fig. 4. AES-CCM encryption/decryption process.

Sender

- Generation: This is for generation of MAC, and is done to support data integrity. Sender generates MAC about some or whole outputs of the message used by CBC.
- Encryption: This is for encryption of MAC using counter mode.

Sender sends encryption data and MAC to receiver after these executions.

Receiver

- Decryption: This is for decryption of transmitted data using counter mode. Receiver can know the data and MAC if he successfully decrypts the data.
- Verification: This is for integrity check, to see whether there are errors or modifications. Receiver can check the integrity of the data by generating MAC with CBC. If the MAC generated by receiver is same as the MAC generated by the sender, the receiver verifies that there are no errors or modifications.

4. Handover Authentication

Handover authentication means UVS authentication and session key generation between UVS and UIS when the mobile node UVS moves to another service network from an existing service network.

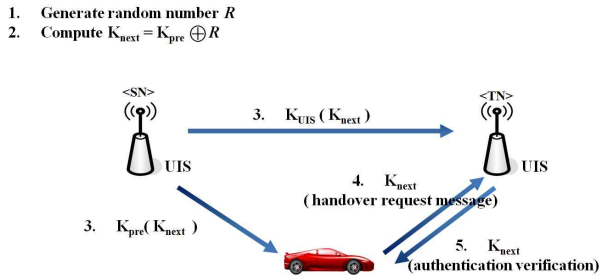


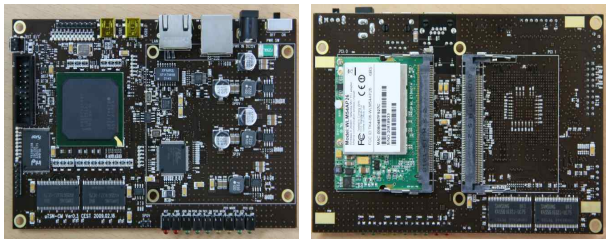
그림 5. 핸드오버 인증 프로토콜
Fig. 5. Handover authentication protocol.

Handover authentication technologies can be divided into two parts according to the existence of the AAA (authentication, authorization, and accounting) server. AAA-based authentication generally provides a high level of security, but it can cause authentication request message delay due to the frequent communication between the AAA server and the UVS. On the other hand, non-AAA-based authentication has advantages in efficiency because only UIS and UVS interact for handover authentication. Among non-AAA-based authentication technologies, Wang's method[13] and Kempf's method [14] are popular. In our u-TSN scenario, we use Wang's method because it provides lightweight computation by using XOR computation.

Figure 5 gives details of handover authentication technology proposed by Wang. When UIS in SN (service network) detects the variation of UVS, it generates a random number R and performs an XOR operation between R and the existing session key K_{pre} to forward the session key from SN to TN. And then UIS in SN sends K_{next} to the UIS in TN through the secure channel. Also UVS receives K_{next}, which is encrypted by the shared session key. When the UVS moves to TN, it sends a handover request message encrypted by K_{next} to UIS in TN. The UIS in TN can authenticate the UVS by verifying the message using K_{next}.

Ⅳ. Implementation

In this section, we show the implemented module



(a) front side (b) reverse side

그림 6. 보안 모듈
Fig. 6. Security module.

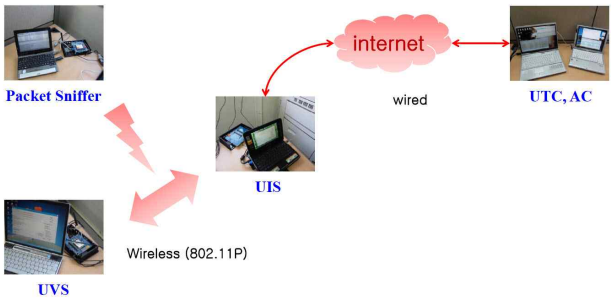


그림 7. u-TSN에서의 보안 구조 구현
Fig. 7. Implemented security architecture in u-TSN.

and the simulation that we performed. The algorithms, ECIES and AES-CCM, which encrypt the session key and messages are implemented on an IXP425 board. Figure 6 shows the security-implemented module. The implemented module can be equipped to both vehicles and UIS.

