정형검증 도구인 Casper를 이용한 VANET 인증 프로토콜 분석

이수연* · 안효범**

요 약

VANET(Vehicular Ad-hoc Network)은 지능형 차량들로 이루어진 애드혹 네트워크 환경으로서 최근 들어 그 연구가 활발하게 진행되고 있는 분야이다. VANET은 원활한 교통 소통, 사고 방지 등 여러 가지 편리한 기능들을 제공하지만 그 기반을 애드혹 네트워크에 두고 있기 때문에 애드혹 망에서 발생하는 보안 문제를 가지고 있고 또한 그 환경적 특성에 따라 추가적인 보안 요구 사항이 존재한다. 본 논문에서는 해쉬함수를 이용한 기존의 V2I 인증프로토콜에 대하여 검토하고, 이를 정형적 검증 방법인 Casper를 이용하여 인증 프로토콜의 안정성을 분석하였고 그 결과 안전함을 증명하였다.

Analysis of VANET Authentication Protocol using Casper in the Formal Verification

Su-Youn Lee* · Hyo-Beom Ahn**

ABSTRACT

VANET(Vehicular Ad-hoc Network) is a kind of ad hoc networks consist of intelligence vehicular ad nodes, and has become a hot emerging research project in many fields. It provide traffic safety, cooperative driving and etc. but has also some security problems that can be occurred in general ad hoc networks. Also, in VANET, vehiculars should be able to authenticate each other to securely communicate with network-based infrastructure, and their locations and identifiers should not be exposed from the communication messages. This paper explains V2I authentication protocol using a hash function that preserves the user privacy. In addition, we analyze the security stability of the V2I authentication protocol using Casper in the formal verification technique. As a result, V2I authentication protocol using hash function prove a stability.

Key words : VANET, authentication protocol, Casper, formal verification

접수일(2012년 3월 3일), 수정일(1차: 2012년 3월 11일), 게재확정일(2012년 3월 21일)

* 백석문화대학교 인터넷정보학부
** 공주대학교 정보통신공학부 (교신저자)

1. 서 론

차량 애드혹 네트워크 (Vehicular Ad-hoc NETwork; VANET)는 MANET (Mobile Ad-hoc NETwork)의 한 형태로 다수의 차량이 무선통신을 이용하여 차량과 차량 (Vehicular to Vehicular: V2V) 또는 차량과 기지국(Vehicular to Interface: V2I)의 네트워킹을 자율적으로 형성하는 차세대 네트워킹 기술이다. VANET에서 제공되고 있는 차량 통신은 교통정보 제공 서비스, 인터넷 접속 서비스, 엔터테인먼트 서비스 등을 주목적으로 V2I통신이 활용되며 차량안전 관리 정보 교환, 교차로 진입 제어, 차량 주변의 상황을 고려한 실시간 서비스 등을 주목적으로 하는 V2V통신이 이용된다. V2I에서는 기존의 무선 환경에서 존재하는 보안 위협과 차량의 고속이동 및 네트워크 환경의 급격한 변화 때문에 발생하는 다양한 보안 위협이 존재한다. 뿐만 아니라 차량의 이동 정보가 쉽게 노출될 수 있는 문제점이 있어 개인의 프라이버시가 침해될 수 있다. 이를 해결하기 위해 기존에 많은 연구가 이루어졌고 익명 ID기반 집합 방식, 그룹서명 방식 등이 프라이버시 침해를 방지하기 위한 해법을 제시했다. 하지만 관련된 연구에서 제시된 기법은 프라이버시 침해를 방지하기 위해 신뢰기관의 키 저장 공간 및 차량의 계산량에 대한 오버헤드 등의 문제점을 갖고 있다 [1][2].

V2I환경에서 인증 프로토콜을 설계하기 위한 보안 요구사항 중 차량 개인의 프라이버시를 보장하고 효율적인 통신량과 저비용의 계산량이 가장 중요한 항목이다.

본 논문에서는 2008년에 Hwange과 Lee[3]가 제안한 해쉬함수를 이용한 VANET 인증 프로토콜을 분석하여 그 취약성을 분석해보고자한다.

본 논문의 구성은 다음과 같다. 2장에서는 VANET에서 프라이버시를 위한 관련 연구 및 보안 요구사항들을 정의하고 3장에서는 정형검증도구를 소개하고 4장에서는 Hwange과 Lee에 의해 제안된 해쉬함수를 사용한 인증 프로토콜을 살펴보고 5장에서는 정형검증을 통해 안정성을 분석해보고자한다. 마지막으로 6장에서는 결론 및 향후 연구방향을 제시한다.

