VANET에서 보안성 향상을 위한 키 분배에 관한 연구

유도경* · 한승조**

A Study of Key Distribution for Security on VANET

Do Kyeong Too* · Seung-jo Han**

이 논문은 2012년도 조선대학교 교내 연구비를 지원받았음

요 약

VANET은 다수의 차량노드들이 무선통신 기술을 이용하여 차량노드간 통신 및 차량과 RSU 사이의 통신을 제공하는 네트워크 환경으로써, 사람의 안전과 생명을 보호 하는 중요한 역할을 한다. 때문에 보안은 충분히 고려되어야 하며, 차량간 교환되는 메시지는 인증이 매우 중요하다. 최근 Zhang등은 RAISE를 통해 VANET에서 메시지를 교환하는 방법으로 Diffie-Hellman 키 교환 프로토콜을 사용하는 제안하였으나 이는 여러 공격에 취약한 문제점이 있다. 본 논문에서는 ECDH 키 교환 프로토콜을 사용하여 대칭키를 수립하는 기법을 제안하고 비교분석을 통해 안전성과 키 생성과 교환에 걸리는 시간 단축을 확인한다.

ABSTRACT

VANET is a network environment which provides the communication between vehicles and between vehicle and RSU using wireless communication. VANET is very important to protect safety and life of people. Because of that, security is considered enough and certification is very important when messages exchanged between vehicles. Recently, Zhang proposed using Diffie-Hellman key exchange protocol that is method exchanging messages in VANET system through RAISE. But this is many problems on weakness from various attacks. In this paper, proposed the method that establish symmetric key using ECDH key exchange protocol and confirm safety and time spending that generate key and exchange through comparison.

키워드

VANET, RSU, 타원곡선 알고리즘, ECDH

Key word

VANET, RSU, Elliptic Curve Cryptography, ECDH

* 정회원 : 조선대학교 정보통신공학과(rcjlove@naver.com)
** 종신회원 : 조선대학교 정보통신공학과

접수일자 : 2012. 07. 27
심사완료일자 : 2012. 09. 07

Open Access http://dx.doi.org/10.6109/jkiice.2012.16.10.2192

Ⅰ. 서 론

최근 인터넷과 무선통신의 발달로 인해 사람이 사용하는 모든 장치에 IT를 접목시키려는 노력이 증가하고 있으며, 특히 차량에 IT기술을 접목 시키려는 노력이 가속화 되고 있다. 사람의 편의성 증진을 위한 다양한 서비스들이 차량에 적용되고, 향후에는 차량의 지능화로 실현될 것으로 전망된다.

특히 ITS(지능형 교통 시스템, Intelligent Transportation System)에서 최근 가장 떠오르고 있는 기술은 무선 통신 시스템 및 원격 센싱 기술로써, 최근들어 다양하고 복잡한 컴퓨팅 시스템 및 센서들이 차량에 장착되어 자신의 정보를 수집함은 물론 무선 통신 시스템을 통하여 근접 차량 간에 실시간으로 정보를 교환 할 수 있게 되었다.

이러한 서비스는 C2E(Car to Enterprise), C2C(Car to Car), C2H(Car to Home)에서 이루어지며, 그 종류 역시 다양하다. 그중 VANET (Vehicular Ad-hoc Network)은 차량과 차량사이 또는 차량과 RSU(도로 노변장치, Road Side Unit)사이의 통신을 위한 네트워크로써, 다수의 차량, RSU, CA(Certificate Authority)로 구성되어 있다.[1-3]

VANET의 통신 방법은 크게 V2V(Vehicle to Vehicle)와 V2I(Vehicle to Infrastructure)로 분류 할 수 있으며, 인프라 통신이란 RSU와 통신하여 기존 인프라 네트워크로부터 정보를 수집하는 것이다. V2V 환경은 이동 애드혹(Mobile Ad-hoc) 네트워크 구조이고, V2I는 RSU를 거쳐 기존 인프라 구조에 액세스 할 수 있는 구조이다. V2V를 이용할 경우 운전자는 시간에 따라 변하는 도로 방향 변화, 응급 정지, 차량에 따른 위험 상황 등의 정보를 실시간으로 보고 받게 되며, RSU로부터 차량 혼잡 상황 및 위험을 보고 받을 수 있다[1].