We equipped two vehicles with the security module and tested it on the roads. And we installed four UIS on lamp posts that are connected to the UTC. Figure 7 shows the implemented security architecture for the u-TSN. The packet sniffer can identify the validity of the data transmitted between UVS and UIS. According to the system setting, the packet sniffer

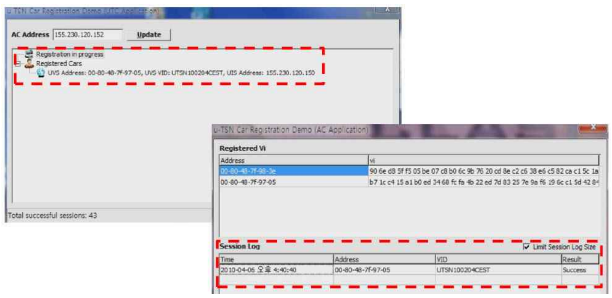


그림 8. UTC와 차량 사이의 차량 인증 과정
Fig. 8. Vehicle registration between UTC and vehicle.

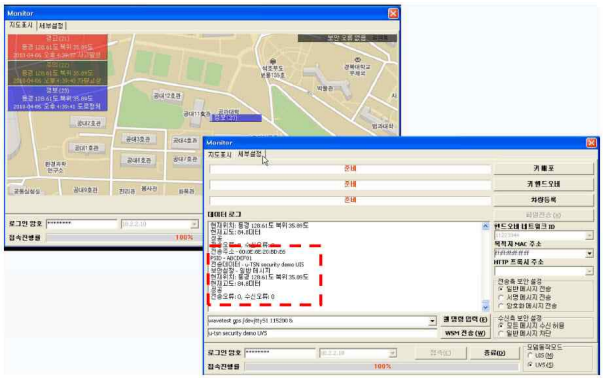


그림 9. 메시지 전송 (경고, 주의, 정보, 텍스트)
Fig. 9. Message transmission.
(warning, caution, notice, text).

표 2. 연산 시간
Table 2. Computation time.

Processor Information	Algorithms	Computation Time
CPU : Network Processor IXP 425 (533MHz) RAM : SDRAM 128MB	ECIES	10ms
	AES-CCM	80us

identifies the message when sending of the message is unencrypted. But when the message is encrypted, the packet sniffer cannot recognize the message as valid or not.

Figure 8 shows the process of vehicle registration when UVS connects UTC through UIS for the registration process.

Figure 9 shows message transmission between UVS and UIS. The messages are warning, caution, notice and text.

We checked the computation time. We assumed that the session key length be 160bit. The computation time of the AES-CCM algorithm varies depend on the data length because the process uses 128-bit block encryption. It takes 80 to operate one block (128bit). The ECIES algorithm uses a WTLS #7(secp170r2) elliptic curve[15] and takes 10ms. Table 2 gives the details of the operation results.

We make sure that it is possible to operate this system as a real time data process. As we have seen above, AES-CCM and ECIES are suitable algorithm for real-time communication in u-TSN.

V. Conclusions

The u-TSN is the newest network technology that can automatically set up a network and communicate between vehicles or vehicle and infrastructure. But the security problems are not yet clearly solved. Therefore, it is necessary to construct a secure scenario essentially in u-TSN such that new member registration and data encryption can provide confidential and reliable service.

In this paper, we presented a secure communication scenario for u-TSN. On the basis of IEEE Std. 1609.2, ECIES and AES-CCM were used to encrypt session keys and data. In addition, we studied a vehicle registration authentication protocol and adopted Wang's handover authentication protocol. Based on this scenario, we implemented a security module on an IXP 425 board and tested the system on the road. The whole system supports security for V2V or V2I communication and the computational time of the implemented algorithms is permissible in VANET.

