http://www.jsebs.org
ISSN: 2288-3908

The Journal of Society for e-Business Studies
Vol.24, No.2, May 2019, pp.55-70
https://doi.org/10.7838/jsebs.2019.24.2.055

MACSec의 단말 이동성 성능평가

Performance Evaluation of MACSec for Host Mobility

안상준(Sangjun Ahn)*, 신동천(Dongcheon Shin)**

초 록

통신 인프라 구축과 최적화를 위해서는 각 구성 요소들의 연관성을 고려할 필요가 있다. 본 논문에서는 최적화된 통신 인프라 구축을 위해 필요한 주요 고려사항을 바탕으로 성능이 향상된 MACSec 기반의 통신 인프라 구성 방안을 제시한다. 제안된 MACSec 기반 기술은 통신 인프라를 처음부터 다시 설계하지 않고 IPSec 기술을 별도의 장비를 추가하지 않고 대체할 수 있다. 아울러, 구성 시 주요 고려사항인 메시지 오버헤드와 암호화 처리 성능, 그리고 이동성 측면에서 실험을 통해 IPSec과 성능을 평가한다. 시험 결과에 따르면 MACSec으로 구현된 암호화 네트워크에서 IPSec보다 Hop 지연과 메시지 오버헤드와 같은 일반적 성능뿐만 아니라 연결 지점 변경 시험을 통해 이동성 성능이 우위에 있다.

ABSTRACT

It is essential to consider the relationships between each component in the communication infrastructure in order to build and optimize the infrastructure. In this paper, based on the major factors to consider for the optimized communication infrastructure, we propose an enhanced MACSec-based deployment mechanism for communication infrastructure. The proposed MACSec mechanism can replace the IPSec without the additional devices and redesign of the communication infrastructure. In addition, we evaluate the performance of MACSec and IPSec in terms of the major factors such as message overhead, encryption processing, and host mobility. According to the evaluation results, we can say that MACSec is superior to IPSec with regard to mobility as well as hop delay and message overhead.

키워드 : 근거리통신망, MACSec, 호스트 이동성, IPSec, 서비스제공자 가설 사설망
Local Area Network, MACSec, Host Mobility, IPSec, PPVPN

* First Author, Department of Convergence Security, Graduate School of Chung-Ang University (sj@eknowtek.com)
** Corresponding Author, Department of Industrial Security, Chung-Ang University(dcshin@cau.ac.kr)
Received: 2019-01-11, Review completed: 2019-03-21, Accepted: 2019-04-18

1. 서 론

통신 인프라 사업자는 증가하는 네트워크 트래픽 요구사항을 위한 충분한 용량과 이동성의 지원과 같은 고도의 연결 서비스를 충족시키기 위해 발생하는 투자(CAPEX)와 운영 비용(OPEX) 증가에 고심하고 있다. 우리나라에서 세계 최초로 상용화를 시작한 5G 모바일 네트워크는 기존 LTE 방식에 비해 1/10 이하의 응답속도와 20배 이상의 대역폭, 시속 500km의 고속열차 내에서도 성능이 보장되는 모바일 통신을 목표로 하고 있다. 그리고 향상된 암호화와 인증, 프라이버시에 대한 개선 또한 요구되고 있다. 그러나 보편적인 네트워크 보안의 경직된 구조 측면에서, “정적 부품을 통해 서비스를 사전 정의하고, 운영자는 사소한 변경작업을 반복 수행하고 장비를 추가 구매” 하는 형태의 투자방식으로 현재 더 많은 가입자 단말을 수용하고 있다. 통신 인프라의 안정성 및 품질 보장 중심으로 고려한 이러한 투자 방식은 현재에도 통신업계에서 고수되고 있다[10]. 서비스 공급자 영역에서 과거에는 독점적인 장비로 정적인 서비스를 사용하는 것이 보안 측면에서도 장점이 많았다[13]. 그러나 이러한 초기 투자방식은 새로운 기능이나 역할의 추가로 인한 재작업 및 배포에 불리하다[10]. 보안과 이동성의 결합은 중앙 집중화와 대규모의 운용을 의미하지는 않으나 현재의 기술적 조건은 융통성이 부족하고 인프라의 중앙 집중화를 더욱 가속화 한다[3].

모바일 인터넷은 이동성(Mobility)과 접근성(Reach)이 유선과는 다른 차별적인 특성이라고 할 수 있다. 특히 “언제 어디서나 끊임없이”의 개념은 모바일 인터넷의 고비용, 저성능 단말, 낮은 망 서비스 품질 등의 한계에서 성능저하를 감수하더라도, 이동하면서 사용할 수 있다는 측면을 강조했다[14]. 향후 고신뢰 모바일 네트워크 인프라에서는 이동하는 단말들의 네트워크 접속이 보다 안전하고 원활해야 한다. 그러나 널리 분포되어있는 인프라 연결 지점의 장치들을 물리적으로 완벽하게 보호하기는 앞으로도 쉬운 일은 아니다. 광학 전송링크는 간단한 물리적 TAP 장비 연결을 통해 손쉽게 도청이 가능한 상태이다. 그리고 여전히 모바일 장치들은 접속 지점을 더욱 빈번하게 변경하고, 이동성을 지원하기 위한 엔터티들을 다양한 계층에서 복잡하게 관리하여 전반적인 통신 성능의 저하를 일으킨다. 통신 시스템 내 무결성과 기밀성을 제공하는 암호화 장비는 반복되는 수작업을 요구하며, 암호화에 따른 데이터 오버헤드 등으로 인해 통신 고유성능과 비용 효율성을 떨어트리고 복잡성을 증가시키고 있다[9].

최근 주목되고 있는 사물 인터넷(Internet of Thing)은 사물간의 연결을 통하여 의미가 있는 정보가 창출되며, 다양한 웹 콘텐츠 및 구조, 사용 기록, 센서 및 위치 등 다양한 종류의 데이터를 처리가 요구되어 이에 따른 전송 중요도나 민감도가 높아질 것이다. 장치들은 이동성을 위해 모바일 네트워크에 더욱 빈번하게 연결되어 다양한 인터넷상의 보안 위협에 노출될 가능성이 지속 증가하고 있다. 이에 보안과 규제를 적용함과 동시에 사용에 제한이 되지 않는 모델을 구축하여야 한다[11].