2. 관련 연구 및 보안 요구 사항

2.1 보안요구사항

차량 애드혹 네트워크에서는 기본의 네트워크와 유사하지만 특히 다음의 보안 요구사항에 대하여 고려하여야 한다.

- **익명성(anonymity)**

익명성은 이웃 차량이나 RSU가 특정 메시지로부터 메시지 근원 차량의 아이디 정보를 알 수 없어야 한다는 것을 의미한다. 사용자의 아이디 노출에 대한 프라이버시를 제공하기 위한 성질이다.

- **비연결성(stateless)**

이웃 차량이나 신뢰 서버는 특정 메시지로부터 특정 차량의 이동경로를 파악할 수 없어야한다. 비연결성은 사용자의 위치에 대한 프라이버시를 제공하기 위한 성질이다. 익명 아이디를 주기적으로 변경해줌으로써 이 성질을 만족시킬 수 있다.

이 요구사항을 바탕으로 하여 차량의 프라이버시를 보호하기 위한 관련 연구에서는 익명 ID기반 집합방식과 그룹서명 방식으로 인증방법이 분류된다.

2.2 익명 ID기반 집합 방식

VANET에 참여하는 차량이 신뢰기관으로부터 익명 ID집합과 그에 따른 개인키 및 인증서의 집합을 부여받아 사용하는 방법을 제안하고 있다. 이들 방법에서 차량은 익명ID를 이용해 익명성을 보장받고 그에 따른 개인키로 메시지의 인증 문제를 해결한다. 차량은 익명ID를 메시지마다 갱신하여 사용하고 소진시 다시 신뢰기관에 접속하여 새로운 집합을 부여받는다.

Raya와 Hubaux는 다량의 익명인증서를 사용하는 시스템을 제안하였다[4]. 각 차량은 초기에 다량의 익명 인증서와 인증기관의 인증서가 설치 된 상태이며 주기적으로 다량의 익명인증서를 발급받아 교체해야 한다. 따라서 차량에 많은 저장 공간이 요구되며 일반 인증서 철회 방법을 사용할 경우에는 CRL (Certificate Revocation List) 크기가 매우 커지는 문제점을 지니고 있다. 따라서 인증서 철회방식에 대한 여러 가지

해결책이 필요하다.

2.3 그룹 서명 방식

사용자 각자의 그룹 서명키와 그룹이 갖는 하나의 그룹 공개키를 이용하여 메시지에 대한 서명 및 확인을 할 수 있는 기법으로 익명성을 보장하면서 서명을 확인할 수 있다는 장점을 갖는다. Lin 등 [5]은 Boneh 등의 그룹서명 [6]과 신원기반 공개키 시스템을 활용한 시스템을 제안하였다. 이 시스템은 차량 간 통신은 그룹서명을 사용하고 RSU가 차량에 메시지를 전달할 때에는 일반 신원기반서명기법을 사용하고 있다. 이 방식은 익명 ID기반과 마찬가지로 철회 목록을 각 차량에게 전달하여 철회하는 형태를 VANET에서 사용하기에는 적절하지 못하며 이 서명기법은 영지식 기술을 이용하는 서명이므로 서명자체가 효율적이지 못하다. Calandriello 등 [7]도 Lin과 마찬가지고 그룹서명기법을 사용하지만 그룹서명을 사용하여 메시지를 교환하는 것이 아니라 각 차량은 그룹 서명키를 이용하여 익명인증서를 스스로 만들어 사용하는 방법을 제안한다. 자체적으로 불연결성을 제공하는 익명의 공개키 쌍을 지속적으로 생성하여 사용할 수 있다는 장점을 지니고 있지만 생성된 익명인증서를 사용하기 위해서는 인증서를 사용하기 위해 그룹서명을 확인해야하고 익명인증서를 이용하여 서명된 메시지를 확인해야한다. 따라서 각 메시지를 확인하기 위한 비용이 비교적 크다.

3. 정형적 검증 도구

보안 프로토콜이란 보안성을 만족하기 위해 암호 알고리즘을 이용하여 메시지를 전달하는 프로토콜이다. 보안 프로토콜을 설계·검증하는 도구로는 크게 1980년 후반부터 사용하기 시작한 정리 증명방법과 1990년 후반부터 사용하기 시작한 모델체킹으로 나누어질 수 있다.