References

[1] IEEE Trial-use Standard for Wireless Access in Vehicular Environments (WAVE) - Networking Services, 2007.
[2] J. K. Bae, and D. S. Han, "Packet Transmissin Scheme for Collecting Traffic Information based on Vehicle Speed in u-TSN System," Journal of IEEK, vol.47, no.6, 2010.
[3] X. Lin, R. Lu, C. Zhang, H. Zhu, P. H. Ho, and X. Shen, "Security in Vehicular Ad Hoc Networks," IEEE Communications Magazine, April, pp. 88-95, 2008.
[4] M. Raya, P. Papadimitratos, and J. P. Hubaux, "Securing Vehicular Communications," IEEE Wireless Communications Magazine, Oct., pp. 8-15, 2006.
[5] Hannes Hartenstein, and Kenneth P. Laberteaux, "A Tutorial Survey on Vehicular Ad Hoc

Networks," IEEE Communication Magazine, June, pp.164-171, 2008.
[6] A. Aijaz, B. Bochow, F. D¨otzer, A. Festag, M. Gerlach, R. Kroh, and T. Leinm¨uller, "Attacks on Inter Vehicle Communication Systems and Analysis," The Network on Wheels Project, Tech. Rep., 2005.
[7] M. Gerlach, "Assessing and Improving Privacy in VANETs," in Proceedings of Fourth Workshop on Embedded Security in Cars (ESCAR), November, 2006.
[8] U.S. Dept. of Transportation, "National Highway Traffic Safety Administration, Vehicle Safety Communications Project," April, 2006
[9] IEEE Std. 1609.2-2006, IEEE Trial-Use Standard for Wireless Access in Vehicular Environments-Security Services for Applications and Management Messages, 2006.
[10] IEEE Std. 1363a, IEEE Standard Specification for Public-Key Cryptography-Amendment 1 : Additional Techniques, 2004.
[11] NIST, Announcing the advanced Encryption Standard (AES), FIPS PUB197, 2001.
[12] NIST, Recommendation for Block Cipher Modes of Operation, NIST Special Publication 800-38A, 2001.
[13] H. Wang and A. R. Prasad, "Fast Authentication for Inter-domain Handover," International Conference on Telecommunications 2004, August, pp.973-982, Springer-Verlag, 2004.
[14] J. Kempf and R. Koodli, Distributing a symmetric FMIPv6 Handover Key using SEND, IETF draft-ietf-mipshop-handover-key-03, Nov., 2007.
[15] Certicom Research, SEC2: Recommended Elliptic Curve Domain Parameters, Standard For Efficient Cryptography, 2000.

저 자 소 개

박 요 한(정회원)
2006년 경북대학교 전자전기 컴퓨터학부 학사
2008년 경북대학교 전자공학과 석사
2008년～현재 경북대학교 전자공학부 박사과정
<주관심분야 : 무선통신, 네트워크 보안, 모바일 컴퓨팅>

문 상 재(평생회원)
1972년 서울대학교 전자공학과 학사
1974년 서울대학교 전자공학과 석사
1984년 미국 UCLA 전자공학과 박사
1984년～1985년 미국 OMNET 회사 컨설턴트
1984년～1985년 미국 UCLA 포스트닥터
2001년～2002년 한국정보보호학회회장
1974년～현재 경북대학교 전자공학부 교수
<주관심분야 : 무선통신, 네트워크 보안, 암호학>

박 영 호(정회원)-교신저자
1989년 경북대학교 전자공학과 학사
1991년 경북대학교 전자공학과 석사
1995년 경북대학교 전자공학과 박사
1996년～2008년 상주대학교 전자전기공학부 교수
2003년～2004년 Oregon State University 방문 교수
2008년～현재 경북대학교 산업전자전기공학부 교수
<주관심분야 : 무선통신, 네트워크 보안, 모바일 컴퓨팅>