무결성과 기밀성 제공에 따른 기존 형태의 성능저하 문제점을 최소화하고, 이동성을 보장하는 모바일 보안 통신기술 검토는 현시점에서 중요하다고 할 수 있다. 계층적 관점에서 보안 엔터티들의 동작은 현재 보편적인 3계층 이상의 방식에서 낮은 계층으로 통합하는 방법을

고려해 볼 수 있다. 이에 따른 모바일 단말의 이동성 성능향상을 측정하여 기술 타당성을 파악하고 제안할 필요가 있다.

본 논문에서는 모바일 통신 인프라의 암호화 기술에서 기존의 IPSec VPN 방식보다 MACSec 방식이 비용과 성능 한계를 극복할 수 있을 것이라는 가설을 전제로 시험한다. 이는 기존 통신 인프라를 새로 설계하지 않고 현재 MPLS를 사용하고 있는 모바일 네트워크 구조의 변경을 단순화 및 최소화하여 투자비 보호를 고려하는 것을 주요 목표로 한다, 아울러 보안 설계에서 성능향상의 평가 척도로 메시지 오버헤드와 암호화 처리 성능, 그리고 이동성을 고려하여 실증 시험을 통해 제시된 방안의 성능평가를 한다. 이러한 보안기술을 시험할 수 있음에 따라 고유한 조건이나 상태에서 어떻게 작동하는지 모니터링 할 수 있으며, 이러한 시험을 통해 수용자에게 기술 도입에 따른 불완전한 요소를 제거할 수 있다[4].

본 논문의 구성은 다음과 같다. 제2장에서는 IPSec 과 MACSec을 중심으로 관련된 이슈들을 간략히 소개하고 시사점을 기술한다. 제3장에서는 IPSec과 MACSec의 일반적인 성능과 메시지 오버헤드를 평가한다. 제4장에서는 이동성 관점에서 평가한다. 마지막으로 제5장에서는 결론을 맺는다.

2. 관련 연구

2.1 IPSec과 MACSec

통신 무결성과 기밀성 그리고 재생방지 기능을 통한 보안 제공은 현재 주로 OSI의 3계층 이상에서 IPSec과 SSL/TLS, 그리고 SSH등의 프로토콜을 보편적으로 이용하고 있다. 이러한 프로토콜들은 2계층 메시지를 직접 보호하지 못하며, 특정 계층의 보호를 해당 계층에서 직접 수행하지 않는다면, 터널링과 캡슐화 등의 메시지 오버헤드가 발생하게 된다. 한편 2계층 보호 프로토콜을 사용하면 2계층을 직접 보호할 수 있어 오버헤드 최적화에 유리하다[9].

MACSec은 데이터 암호화 전송 기술로서 EAPOL-MKA 프로토콜로 802.1X를 확장하고 상호 인증 확인 및 MACSec 비밀키 공유를 통해 MACSec 장치를 탐색하고 데이터를 보호한다[8]. 이더넷 연결에서 기밀성, 무결성, 그리고 사용자 데이터의 진위 판별을 제공하고 물리적으로 완벽하게 보호하기 어려운 환경에서 원본 데이터의 변조나 유실, 권한이 없는 사람의 전송과 수신으로 발생하는 서비스 중단 손실을 방지할 수 있다.

인터넷 패킷의 목적지 전달 신뢰성을 기반으로 한 가상 사설망(IP-VPN)은 기업의 사설 네트워크 구축비용을 전용회선 임대 서비스에 비해 절감 효과 면에서 크게 기여하는 장점이 있다. 하지만 IP-VPN은 투자비용과 관리의 복잡성, 데이터의 추가적인 오버헤드는 단점으로 작용해 왔다. MACSec은 기능에 의한 별도의 투자를 요구하지 않는 2계층 스위치 내에서 자체 구현하여 관리의 복잡성과 터널링 오버헤드를 발생하지 않는다. 이와 관련하여 LTE, 혹은 다음 세대의 모바일 네트워크에서 MACSec 이 모바일 중앙 네트워크에서 사용자 단말 사이의 터널에서 데이터 전송을 보호할 수 있다[7].

MACSec의 특징은 통신 인프라 구조의 2계층 Hop-by-Hop 동작을 전제로 한다. Gu et al.[7]에서는 MACSec over VxLAN 오버레이 기술을

이용하여 기존 통신인프라 구성을 최종적으로 2계층에서 암호화 통신을 설계 평가하였다. 아울러 기존의 인프라를 재설계하지 않고도 지리적 제한과 서로 다른 서비스 제공자 구간을 극복할 수 있음을 제시하였다. 그리고 연결 시도 회수 증가에 따른 플러딩 공격 등의 시나리오에서 지연시간 성능을 측정하였다. 그러나 VxLAN 터널 방식은 본 논문에서 전제로 하는 MPLS-VPN 통신 방식에 비해 터널 오버헤드가 증가하고, 모바일 네트워크의 중요 성능척도인 이동성에 관련된 연구 결과가 결여되어 있다.

2.2 핸드오프 계층

IP주소 속성기반의 3계층 핸드오프에는 기본 게이트웨이 탐색, IP주소 수집 및 중복 검색, 인접 라우터 도달 가능성 감지, 로컬 액세스 인증 등과 같은 몇 가지 기본 작업이 포함된다. 이러한 작업 간에는 라우터, DHCP 및 인증 서버와 같은 모바일 및 기타 네트워크 엔터티 간의 여러 가지 메시지 교환을 포함한다. 또한 상위 응용 프로그램 계층의 핸드오프 지연은 대부분 응용프로그램 바인딩 업데이트, 최종 호스트에서 처리, 등록 및 상위 계층 암호화(TLS, SRTP)와 같은 작업에 기인한다[6]. 그러나 2계층의 핸드오프는 3계층 식별자 획득과 변동되지 않는 주소의 중복 검출로 인한 추가 지연시간을 수반하지 않는다. 2계층 탐색 프로세스 동안 3계층 탐색 프로세스를 계획하거나 2계층 식별자가 구성 완료되기 전 3계층 식별자 구성을 시도하는 형태로 핸드오프 지연시간을 최소화하고 있다[6].

MPTCP는 TCP 계층에서의 핸드오프 최적화 방안으로 이를 이용한 다중 엑세스 포인트 접속 방식도 고려할 수 있다[5]. 이는 복수의 주소 할당 및 관리를 필요로 하며 이에 보안 관리 엔터티를 증가시킬 가능성이 있으며, 액세스 포인트가 중복으로 필요하고 TCP 프로토콜 계층에서만 동작하는 등 여러 제약이 있다.