모델체킹의 장점은 자동화 검증도구가 지원된다는 사실이다. 정리증명 방식은 증명과정에서 사람의 개입이 필요하기 때문에 보안 프로토콜을 논리적으로 증명하기에 앞서 가정을 세우고 논리 추론 규칙에 따라 보안 취약점을 추론해 내기가 쉽지 않다.

3.1 CSP(Communication Sequential Process)

CSP[8]는 프로세스 알제브라 언어로서 병렬성을 갖는 통신프로토콜의 동작을 효율적으로 명세하기 위한 언어이다. 최초 일반 통신 프로토콜 및 제어 시스템의 명세를 위해 사용되어졌으나 점차 보안 프로토콜의 명세를 위한 영역으로 확대되어 가고 있다. CSP에서 제공하는 pure synchronization(|||)과 Interleaving par-all-elism(||)개념을 사용하여 분산 시스템 환경하에서 동작하는 클라이언트 서버와 공격자 모델을 정형적으로 표현할 수 있는 장점을 갖고 있다.

3.2 Casper(A Compiler for the Analysis of Security Protocol)

CSP 언어를 이용하여 보안프로토콜 행위를 명세하고 FDR[9] 정형검증 도구를 이용하여 보안속성을 검증하는 연구가 진행되었다. 하지만 CSP 언어를 이용한 정형명세과정은 정형적 설계 방법에 익숙하지 않은 보안 프로토콜 설계자에게는 매우 복잡한 명세언어라는 단점을 갖고 있다. 따라서 Casper[10] 도구로 보안프로토콜의 행위와 검증속성을 명세하게 되면 자동변환기능을 이용해 CSP 명세코드를 생성할 수 있다. 결국, 자동 생성된 CSP 명세코드를 FDR 정형검증도구에 입력하여 보안프로토콜 검증하게 된다.

3.3 FDR(Failure Divergence Refinement)

FDR 도구는 CSP 명세언어를 입력으로 받아들이는 모델체킹 도구로서 CSP 명세언어로 기술 된 보안 프로토콜 모델이 보안성 및 인증속성과 같은 보안 속성들을 만족하는지 검증하게 되며 만일 만족하지 않을 경우에는 CSP 이벤트로 기술된 반례(counterexample)를 보여주어 보안상 취약점 분석을 용이하게 한다.

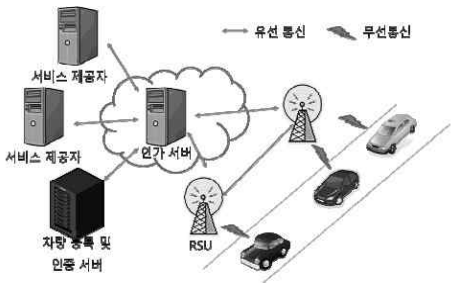
4. VANET 인증 프로토콜

이 장에서는 분석의 대상이 되는 Hwang과 Lee가

제안한 해쉬함수를 사용한 인증 프로토콜을 설명하고자 한다.

4.1 시스템 환경

Hwang과 Lee가 제안한 해쉬함수를 사용한 인증은 (그림1)과 같은 환경으로 RSU와 차량(V) 그리고 차량 등록 및 인증서버(KDC), 인가서버가 서로 통신하는 환경을 갖고 있다.



(그림 1) 시스템 환경

RSU와 차량 V 그리고 KDC는 다음과 같은 역할 및 키를 공유하고 있다.

• RSU(RoadSide Unit)

차량의 통신을 돕기 위한 통신 설비로 도로에 일정한 간격으로 고정되어 있다. 인가 서버와 유선으로 연결되고 대칭키를 공유하고 있다.

• 차량(V)

OBU를 이용하여 무선 통신을 하고 안전한 저장장치(tamper-proof device)를 가지고 있다.

• 차량 등록 및 인증 서버 (KDC)

차량이 판매되면 고유한 아이디와 마스터 키를 부여하고 차량 내부의 안전한 저장장치에 이를 저장한다. 인가 서버와 유선으로 연결되어 있고 대칭키를 공유한다.