Zhang등이 제안한 VANET에서의 RAISE는 차량과 RSU간의 통신이 이루어지는 과정 이전의 키분배 프로토콜로 DH 키교환 프로토콜을 사용한다. 이는 스푸핑 및 재생공격에 취약한 단점이 있으므로 본 논문에서는 보안성을 향상시키기 위해 타원곡선 알고리즘(ECC, Elliptic Curve Cryptography)을 사용하여 차량과 RSU 사이에 보안성이 강화된 키 교환 프로토콜을 설계하고, 메시지 전송 과정을 설명한다[2].

2장에서는 VANET 환경과, Zhang 등이 제안한 연구 방법인 RAISE에 대해서 설명하고 3장에서는 새로운 제안 방법에 대해 설명한다. 4장과 5장은 제안한 방식의 보안성 분석 및 결론으로 구성한다.

Ⅱ. 본 론

2.1. VANET

VANET은 MANET의 형태로 V2V통신 및 V2I통신을 제공하는 네트워크를 말하며 [그림 1]과 같다. 이는 사람의 생명과 관련된 중요한 정보들이 전송된다는 특징이 있으며, 차량간의 충돌회피, 주행간의 장애물 경고등과 같은 운전자의 안전에 대한 기술과 더불어 운전자의 편의를 위한 다양한 멀티미디어 서비스와, 정확한 정보를 전달하는 통합적인 기술 중심으로 발전하고 있다[2].

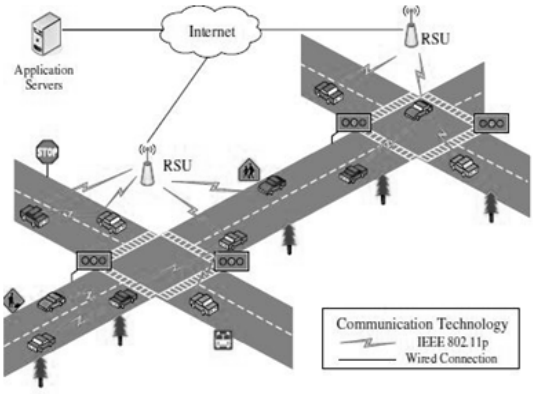

그림 1. VANET 환경
Fig. 1 VANET environment

하지만 무선을 통해 이러한 중요 정보들이 전송된다는 점에서 VANET의 보안과 프라이버시 문제가 제기되고 있으며, 특히 DoS공격, 재생 공격, 통신방해, 위조 공격, 도청공격, ID 노출 공격 및 차량 추적 등의 여러 가지 위험에 노출되어 있다. 따라서 성공적인 VANET 환경을 유지하기 위해서는 보안 문제점들의 해결이 시급하다[3].

2.2. Zhang의 RAISE 제안방식

최근 Zhang 등은 VANET에서 차량의 익명성 보호와 인증 및 조건부 프라이버시를 제공하기 위해 RSU와 각각의 차량이 통신하는 환경 속에서 k개의 차량에 동일한 ID를 부여하는 K-익명성(K-anonymity) 방식을 이용하였으며, 대칭키 수립, 해시 결집, 검증 3단계로 구성된 RAISE를 제안하였다[4-5].

2.2.1. Symmetric Key Establishment

RSU는 차량과 통신을 위해 Diffie-Hellman 키 교환 프로토콜을 사용하여 대칭키를 수립하게 된다.

$$V_i \rightarrow R:\ g^a, \{g^a\}_{SK_{V_i}}, C_{V_i}$$
$$R \rightarrow V_i:\ ID_i \| g^b, \{ID_i \| g^a \| g^b\}_{SK_R}, C_R$$
$$V_i \rightarrow R:\ \{g^b\}_{SK_{V_i}}$$

이때 RSU와 차량 V_i 사이에 생성된 대칭 키 K_i는 Diffie-Hellman 키 교환 프로토콜의 요소인 g^a와 g^b에 의해 생성된 g^{ab}이며, V_i의 첫 번째 메시지로부터 RSU는 차량의 공개키인 PK_{vi}를 확인 할 수 있다. $\{g^a\}SK_{vi}$는 g^a의 전자서명이 된다.

RSU와 차량사이에는 대칭키가 수립된 상태이며 익명의 ID를 받게되고, 이때 RSU는 각 차량에 할당된 ID_i와 대칭키 K_i, 인증서 C_i, 시간정보 T_i를 저장한 테이블을 갖고 있다.