2.3 시사점

IPSec은 IP 트래픽 보안을 위한 가시적 솔루션을 제공하며 이미 상용 네트워크에 많은 사례가 있는 프로토콜이지만, 고려사항이 매우 광범위하다. Server-Client, Site-Site 등의 구성 방식은 상이하며, 수요 증가에 따른 보안 게이트웨이의 투자 및 반복 작업이 필요하다. 뿐만 아니라 암호화 기능을 수행하는 엔진 기반으로 급격하게 증가하는 트래픽에 대해 비용이 많이 발생하는 문제가 있다. IPSec VPN은 하위계층을 보호하지 않으며, 배포와 재작업에 많은 시간이 소요된다. 적절한 솔루션을 선택하는 것은 어려운 작업이며 향상된 보안 수준을 고려한 비용과 성능이 고려되어야 한다.

L2TP 프로토콜을 이용하면 IPSec을 이용한 이더넷 프레임 전달이 가능하다. 하지만 이를 위해 3계층 IP 페이로드에 이더넷 프레임을 수용하기 때문에 패킷당 50바이트의 오버헤드를 발생하는 비효율이 발생하며, 또한 추가로 암호화를 위해 적어도 38~53 바이트의 오버헤드가 발생한다. 아울러 고신뢰 네트워킹 시스템을 달성하기 위해, 네트워크는 적절한 은닉 기술과 가상화, 그리고 망 분리 기술과 이기종 터널을 지원해야 한다.

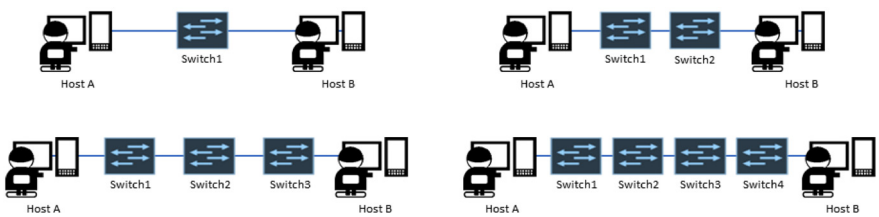
본 논문에서 제시하는 IEEE std. 802.1AE MACSec(Media Access Control Security)은 특정 응용프로그램이나 프로토콜에 의존하지 않는 네트워크 통신 전체를 보호하는 암호화

기술이다. 본 논문에서는 국내/외 모바일 네트워크 사업자가 이미 보편적으로 사용하며, 서비스 제공자들이 기업 관리자를 대신하여 VPN의 설립부터 관리까지 지원하는 상용 MPLS기반 PPVPN 서비스[2]에서 MACSec을 사용하는 모형을 제시한다. 제시된 방식을 통해 물리적으로 서로 다른 지역의 네트워크를 가상의 2계층 네트워크로 재구성하여 기존의 한계를 극복하는 연결성을 제공한다.

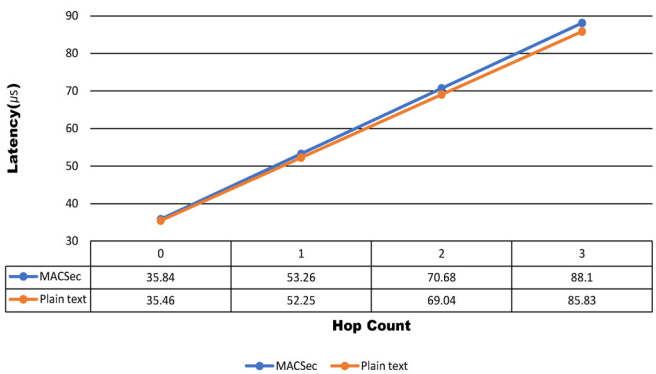
3. 일반 성능과 오버헤드 평가

3.1 MACSec의 Hop 지연시간 성능 평가

PPVPN을 고려하지 않고 IPSec VPN의 게이트웨이 장비를 대체하는 MACSec 구성 시나리오 모형을 설계한다(<Figure 1> 참조). IPSec의 경우 다수의 Hop으로 이루어진 네트워크 내에서 Multi-hop 직접 연결로 동작하지만, MACSec은 Hop-by-Hop 연결 구성에 대해 정의되어 있다. 이는 경유하는 모든 스위치 장비는 MACSec이 동작해야 하며 전체 인프라의 구성 변경을 의미한다. 발신자는 암호화 메시지를 MACSec 포멧으로 전송하고 수신자 경로의 모든 스위치는 입력 포트에서 데이터를 해독하고 출력 포트에서 다시 암호화 한다[7]. MACsec 네트워크의 호스트간에 n개의 스위치가 있는 경우 각 스위치가 두 가지 작업을 수행하기 때문에 2n번의 작업이 필요하며[7], MACsec는 MAC 서비스 데이터 단위 (MSDU) 크기의 증가로 인해 추가 전송 지연을 초래한다[1].



〈Figure 1〉 Test diagram of Hop Increment



〈Figure 2〉 Comparison of MACSec Hopping Delay Time(1Gbps)

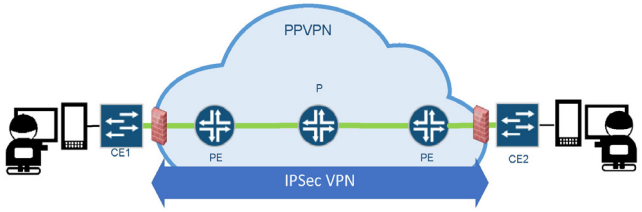
본 논문에서는 여러 Hop으로 구현하는 MACSec의 네트워크 환경에서 대역폭 및 지연시간의 성능제약 유무를 평문 통신과 암호화 통신을 비교하여 시험한다. 시험 결과 Hop 이 증가하는 경우 MACSec 추가 암/복호화 작업으로 인한 추가 지연시간은 Hop 당 약 0.63us정도로 나타나 Hop 증가에 따른 평문과 암호화 통신 간 성능 차이는 미비함을 알 수 있었다(<Figure 2> 참조).