<표 1> 프로토콜에서 사용된 기호

기호	의미
KDC	차량 등록 및 인증 서버
AS	인증 서버
VID	차량 등록 시 차량 등록기관 에서 발급하는 차량의 고유한 아이디
K_{KDC}	차량 등록 및 인증 서버 개인 키
SK	세션 키
$E_k(M)$	대칭키 암호화 함수
$D_k(M)$	대칭키 복호화함수
KEK	키 암호화용 키, 차량과 RSU 사이에 공유된 세션 키를 설립하기 위해 사용
K	차량과 키 분배센터 사이에 공유된 마스터 키
$RID(j)$	j번째 RSU의 아이디
IID	차량의 가상 아이디
$G(\bullet)$	충돌방지 일방향 해쉬 함수
$H(\bullet)$	충돌방지 일방향 해쉬 함수
$H^t(M)$	메시지 M을 해쉬함수 H로 t번 해쉬한 값
T	타임 스탬프

또한, 차량 간 통신과 차량에서 RSU간 통신은 프라이버시가 보장되어야 하지만 RSU에서 차량 간 통신은 프라이버시가 요구되지 않으므로 기존 보안 메커니즘을 사용하여도 무관하다. 그러므로 본 논문은 다음과 같은 내용을 가정한다.

- 차량 노드들은 VANET 환경에 참여하기 전에 차량 등록 및 인증 서버에 신원을 등록하고 익명 ID (PID)와 마스터 키(K), 타임 스탬프 (T)를 지급받는다.
- 차량 등록 및 인증 서버는 신뢰할 수 있는 기관으로 안전하다고 가정한다.

이 프로토콜에 대하여 분석하는 과정에 사용되는 기호는 <표 1>에서 보는 것과 같다.

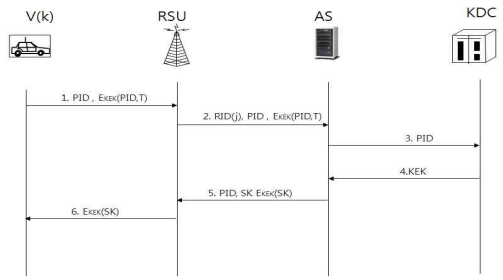
4.2 인증 프로토콜의 설명

4.2.1 차량 등록 단계

차량이 출고되면 차량은 차량 등록 및 인증 서버에 등록한다. 차량이 등록되면 차량 등록 및 인증 서버는 차량에게 아이디 VID와 마스터 키 K, 키 사용 횟수 t를 차량의 안전한 저장장치에 저장한다. 아이디와 마스터키를 입력 받은 차량은 마스터키를 t번 해쉬하여 저장한다.

4.2.2 익명의 차량 인증 단계

차량이 도로를 이용하면서 도로에 설치된 RSU와 인증을 하여 서비스 제공자 서버로부터 콘텐츠를 제공받아서 이용하는 단계이다.



(그림 2) V2I 인증 프로토콜

단계1: V는 RSU에게 ID와 $E_{KEK}(ID, T)$을 전송한다. ID는 $G(G(h^t(MS))||t)$이고 KEK는 $G(H^t(MS))$이다. 차량은 t를 $t-1$로 대체한다.

단계2: V에게 메시지를 받은 RSU는 자신의 아이디 $RID(j)$와 V에게 받은 ID와 $E_{KEK}(ID, T)$를 AS에게 전달한다.

단계3: RSU에게 $RID(j)$,ID,$E_{KEK}(ID, T)$를 전달받은 AS는 내용을 저장하고 ID를 KDC에게 전달한다.

단계4: AS에게 ID를 전달받은 KDC는 ID가 등록된 V의 것인지 확인하고 등록된 V의 것이라면 KEK를 AS에게 전송하고 자신의 데이터베이스에 저장되어 있는 ID와 KEK를 각각 $G(G(h^t(MS))||t)$이고 KEK는 $G(H^t(MS))$로 대체한다.

단계5: KDC에게 KEK를 전달받은 AS는 KEK를 이용하여 $D_{KEK}(E_{KEK}(ID, T))$를 계산하여서 ID가 존재하는지 확인한다. 존재한다면 랜덤하게 SK를 선택하고 $E_{KEK}(SK)$를 계산한다. 그리고 RSU에게 ID,SK, $E_{KEK}(SK)$를 전송한다.

단계6: AS에게 ID,SK, $E_{KEK}(SK)$를 전송 받은 RSU는 ID,SK를 저장하고 차량에게 $E_{KEK}(SK)$를 전송한다.