2.2.2. Hash Aggregation

RSU는 각 차량으로부터 전송받은 메시지를 HMAC 알고리즘을 통해 인증하며, 이렇게 확인된 메시지를 해시 함수를 통해 결집한 후 각 차량으로 전송되게 되며, 결집된 메시지는 다음과 같은 구조를 갖는다.

$$H = H(ID\|M_1)\|H(ID\|M_2)\|\cdots\|H(ID\|M_n)$$

그리고 전자서명을 하여 $H_{Aggt}\|\{H_{Aggt}\}_{SK_R}$를 전송하게 된다.

2.2.3. Verification

다른 차량들로부터 받은 메시지의 Mi와 IDi를 통해 $H(ID\|M_i)$를 계산하게 되고, 계산된 값이 RSU로부터 전송되어진 $H_{Aggt}\|\{H_{Aggt}\}_{SK_R}$ 을 서명된 값에 포함되었는지를 확인 하여 다른 차량으로부터 받은 메시지를 인증 할 수 있다.

2.3. 타원곡선 알고리즘

타원곡선 알고리즘은 유한체 상의 타원곡선 점들 간의 연산에서 정의되는 이산대수 문제의 어려움을 이용한 것으로 다음과 같은 수식을 사용한다.

$$y^2 = x^3 + ax + b (\mathrm{mod} P) \quad (1)$$

즉 위의 식을 만족하려면, $x^3 + ax + b$가 중근을 갖지 않을 때, $4a^3 + 27b^2 \neq 0$인 경우에만 암호화 알고리즘의 수식으로 사용할 수 있다.(단 P는 소수)

타원곡선 알고리즘에서의 안전도는 키 길이의 증가에 따라 거의 지수 함수적으로 증가함으로 RSA나 ElGamal, Diffie-Hellman 등과 같은 기존의 공개키 암호 시스템에 비해 장기적으로 기술의 발전에 따른 키 길이의 증가 비율 면에서도 대단한 장점을 가지고 있다[6-7].

Ⅲ. 제안하는 프로토콜

2장에서 기술한 RAISE 방식은 중간자 공격에 취약하고, 재전송 공격에 의해 공격당할 우려가 있어 보안상의 문제점이 발생하며, 키 생성과 키 교환 시간이 많이 걸리는 단점이 있다.

본 논문에서는 유한체 내에서 이산대수 문제보다 훨씬 더 어렵다고 알려진 타원곡선 알고리즘을 사용하여, 보안성이 강화된 키 교환 프로토콜을 수립한다. 타원곡선을 사용하면 모든 사용자가 같은 지저체 K를 사용한다 해도 각 사용자가 다른 곡선 E를 선택할 수 있다는 것으로, 사용자는 체 연산을 수행하기 위해 같은 하드웨어를 사용할 수 있으며, 추가적인 보안을 위해 주기적으로 곡선 E를 바꿀 수 있다. 본 장에서는 제안하는 방식의 대칭 키 수립 과정을 설명한다.

3.1. ECDH(Elliptic Curve Diffie-Hellman)

ECDH 알고리즘은 타원곡선 암호 알고리즘에서 사용하는 방법으로 송신단과 수신단간의 통신을 통해 비밀키를 생성하게 되며, 유한체 위의 Diffie-Hellman 알고리즘을 유한체 내의 타원곡선 위에서 적용한 것으로, Diffie-Hellman 알고리즘과 동작 방법이 유사하다. [그림 2]는 각 단의 개인키와 곡선상의 점 G를 통해 생성된 공개키를 교환하는 과정과, 비밀키를 생성하는 알고리즘 동작 방법을 나타낸다.