3.2 IPSec의 메시지 오버헤드

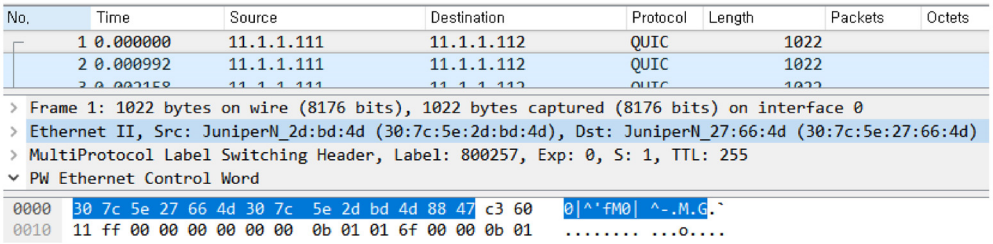
본 논문에서는 PPVPN에서 구현하는 IPSec VPN의 메시지 오버헤드를 측정한다. 오버헤드 크기가 클수록 가용대역폭이 감소하며 성능저하를 유발한다. 시험을 위해 MPLS 백본 인프라를 통한 2계층 PPVPN 구성에 보편적인 IPSec VPN을 추가하는 방식으로 네트워크 종단에 IPSec VPN 게이트웨이 방화벽을 구성한다. 각 PE(Provider Edge) 라우터는 인입 패킷을 P(Provider) 라우터를 경유하는 MPLS 패킷으로 캡슐화하여 전달한다. 모든 PE 라우터는 L2VPN 시그널링을 위한 MP-BGP 피어를 맺고 MPLS 네트워크를 경유하는 2계층 경로를 생성한다(<Figure 3> 참조).

이더넷 프레임은 총 1000바이트 길이로 생성한다. 이더넷 헤더(14바이트)와 802.1Q Vlan-Tag (4바이트), IP 헤더(20바이트), 그리고 UDP 헤더(8바이트) 등의 필요한 헤더와 실제 메시지(954바이트)로 구성한다. PPVPN을 경유하여 평문으로 통신하는 경우, 각 프로바이더 라우터는 MPLS 네트워크를 경유하기 위한 추가적인 이더넷 헤더 14바이트, 그리고 목적지 MPLS 헤더 4바이트, VPWS PW Control word 4바이트 등의 오버헤드 발생하여 총 1,022바이트의 데이터 크기로 전달한다(<Figure 4> 참조).

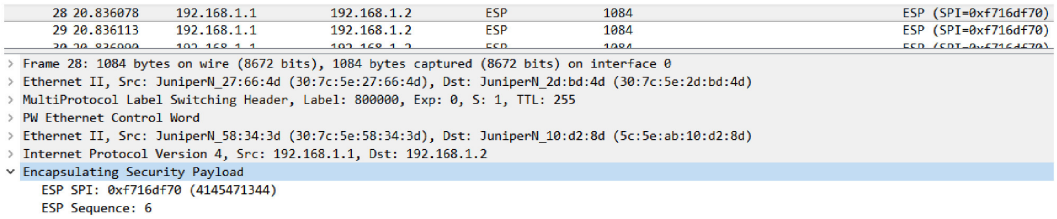
IPSec VPN은 MACSec과 동일한 3계층을 보호하기 위해 터널모드로 구성한다. 구성이 완료되면 N2X 테스터를 이용하여 가상 클라이



〈Figure 3〉 Test Diagram of IPSec over PPVPN



〈Figure 4〉 Plain-Text Messages



〈Figure 5〉 Encrypted Packet by IPSec over PPVPN

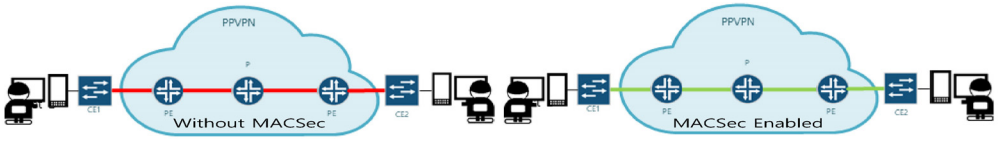
언트를 생성하고 P 라우터에서 전송되는 암호화 패킷을 확인한다. 3계층 패킷의 출발지와 목적지 IP주소는 IPSec VPN의 인터페이스 IP주소로 변환되었으며 실제 출발지 IP주소와 목적지 IP주소, 그리고 전달하는 메시지가 ESP 프로토콜을 이용하여 암호화되어 전달하는 것을 확인할 수 있다. 1,000바이트의 원본 평문을 암호화하여 전송하기 위한 메시지 크기는 총 1,084바이트이며, PPVPN의 총 헤더 22바이트를 제외하면 62바이트의 오버헤드 발생을 <Figure 5>에서 알 수 있다.

3.3 MACSec의 오버헤드

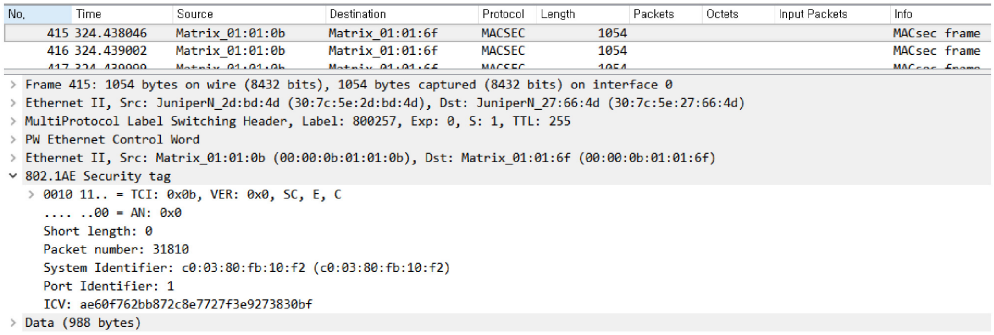
PPVPN에서 구현하는 MACSec의 메시지 오버헤드를 측정한다. 이는 Hop-by-Hop 제약을 PPVPN을 통해 통신 인프라 전체를 변경하지 않기 위해, 아래와 같이 일반적인 사업자 네트워크와 유사한 MPLS 백본 환경의 시험 모형을 구성한다(<Figure 6> 참조).

암호화를 위한 MACSec을 수행하는 스위치는 시험 인프라 구성 완료 후 각 CE(Customer Edge) 에서 설정하고, MACSec 프로토콜을 적용하여 구성이 완료되면 키 교환을 확인한다. 활성화된 인터페이스에서는 Port Access Entity Group 주소(01:80:c2:00:00:03)을 이더넷 목적지 주소로 하고, 인접하고 있는 스위치로 EAPOL-MKA 키교환을 시도한다.