단계7: RSU에게 $E_{KEK}(SK)$를 전달받은 V는 KEK를 이용하여 $D_{KEK}(E_{KEK}(SK))$를 계산한다. V는 SK를 알게 된다. V와 RSU사이에 세션키 SK가 공유되었으므로 공유된 키를 이용하여 데이터를 암호화하여 전송한다.

5. Casper를 이용한 VANET 인증 프로토콜 분석 및 검증 결과

5.1 VANET 인증 프로토콜 분석

Hwang과 Lee는 차량의 익명성을 보장하며 효율성을 높인 해쉬함수 기반 인증 프로토콜을 제안하였다. 본 장에서는 이 효율적인 인증 프로토콜을 분석한다.

본 논문에서는 Hwang-Lee 프로토콜을 Casper 도구를 이용하여 모델링하였다. Casper 명세 중 보안 프로토콜의 행위와 검증속성과 같은 일부 섹션헤더 부분만 보여주고 있다. 자유변수영역(#Free variables)과 프로토콜 기술영역(#Protocol Description), 침입자 영역(#Intruder information)에 대한 표현이다. 다른 명세 부분은 매우 간단하고 명확해서 자세한 설명은 생략하고자 한다.

```
#Free variables
v, u : Agent
s1, s2 : Server
skv: Secretkey
kek: key encryption key
SSK: Agent x Agent -> SSK
(skv, sku): InverseKeys
H: HashFunction
```

#Free variable 섹션 헤더에서는 #Protocol description에서 사용되는 자유 변수의 타입 및 함수를 정의하고 있다. v와 u는 V와 RSU 호스트의 식별자를 의미하고 s1과 s2는 AS와 KDC 서버의 식별자를 나타낸

다. skv는 V의 마스터 키 K를 의미한다. 그리고 SSK는 두 Agent간의 세션 키를 의미한다. InverseKey는 메시지에 대한 암호화 및 복호화를 표현하며 H는 해쉬함수 $H(\bullet), G(\bullet)$를 의미한다.

#protocol description
0. v → u: v, {v, t}{kek(skv)}
1. u → s1: u, v, {v, t}{kek(skv)} % dig U
2. s1 → s2: H(H^t(skv))||t) % dig S1
3. s2 → s1: H(H^t(skv))
4. s1 → u: v, SSK, {SSK}{kek}
5. u → v: {SSK}{kek} % dig U

#protocol description 섹션 헤더는 프로토콜의 교환 동작을 나타내기 위해 사용된다. 표현식에서 {m}{k}은 키 k로 암호화 한 메시지 m을 나타낸다. 그리고 표현식 m%d에서 m은 전달하고자하는 메시지를 의미하고 d는 메시지를 저장하기 위한 변수로 메시지를 수신한 호스트가 메시지 m을 건드리지 않고 단지 다른 호스타나 서버에 전달만 하는 기능을 표현하기 위해 사용된다.

본 논문에서는 익명성과 비연결성 두 가지의 보안 속성을 검증하고자 한다.

#Intruder information
Intruder = Mallory
IntruderKnowledge = {Vender, User, Kim, Lee, Mallory, v, u, SSK}

#Intruder information 섹션 헤더에서는 통신 프로토콜을 공격하기 위한 공격자의 사전 정보를 표현한다. 예를 들어, 위의 명세 코드를 보면 공격자 호스트의 이름은 Mallory라고 설정하였으며 Vendor, User, Kim 그리고 Lee는 각각 V, RSU , AS, KDC에 대한 도메인 이름을 나타내고 있다.

본 논문에서는 공격자는 모든 호스트의 식별자를 도청을 통해 알 수 있다고 한다.

5.2 VANET 인증 프로토콜 검증 결과

본 장에서는 제안한 Hwang-Lee 인증 프로토콜을 보안 요구사항에 대해 암호학적 안전성을 분석한다.

Secret(V, skv(V,S), [V])
Secret(V, skv(V,S), [S])
Agreement(V, S, [skv, t, SSK])

첫 번째 표현은 “V는 skv(V,S) 정보를 오직 S와만 알고 있다”라고 풀이할 수 있고 두 번째 표현은 “V는 skv(V,S) 정보를 오직 V와만 알고 있다″로 풀이 할 수 있다. 세 번째 표현은 ”V는 skv, t, SSK 정보를 S로부터 자신의 개체를 인증 받는다“라고 풀이할 수 있다.

▪ **익명성(anonymity)**

공격자가 사용자의 PID 정보를 도청하여 소유하고 있다고 가정하자. PID는 $G(G(h^t(MS))||t)$로 계산이 되어지고 여기서 t는 V와 S만이 소유하고 있는 정보이므로 실제 V의 아이디인 VID를 알아 낼 수 없으므로 익명성이 보장된다.