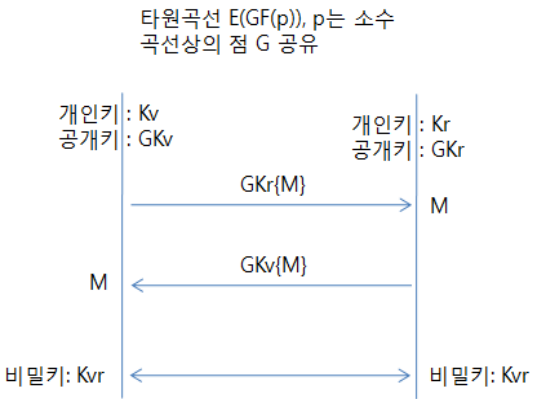

그림 2. ECDH 알고리즘 동작과정
Fig. 2 Operation of ECDH Algorithm

먼저 통신에 사용할 비밀키는 타원곡선 알고리즘을 통해 설립되게 되며, 개인키 K_v를 생성하게 되고, 공개키는 유한체 F상의 타원 곡선군 E(F)와 E(F)의 원소 중 큰 위수를 갖는 G를 정하게 된다. 이렇게 생성된 G와 송신측의 개인키 K_v를 곱해 송신측의 공개키 PU_v를 생성하게 되고 이를 수신측으로 전송한다.

수신측에서도 마찬가지로 수신측의 개인키 K_r을 생성하고 이를 G과 곱해 수신측의 공개키 PU_r을 송신측으로 보내게 된다. 이 과정을 통해 송신측과 수신측 간의 비밀키인 K_{vr}이 생성되게 된다.

$$K_{vr} = K_v \times PU_r = K_r \times PU_v$$

3.2. 차량과 RSU 사이의 키 관리와 ID 생성

RSU와 차량간의 통신을 위해 ECDH를 사용하여 대칭키를 수립한다.

용어의 표기법

표기법	설명
K_v	차량의 개인키
PU_v	차량의 공개키
K_r	RSU의 개인키
PU_r	RSU의 공개키
K_{vr}	차량과 RSU에 의해 생성된 비밀키
CM	전송되는 암호문
CU	U의 인증
{M}KU	M에 대한 U의 전자서명
R_k	난수

송신측에서 암호문을 전송할 때는 난수 R_k에 G를 곱한 값과, 보내고자 하는 메시지 M을 숨기기 위해 메시지 M에 난수 R_k와 송신측의 공개키를 곱한 값을 더하게 된다. 송신측에서 이를 복호화 할 때는 다음과 같은 방법을 사용한다.

$$M + R_k PU_r - K_r(R_k G)$$
$$M + R_k(K_r G) - K_r(R_k G) = M$$

제안하는 알고리즘은 암호문을 생성하는 과정에 있어서 전송하고자 하는 메시지 M을 바로 보내는 것이 아닌 메시지 M에 난수 R_k와 송신측의 공개키를 곱한 값을 더하는 과정을 통해 도청공격으로부터 안전하게 메시지를 전송 할 수 있다.

ID 생성은 Zhang등이 제안한 K-익명성 방식을 유지하기 위해 각 차량과 RSU 사이에 유일한 비밀키가 저장되어 있으며, 동일한 ID를 부여하게 된다. 차량은 RSU로 ID_i와 초기에 설정한 암호문 CM을 차량의 비밀키를 사용해 전자서명하고, 이를 인증하여 RSU로 전송하게 된다.

RSU는 차량으로부터 온 정보를 통해 CM안에 들어있는 정보인 난수 R_k와 ID_i, 차량과 RSU사이의 비밀키인 K_{vr}을 알게 되며 이를 다시 차량으로 보내게 되는데, 이 때는 RSU의 개인키로 전자서명하고, 이를 인증하여 차량으로 전송하게 된다.

마지막으로 차량은 RSU에게 K_{vr}을 전송하게 되고, RSU는 해당 차량에 대한 정보를 RSU 내부 테이블에 저장하게 된다.

Ⅳ. 비교분석

본 장에서는 제안된 방식을 중간자 공격, 조건부 프라이버시, 키생성 및 교환 측면에서 기존의 연구방법과 비교분석한다.

4.1. 중간자 공격(Man in the Middle Attack)

공격자는 차량과 RSU 사이에 전송되는 메시지를 도청하고 서명키를 계산하여 신분을 위장하려고 시도 할 수 있다. 특히 RAISE에서 제안한 DH 프로토콜은 공격자가 ga에 관한 정보와 서명키를 통해 중간자 공격을 시도 할 수 있다. 하지만 제안한 기법은 암호문 CM을 생성하는 과정에서 난수Rk와 RSU의 공개키 값을 곱한 값을 전송하고자 하는 메시지 M과 더한 값을 전송하기 때문에 공격자는 중간자 공격을 통해 획득한 정보를 통해 서명키를 생성 할 수 없으므로 중간자 공격에 안전하다.