N2X를 이용하여 가상 클라이언트를 생성하고 총 길이 1,000바이트 의 이더넷 프레임을 생성한다. 라우터에서 전송되는 암호화 패킷의 오버헤드를 확인한다. 2계층 프레임의 출발지와 목적지 IP주소는 MPLS VPN의 인터페이스 IP주소로 변환되었으며 실제 출발지 IP주소와 목적지 IP주소, 그리고 전달하는 메시지가 암호화되어 전달하는 것을 확인할 수 있다. 1,000바이트의 원본 평문을 암호화하여 전송하기 위해 총 1,054바이트를 생성하였으며, 이는 PPVPN의 22바이트 오버헤드를 제외하면 32바이트의 MACSec 오버헤드를 확인할 수 있다(<Figure 7> 참조). IPSec VPN을 사용할 경우 62바이트에 비해 약 1.4배 향상된 오버헤드가 절감됨을 알 수 있다.



〈Figure 6〉 Test Diagram of MACSec over PPVPN



〈Figure 7〉 Encrypted Ethernet frame by MACSec over PPVPN

3.4 IPSec과 MACSec 구성 차이에 따른 성능 비교 분석

현재 광범위하게 사용되는 IPSec VPN 환경을 가정하고, 가용대역폭과 암호화 성능, 그리고 지연시간 특징을 시험 메시지 대역폭을 증가시켜 비교한다. 128bit 암호화 비트 길이를 이용한 대역폭별 성능을 시험한 결과를 <Table 1>, <Table 2>, <Table 3>과 <Figure 8>이 보여주고 있다. 실제 대역폭의 12% 정도인 단방향 120Mbps를 초과하는 경우 데이터의 암호화 처리하는데 지연시간 및 패킷 손실이 지속적으로

〈Table 1〉 Performance of Plain-Text over PPVPN

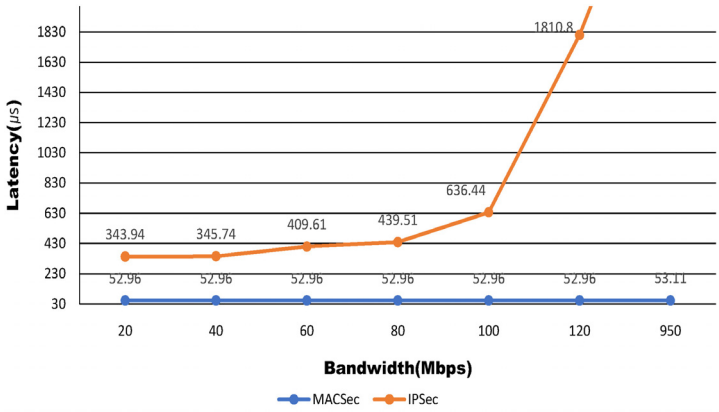
Packet load bandwidth	10% (100Mbps)	20% (200Mbps)	40% (400Mbps)	60% (600Mbps)	95% 930Mbps
Packet arrival rate	100%	100%	100%	100%	100%
Packet loss rate	0%	0%	0%	0%	0%
Packet Delay time	52.22㎲	52.22㎲	52.22㎲	52.22㎲	52.23㎲

〈Table 2〉 Performance of IPSec over PPVPN Encryption

Packet load bandwidth	20Mbps	40Mbps	60Mbps	80Mbps	Over 100Mbps
Packet arrival rate	100%	100%	100%	100%	Under 100%
Packet loss rate	0	0	0	0	Loss after Exceeding Queue
Packet Delay time	343.94us	345.71us	409.91us	439.51us	Continually increased

〈Table 3〉 Performance of MACSec over PPVPN Encryption

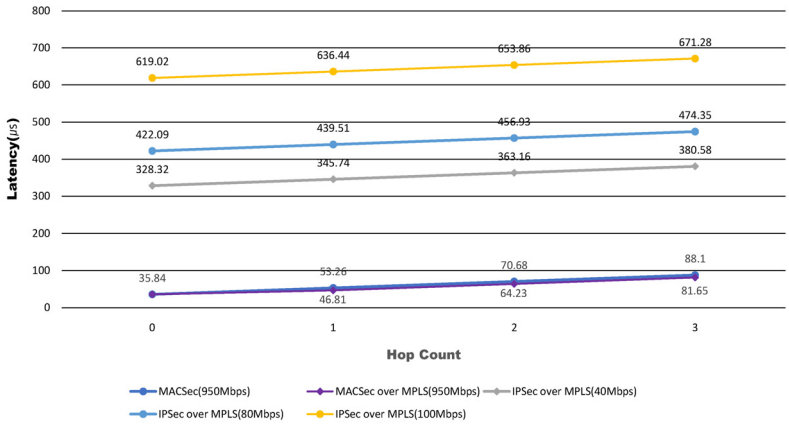
Packet load bandwidth	Under 10% (100Mbps)	20% (200Mbps)	40% (400Mbps)	60% (600Mbps)	95% 930Mbps
Packet arrival rate	100%	100%	100%	100%	100%
Packet loss rate	0	0	0	0	0
Packet Delay time	52.96㎲	52.96㎲	52.96㎲	52.96㎲	53.11㎲



〈Figure 8〉 Comparison of MACSec and IPSec Latency by Bandwidth

증가하는 것을 알 수 있다. PPVPN 시험 환경에서 IPSec과 MACSec의 비교 결과 가용대역폭은 10배 이상 발생하여, 서비스 품질 측정 척도는 가용 대역폭 내에서 전송 속도별로 지연시간이 증가함을 알 수 있다. 또한 MPLS 자체와 MACSec 오버헤드로 인한 제약사항에 따라 최대 대역폭의 95%까지 측정하는 경우 가용 대역폭을 성능과 지연시간 성능저하 없이 사용할 수 있는 것을 알 수 있다. IPSec VPN의 경우 트래픽 양이 증가함에 따라 지연시간이 증가하였으며, MACSec의 경우 위와 같이 거의 증가하지 않았다. IPSec VPN 게이트웨이에서 안정적으로 처리가 가능한 대역폭인 20Mbps에서 100Mbps에서 비교하는 경우 메시지 지연시간은 6배 이상 차이를 보임을 알 수 있다.