▪ **비연결성(stateless)**

차량은 인증을 할 경우 PID만을 자신의 식별자로 사용한다. 하지만 PID는 t에 의해 매번 인증시마다 변경되기 때문에 각 인증 사이의 관계를 다른 차량이나 RSU가 알 수 없다.

6. 결 론

본 논문에서는 VANET 환경에서 차량의 프라이버시를 보호하기 위해 Hawang-Lee가 제안한 해쉬함수를 사용한 인증프로토콜을 정형검증 기법인 Casper을 사용하여 암호학적 안정성을 분석하였다.

분석 결과 익명성 부분에서는 해쉬 함수를 사용시 실제 차량의 아이디를 사용하지 않고 가상의 아이디를 사용하였고 이때 타임스탬프 t 값을 사용하므로 익명성이 보장이 되는 것으로 분석되고 아이디가 t 값에 의해 매번 변경되므로 비연결성을 만족하는 것으로 분석되었다. 그러므로 해쉬함수를 사용한 인증 프로토콜은 VANET에서 인증을 위해 사용하는 방법으로는 적절하다. 그러나 이런 정형적 분석방법은 도구를 이용하여서도 더 세분화하여 검증할 수 있다.

향후에는 정형검증 도구 중 자동화 검증도구인 AV

ISPA를 사용하여 좀 더 정밀한 분석과 함께 새로운 VANET 인증 프로토콜을 연구할 계획이다.

참고문헌

[1] G. Calandriello, P. Papadimitratos and J. P. Hubaux, "Efficient and Robust Pseudonymous Authentication in VANET, " In Proc. International Workshop VANET, pp.19-28, 2007.

[2] J. Zhang, L. Ma, W. Su, and Y. Wang, "Privacy-Preserving Authentication Based on Short Group Signature in Vehicular Networks," Proceedings of the First International Symposium on Data, Privacy, and E-Commerce, pp. 138-142,

[3] B.H.Hwang, D.H.Lee, "An efficient authentication protocol between vehicle and communication infrastructure for intelligent vehicular networks", proceeding of the ITFE Summer conference, pp 500-503,August, 2008.

[4] M..raya and J.Hubaux, "Securing vehicular ad hoc networks," J. of Computer Security, vol. 15, no. 1, pp. 39-68, Jan.2007

[5] X. Lin, X. Sun, P,-H, Ho and X. Shen, "GSIS: A Secure and Privacy Preserving Protocol for Vehicular Coomunications", IEEE Trans, on Vehicular Technology, vol, 56, no.6, pp.3442-3456, 2007.

[6] Hoare, C.A.R., Communication Sequential Porcesses, Prentice-Hall, 1985

N), LNCS, pp 149-164, 2004.

[7] G. Calandriello, P. Papadimitratos and J. P. Hubaux, "Efficient and Robust Pseudonymous Authentication in VANET," In Proc. International Workshop VANET, pp. 19-28, 2007.

[8] Hoare, C.A.R, Communicating Sequential Processes, Prentice-Hall, 1985.

[9] Formal System Ltd, FDR2 User Manual, Aug, 1999.

[10] Lowq, G., "Casper: A Compiler for the analysis of Security Protocols," In Proc. of the 1997 IEEE Computer Security Foundation Workshop X, IEEE Computer Society, Silver Spring, MD, pp, 18-30, 1997.

[저자소개]

이 수 연 (Su-Youn Lee)

1990년 단국대학교 전자계산학과 (이학사)
1993년 단국대학교 전산통계학과 대학원 석사(이학석사)
2003년 성균관대학교 전기전자 및 컴퓨터공학부 대학원 박사 (공학박사)
1997년 3월 ~ 현재 백석문화대학교 인터넷정보학부 교수

e-mail : sylee@bscu.ac.kr

안 효 범 (Hyo-Beom Ahn)

1992년 단국대학교 전자계산학과(이학사)
1994년 단국대학교 전산통계학과 대학원 석사(이학석사)
2002년 단국대학교 전산통계학과 대학원 박사(이학박사)
1997년 9월 ~ 2005년 3월 천안 공업대학 정보통신과 부교수
2005년 3월 ~ 현재 공주대학교 정보통신학부 교수

e-mail : hyobeom.ahn@gmail.com