4.2. 재전송 공격(Replay Attack)

공격자가 사용자의 메시지를 재전송 하여 이미 정상적인 사용자에 의해 생성된 이전키를 다시 생성하기 위해 사용하는 공격으로, DH 키 교환 프로토콜을 사용할 경우 재전송 공격을 시도할 수 있다. 하지만 제안한 기법은 난수 값 R_k 값과 RSU의 공개키인 PU_r 값을 계산한 후 이를 M과 더한 연산을 하였기 때문에 반복을 통해 이전 키의 생성은 불가능 하다. 따라서 제안하는 프로토콜은 재전송 공격으로부터 안전하다.

4.3. 조건부 프라이버시

본 논문에서는 RAISE 시스템에서와 같이 K-익명성을 만족하도록 차량과 RSU사이에 유일한 비밀키를 사용하였으며, RSU에는 내부 테이블에 모든 차량의 비밀키가 저장되어 있으므로 조건부 프라이버시를 만족한다.

4.4. 키생성 및 교환

차량노드의 수에 따라 결정되는 네트워크인 VANET 환경에서 안전한 키 관리 및 분배는 필수적인 부분이다. Zhang등이 제안한 RAISE 기법에서 사용하는 DH 알고리즘의 경우 사용되는 키의 길이는 1024~2048 bit인 반면, 본 논문에서 제안한 타원곡선 암호 알고리즘을 적용한 ECDH를 사용하면, 동일한 보안성을 고려했을 경우 192bit 만을 사용하여 키의 안전성을 확보 할 수 있으며, [그림 3]은 DH 알고리즘과 본 논문에서 제안한 프로토콜을 사용했을 때 키 생성에 걸리는 시간을 분석한 그림이고, [그림 4]는 DH 알고리즘과 제안한 프로토콜의 키 교환 시간을 분석한 그림이다. 이는 같은 안전도를 고려하여 1024bit의 DH 키교환과, 192bit의 제안하는 프로토콜의 시간을 분석한 결과로 0.086ms 차이가 나는 것을 확인할 수 있었다.

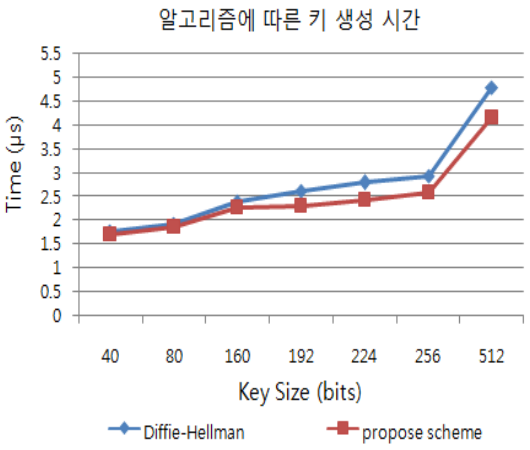

그림 3. 알고리즘에 따른 키 생성 시간
Fig. 3 Key generation time to algorithm

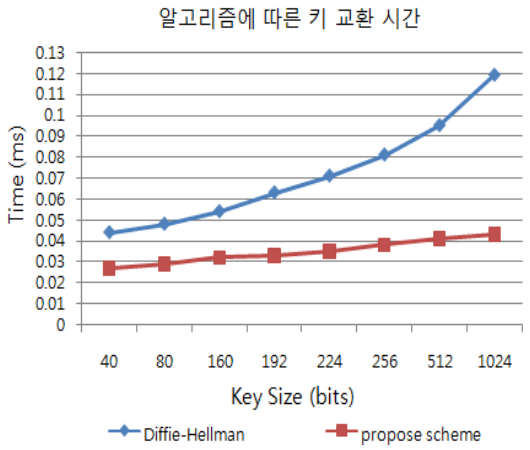

그림 4. 알고리즘에 따른 키 교환 시간
Fig. 4 Key exchange time to algorithm

표 1. RAISE 기법과 제안한 기법의 비교 분석
Table.1 Comparative analysis RAISE and new proposed scheme

구분	중간자 공격	재전송 공격	조건부 프라이버시	키관리
RAISE	×	×	○	△
제안 기법	○	○	○	○

○ : 안전, △ : 조건부 안전, × : 취약

V. 결 론

본 논문에서는 차량과 RSU간의 통신을 하기전인 대칭키 수립 과정에서의 보안성을 강화하기 위해 기존의 DH 키 교환 프로토콜 대신 유한체 상의 타원곡선 점들 간의 연산에서 정의되는 이산대수 문제의 어려움을 이용하여, 타원곡선 알고리즘을 적용한 ECDH 키 교환 프로토콜을 사용하였다.