Hop 증가에 따른 제공 성능 기준을 MACSec과 물리적으로 동일한 케이블 길이와 전송 속도의 조건으로, 프로토콜을 MACSec 대신 단말의 종단에 IPSec VPN 게이트웨이를 이용한 환경 시험하였을 때와 부하별 비교 결과를 <Figure



〈Figure 9〉 Comparison of IPSec vs. MACSec Performance by Hop and Load

9>는 보여주고 있다.

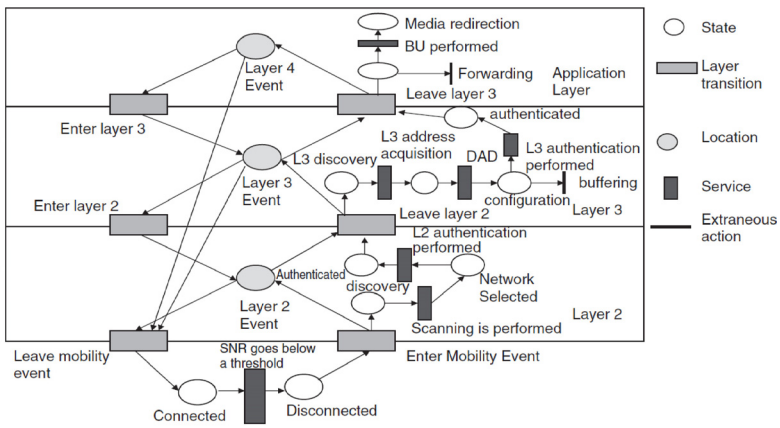
새로운 인프라로 재설계를 고려하더라도, 기존 IPSec VPN을 대체하는 프로토콜인 MACSec의 성능 관점에서, 지연시간과 대역폭에서 나은 성능을 제공하고 있다. 대부분의 상용 통신 인프라에 적용되어 있는 IPSec VPN 게이트웨이는 실제 물리 대역폭을 사용하는데 성능 제약이 발생한다. 그러나 MACSec은 물리적 가용 대역폭의 사용이 가능함을 알 수 있다. 이는 사용자가 향후 IPSec과 MACSec에 대한 선택을 고려할 때, 프로토콜 적용의 범위를 사전 정의하여야 하며, 중복 투자를 방지함과 동시에 최적의 성능을 고려할 수 있는 사전 검증의 기초가 된다는 의미를 나타낸다.

4. 이동성 평가

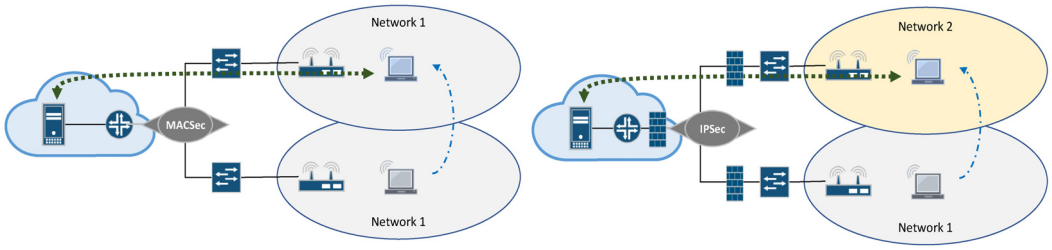
4.1 이동성 시험 평가 모형

본 시험에서는 2계층으로 구성된 환경에서 제안 기술을 평가하기 위해 페트리넷으로 “계층화된 핸드오프 모형”을 참조한다(<Figure 10> 참조). 시험 환경으로는 브로드컴 BCM43460 칩셋을 사용하는 상용 엑세스 포인트로 802.11n 방식의 무선 네트워크를 구성한다. 인텔 Advanced-N 6205를 무선 네트워크 어댑터로 사용하는 윈도우7 랩탑을 무선 단말 역할로 구성하고, 정확한 핸드오프 지연시간 측정을 위해 Agilent의 N2X Router tester900을 각 종단에 연결한다. 유선 네트워크는 IPSec과 MACSec의 암호화 통신 인프라 구성 특성에 의해 각 계층의 핸드오프에서 발생하는 엔터티 변화 감소에 따른 이동성 확보 방안을 고려하여 적용한다.

802.11 무선 랜 설계에서, 단독 액세스 포인트의 서비스 영역을 기본 서비스 세트(BSS, Basic Service Set)라 하며, 확장 서비스 세트(ESS, Extended Service Set)는 모든 동일한 ESSID를 브로드캐스트 하는 액세스 포인트들의 수집으로 구성된다[12]. 802.11 무선 단말이 서로 다른 BSS로 이동하는 핸드오프 시나리오에서 단말(STA)은 핸드오프 지점 전후의 ESSID가 동일한 경우, 재연결(re-association)을 발송한다. 아울러 하나의 ESS 내 BSS 변경은 액세스 포인트



〈Figure 10〉 Layered Modeling with a Petri-net[6]



〈Figure 11〉 Layer based Hand-off Model

가 동일한 IP 서브넷으로 패킷을 보낼 수 있는지 여부에 따라 3계층 핸드오버가 필요할 수도 있고 필요하지 않을 수도 있다[12]. 두 지점이 동일 서브넷의 일부로 네트워크가 구성되어 있는 경우, 브로드캐스트 도메인이 변경되지 않고 통신이 재개되는 과정에서 기존 3계층 식별자가 유효하기 때문에 빠른 통신 재개가 가능하다. 따라서 802.11의 각 무선 ESSID 구성별 핸드오버 특성에 맞게 제안하는 암호화 기술을 적용할 수 있는 2계층 네트워크 구성 방안의 타당한 시나리오를 제시한다(<Figure 11> 참조).

서로 다른 통신 인프라에 상호 접속하기 위해 IP주소의 동적 할당이 필요하며, 모든 시험은 IP주소의 동적 할당을 전제로 인프라 접속 구간에 DHCP 서버를 각각 별도로 구성한다. 최초 접속점에서 IP주소를 최초 자동할당 받고, 다른 서브넷에 속하는 무선 액세스 네트워크 사이를 이동할 때, SNR 임계값에 의한 이동성 이벤트에 진입한다. 서로 다른 서브넷에 속하는 2개의 무선 액세스 네트워크 사이를 이동할 때, 3계층 핸드오프 이벤트 진행 과정 중에도 통신을 바로 재개할 수 있는 2계층 구성과, 통신을 즉시 재개할 수 없는 3계층 구성 방법을 통하여 추가 통신 지연시간을 확인할 수 있다.

핸드오프 상태 변화에 따른 동작 과정 및 시험범주 대상은 <Table 4>와 같다. 인증과정과 키분배, 보안 관계 설립 과정은 핸드오프 성능 비교를 위한 구성 방식과 관계없는 공통 기능 범주로 간주하여 시험 범위에서 제외하였다. 액세스 포인트는 상호 영향을 주지 않는 단독형으로 구성하고, 주파수 간섭을 배제하기 위해 서로 중첩되지 않는 주파수 채널을 할당하였으며, 액세스 포인트의 신호 출력 세기는 동일한 고정 값을 사용하였다.

〈Table 4〉 Atomic Operations during Handoff[6]

Transition	Handoff Operation	Category
t_0	Disconnect trigger	Included
t_1	Network discovery	Included
t_2	Network attachment	Included
t_3	Mobile configuration	Included
t_4	Authentication	Excluded
t_5	Security association	Excluded
t_6	Binding update	Included
t_7	Hierarchical binding update	Included
t_8	Media redirection	Included
t_9	Local data redirection	Excluded

4.2 IPSec VPN의 서로 다른 ESSID 구성

MPLS 기반 PPVPN상 IPSec VPN 연결을 위한 방화벽을 구성한다. 서로 다른 두 개의

〈Table 5〉 Handoff Performance of IPSec

Packet per Second	1st Test	2nd Test	3rd Test	4th Test	5th Test	Avg. Handoff Time
1000pps	1,089ms	1,045ms	981ms	948ms	1,019ms	1,016ms
2000pps	2,234ms	2,296ms	2,451ms	2,231ms	2,150ms	1,136ms
3000pps	3,329ms	3,088ms	2,978ms	3,075ms	3,078ms	1,036ms

ESSID를 각 AP에 구성하고 AP1에 단말을 최초 접속 후 정해진 양의 트래픽을 인가한다, 다음에 단말에서 재접속 과정을 통한 핸드오프를 트리거하여, 단말이 AP1에서 AP2로 재접속하는 핸드오프를 재현한다. 이는 핸드오버 시점의 사전 스캔정보의 의존을 배제하기 위함이다. 트래픽 생성기(N2X)에서는 프레임의 크기를 1,000바이트로 생성하고, 실시간 프로토콜로 가정한 UDP 프로토콜을 생성한다. 트래픽 양 증가와 핸드오프의 영향도 분석을 위해 1000pps에서 5000pps까지 다섯 단계를 생성한다. 총 손실 개수를 각 pps로 나누어 핸드오프 경우에 발생하는 프레임의 손실 개수를 통해 단절시간을 밀리 초 단위로 계산한다. 또한 각 시험은 양방향으로 5회 실시하여 편차를 확인한 결과는 <Table 5>와 같다.

4.3 MACSec의 서로 다른 ESSID 구성

MACSec의 경우에는 별도의 게이트웨이 없이 PPVPN상에서 2계층 암호화를 구현한다. IPSec VPN을 위한 방화벽을 제거하고 스위치에 MACSec 기능을 활성화한다. IPSec VPN과 동일한 무선 네트워크를 구성하여 단말을 접속하고 각 대역폭별 통신을 인가하고 핸드오프를 트리거 하였을 때 핸드오프 지연시간은 <Table 6>과 같다.

4.4 MACSec의 동일 ESSID 구성

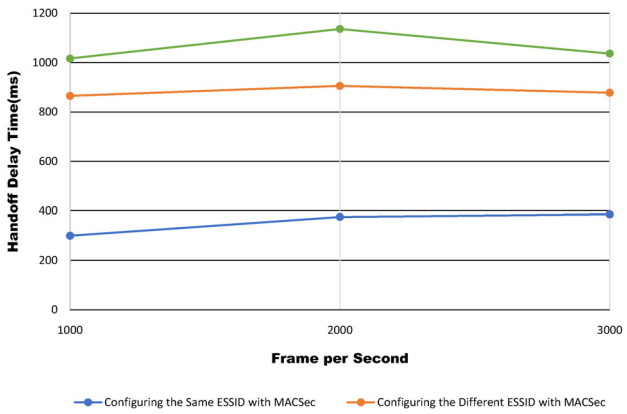
2계층으로 구성하는 무선 네트워크는 엑세스 포인트들 간 동일한 ESSID로의 구성으로 구현이 가능하다. 3계층 동일 ESSID 핸드오프 시나리오의 경우 Proxy ARP, Mobile IP와 같은 별도의 기술이 필요하다. Proxy ARP 구현은 특정 제조사 제품 등에 의존하는 무선 랜의 앵커 컨트롤러에서 초기 주소 유지 역할이 필요하며, Mobile IP 구현은 별도로 서버와 응용 프로그램의 지원이 필요하다. 한편, Mobile IP는 삼각형 라우팅, 더블 크로싱 등의 비효율성 개선에 추가적인 논점이 필요하므로 본 논문의 통신 인프라 통합 관점에서는 3계층 구성의 동일 ESSID 시험의

〈Table 6〉 Different ESSID Handoff Performance of MACSec

Packet per Second	1st Test	2nd Test	3rd Test	4th Test	5th Test	Avg. Handoff Time
1000pps	851ms	884ms	874ms	851ms	866ms	865.2
2000pps	1,864ms	1,670ms	1,832ms	1,789ms	1,901ms	905.6
3000pps	2,601ms	2,604ms	2,676ms	2,674ms	2,614ms	877.9

〈Table 7〉 Same ESSID Handoff Performance of MACSec

Packet per Second	1st Test	2nd Test	3rd Test	4th Test	5th Test	Avg. Handoff Time
1000pps	268ms	323ms	295ms	301ms	311ms	299.6ms
2000pps	758ms	769ms	751ms	720ms	758ms	375.6ms
3000pps	964ms	1,074ms	1,181ms	1,186ms	1,388ms	386.2ms



〈Figure 12〉 Comparison of Handoff Delay Time between IPSec and MACSec

대상 범주로 진행하지 않는다.

2계층 구성 네트워크에서 서로 동일한 ESSID를 각 AP에 구성하고 AP1에 호스트를 최초 접속 후 트래픽을 인가한다. 다음에 AP1의 무선 신호를 엑세스 포인트에서 단절하여 핸드오프를 트리거하고 단말이 AP2에 자동 접속하는 방법으로 시험한다. 트래픽 생성기에서는 핸드오프 경우에 발생하는 프레임의 손실 개수를 통해 밀리 초 단위의 단절시간을 확인한다. 각 시험은 양방향으로 5회 실시하여 편차를 확인한 결과를 <Table 7>에서 알 수 있다.