새로운 제안 과정을 통해 중간자 공격과 재전송 공격으로부터 안전한 키 교환을 통해 대칭키를 수립 할 수 있으며, 조건부 프라이버시를 만족하는 것을 확인 할 수 있었다. 또한 비교분석을 통해 키 생성에 걸리는 시간이 단축되는 것을 확인 할 수 있었으며, 같은 안전성을 고려했을 때, 키 교환에 걸리는 시간이 단축되는 것을 확인할 수 있었다. 그 결과 기존의 RAISE 기법에서 제안한 키 교환 방식보다 작은 키의 길이를 통해 안전성을 확보 할 수 있었다.

사람의 목숨과 관련된 중요한 정보를 전송받는 VANET 환경에서 키 관리와 키 분배 문제는 필수적인 상황이다. 본 논문에서 제안한 키 교환 프로토콜을 통해 기존의 RAISE 방식보다 보안성이 강화 되었으며, 키 생성 및 교환시간을 단축시키는 효율적인 방식임을 확인하였다. 하지만 K-익명성을 만족하는 RAISE 방식에서 RSU와 통신하는 차량의 수가 많아질수록 RSU에서는 비밀키를 찾기 위해 RSU에 저장된 모든 키 값을 사용하여 HMAC을 계산하는 문제점이 발생한다.

향후에는 본 논문에서 제안한 기법을 만족하는 동시에 RSU에서 비밀키를 찾기 위해 모든 값을 사용하여 HMAC 하는 단점을 보완 할 수 있는 방법에 대해 연구할 계획이다.

참고문헌

[1] 조영준, 이현승, 박남제, 최두호, 원동호, 김승주, “VANET에서의 보안기술동향”, 정보보호학회지 19권 1호, 2009.02

[2] C. Zhang, X. Lin, R. Lu, and P.-H. Ho, “RAISE: an efficient RSU-adided message authentication scheme in vehicular communication networks,” in Proc. IEEE ICC 2008, 2008, pp. 1451-1457.

[3] S.Mohanty, D.Hena S.Panigrahy, ″A Secure RSU-Aided Aggregation and Batch - Verification Scheme for Vehicular Networks″ Intemational Conference on Soft Computing and its Applications(ICSCA2012), pp174-178

[4] S. Lee, G. Pan, J. Park, M. Gerla, and S. Lu, “Secure incentives for commercial ad dissemination in vehicular networks,” in Processings of the ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc’’07), Montreal, Canada, 2007.

[5] M. Scott, Implementing Cryptographic pairings. Pairing 2007, LCNS, Vol. 4575, pp. 177-196, Tokyo, Japan, July 2007.

[6] K. Sha, Y. Xi, W. Shi, L. Schwiebert, and T. Zhang, ″Adaptive Privacy-Preserving Authentication in Vehicular Networks,″ Proc. of the International Workshop on Vehicle Communication and Applications 2006, pp.1-8, Oct. 2006.

[7] SEC1 : Elliptic Curve Cryptography v1.0, SECG, September 20, 2000.

[8] SEC2: Recommended Elliptic Curve Cryptography Domain Parameters v1.0, SECG, September 20, 2000.

저자소개

유도경(Do Kyeong Yoo)

2008년 호남대학교 정보통신공학과(학사)
2010년 조선대학교 산업대학원 IT공학과 (공학석사)
2010년～현재 조선대학교정보통신공학과(박사수료)
※관심분야 : USN, 네트워크 보안

한승조(Seung-jo Han)

1980년 조선대학교 전자공학과 (학사)
1982년 조선대학교 전자공학과 (공학 석사)
1994년 충북대학교 전자계산학과 (공학 박사)
1986년 6월～1987년 3월 : 뉴올리언즈대학 객원교수
1995년 2월～1996년 1월 : 택사스대학 객원교수
2000년 12월～2002년 3월 : 버클리대학 객원교수
1998년 3월～현재 : 조선대학교 전자정보통신공학부 교수
※관심분야 : 통신보안시스템설계, S/W 불법복제방지 시스템, ASIC 설계