위 시험들을 종합한 결과를 보여 주는 <Figure 12>에 따르면 IPSec VPN 네트워크 환경과 MACSec 네트워크 환경에서 호스트가 이동시 발생하는 핸드오프 단절시간이 절감됨을 알 수 있다.

5. 결 론

지속적으로 증가하는 단말 수와 이에 따른 모바일 트래픽 증가로 이미 많은 환경에서 IPSec VPN의 비용과 성능은 문제가 되어왔다. 이 문제는 IPSec VPN의 용량 확충과 별도의 부하를 분산하는 솔루션(VPN Load balancing 등)을 추가하는 방식으로 성능제약을 회피하여 개선해 왔다. 그러나 이러한 해결책은 네트워크의 고비용과 복잡한 요소로 작용하는 단점이 지적되어 왔다. 본 논문에서 제안된 MACSec 기반 기술은 통신 인프라를 처음부터 다시 설계하지 않고 IPSec 기술을 별도의 장비를 추가하지 않고 대체할 수 있는 방안이다. 통신 인프라 구성에서 메시지 오버헤드, 암호화 처리 성능, 그리고 이동성을 주요 고려 사항으로 하였다.

제안된 MACSec 암호화 통신이 기존 IPSec과 동등하게 공격의 위험을 줄이면서도 오버헤드가 적으며 짧은 핸드오프 지연시간을 제공하는지 시험을 하였다. 시험 결과에 따르면 MACSec으로 구성한 보안 시험 환경이 IPSec보다 전반적으로 향상된 성능을 보인다고 할 수 있다. 뿐만 아니라 네트워크 구조를 보다 단순화 할 수 있음을 알 수 있다. 결과적으로 IPSec에 비해 이동성뿐만 아니라 다른 여러 가지 성능을 개선하는 MACSec 구성이 가능함을 실증적인 구현을 통해 알 수 있다.

끝으로 본 논문은 다음과 같은 한계점이 있다. 첫째, 현실적인 적용을 위해서는 상용 환경과 동일한 단말의 수와 모바일 패킷 코어, 그리고 실제 기지국과 유사한 통신 흐름으로 구성하여야 한다. 그러나 현실적으로 무선 랜 방식을 사용하여 유의한 결론을 도출하였다. 둘째, 인증, 주파수 간섭, 단말 제조사의 고유 특성 등의 추가 변수를 시험 과정에 현실적으로 충분히 반영하지 못했다는 것이다. 따라서 향후 결과에 영향을 줄 수 있는 다른 변수들의 반영, 그리고 본 연구의 범주에 포함하지 못한 기존 계층 환경 변화에 따른 IP 라우팅 관점, 마지막으로 실제 환경과 유사한 시험 조건에서 추가 연구가 필요하다고 할 수 있다.

References

[1] Altunbasak, H., Krasser, S., Owen, H. L., Grimminger, J., Huth, H. P., and Sokol, J., “Securing Layer 2 in Local Area Networks,” Networking-ICN, pp. 699-706, 2005.

[2] Barceló, F., Paradells, J., Setaki, F., and Gibeaux, M., “Design and Modeling of Internode: A Mobile Provider Provisioned VPN,” Mobile Networks and Applications, Vol. 8, No. 1, pp. 51-60, 2003.

[3] Beauchamps, M., Hoitjink, M., and Leese, M., “Introduction: Security/Mobility and the Politics of Movement,” Manchester University Press, pp. 1-13, 2017.

[4] Choi, W. G. and Lee, Y. J., “Factors Influencing the Introduction of Mobile Security Technology,” The Journal of Society for e-Business Studies, Vol. 18, No. 4, pp. 215-240, 2013.

[5] Croitoru, A., Niculescu, D., and Raiciu, C., “Towards WiFi Mobility without Fast Handover,” Proceedings of the 12th USENIX Conference on Networked Systems Design and Implementation, pp. 219-234, 2015.

[6] Dutta, A. and Shulzrinne, H., “Mobility Protocols and Handover Optimization,” John Wiley & Sons, Ltd-IEEE Press, 2014.

[7] Gu, R., Zhang, X., Yu, L., and Zhang, J., “Enhancing Security and Scalability in Software Defined LTE Core Networks,” 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering(TrustCom/BigDataSE), IEEE, 2018.

[8] IEEE Std. 802.1AE, “Media Access Control (MAC) Security,” 2006.

[9] Jaggi, C., “Ethernet Encryptors for Metro and Carrier Ethernet,” http://www.uebermeister.com/publications.html, 2017.

[10] John, W., Pentikousis, K., Agapiou, G., Jacob, E., Kind, M., Manzalini, A., Risso, F., Staessens, D., Steinert, R., and Meirosu, C., “Research Directions in Network Service Chaining,” SDN4FNS 2013 Workshop on Software Defined Networks for Future Networks and Services, IEEE SDN, pp. 1-7, 2013.

[11] Lee, S. and Jahng, J., “The Diffusion of Internet of Things: Forecasting Technologies and Company Strategies using Qualitative and Quantitative Approach,” The Journal of Society for e-Business Studies, Vol. 20, No. 4, pp. 19-39, 2015.

[12] McCann, P., “Mobile IPv6 Fast Handovers for 802.11 Networks,” IETF RFC 4260, November 2005.

[13] Quinn, P. and Nadeau, T., “Problem Statement for Service Function Chaining,” IETF RFC 7498, April 2015.

[14] Shin, H., Song, Y. U., Sung, N. H., “The Impact of Perception on the Difference Between Mobile and Stationary Internet Toward the Intention to Use Mobile Internet,” The Journal of Society for e-Business Studies, Vol. 15, No. 3, pp. 99-129, 2010.

저 자 소 개

안상준 (Email: sj@eknowtek.com)
2016년 서울과학기술대학교 전자IT미디어공학과 (학사)
2019년 중앙대학교 융합보안학과 (석사)
관심분야 TCP/IP, MPLS

신동천 (Email: dcshin@cau.ac.kr)
1985년 서울대학교 컴퓨터공학과 (학사)
1987년 KAIST 전산학과 (석사)
1991년 KAIST 전산학과 (박사)
관심분야 소프트웨어 보안, 접근 제어