Journal of the Korea Academia-Industrial cooperation Society
Vol. 13, No. 11 pp. 5496-5505, 2012

http://dx.doi.org/10.5762/KAIS.2012.13.11.5496

스마트폰 환경에서 신뢰기관을 이용한 이동 통신사 AP 접속 인증에 관한 연구

이기성[1], 민대기[2*], 전문석[2]
[1]호원대학교 컴퓨터게임학부, [2]숭실대학교 컴퓨터학부

A Study on Authentication of Mobile Agency AP Connection Using Trusted Third Party in Smart Phone Environment

Gi-Sung Lee[1], Dae-Gi Min[2*] and Moon-Seog Jun[2]
[1]**Department of Computer & Game, Howon University,**
[2]**Department of Computer Science, SoongSil University**

요 약 IT 산업이 발달하면서 활발히 연구되어 지고 있는 스마트폰의 기술과 기능들은 생활 전반에 걸쳐 많은 영향을 주고 있다. 이러한 스마트폰을 이용하여 시간과 장소에 구애받지 않고 인터넷을 이용할 수 있는 무선랜에 대한 관심이 날로 증가하고 있지만, 무선 전파의 특성으로 인해 개인적이면서 중요한 정보들이 악의적인 공격자의 스푸핑, 서비스 거부 공격, 중간자 공격에 쉽게 노출되어 보안성 요구가 더욱 증가 하고 있다.
본 논문에서는 스마트폰 환경에서 사용자가 이동 통신사 AP 접속을 통하여 무선 인터넷을 이용할 때 USIM에 있는 사용자 고유정보와 AP 정보, 통신사 정보를 사용하여 사용자 인증, AP 인증, 통신사 인증을 함으로써 스푸핑, 세션 하이재킹 및 중간자 공격에 대한 취약성을 보완하여 안전한 무선 네트워크 서비스 환경을 제공한다.

Abstract As the IT industry develops, the smart-phone technology and functions which are actively being studied at the moment greatly influence the entire living environment. With the smart-phone technology and functions, people's interest for the wireless LAN which can be used to get access to the Internet anytime anywhere is gradually increasing. However, since the malicious attacker can easily carry out hacking or approach the contents due to the characteristics of the wireless radio wave, the personal information with a high level of importance for data security is easily exposed due to Spoofing, Denial of Service attack and Man in the Middle attack. Therefore, the demand for security is gradually increasing.
In this paper, the safe wireless network service environment is provided by supplementing the vulnerability in regard to Spoofing, Session Hijacking and Man in the Middle attack after executing the client's authentication process, the AP authentication process and the Mobile Agency authentication process with the client's information in the USIM, the AP information and the Mobile Agency information when the client uses the wireless Internet through the Mobile Agency AP access in the smart phone environment.

Key Words : Smart phone, Access Point, Wireless, Authentication, Security

1. 서론

오늘날 활발히 연구되어지고 있는 스마트폰의 기술과 기능들은 생활 전반에 걸쳐 많은 영향을 주고 있고, 앞으로도 미래의 생활과 IT산업에도 큰 영향을 끼칠 것으로 예측되고 있다.

본 연구는 2012년도 호원대학교 학술연구조성비 지원에 의하여 연구되었음
*Corresponding Author : Dae-Gi Min
Tel: +82-10-5333-6230 email: pwohaha@naver.com
접수일 12년 09월 11일 수정일 12년 10월 12일 게재확정일 12년 11월 08일

또한 스마트폰을 이용하여 시간과 장소에 구애받지 않고 인터넷을 이용할 수 있는 무선랜에 대한 관심이 날로 증가하고 있다. 무선랜은 단말기의 재배치가 쉽고 빠른 시간 안에 네트워크 구축이 용이하지만 무선 전파의 특성으로 인해 악의적인 공격자가 해킹 및 접근이 용이하기 때문에 스푸핑, 서비스 거부 공격, 중간자 공격 등 데이터 보안 중요도가 높은 개인적이면서 중요한 정보들은 쉽게 노출되어 보안성 요구가 더욱 증가 하고 있다.

따라서 본 논문은 스마트폰 환경에서 사용자가 이동 통신사 AP 접속을 위한 안전한 인증 기법을 통해 스푸핑, 세션 하이재킹 및 중간자 공격에 대한 취약성을 보완하여 강화된 인증 및 안전한 통신 서비스를 제공하는 무선 네트워크 보완시스템을 제안한다.

제안하는 시스템은 USIM에 있는 사용자 고유정보와 AP 정보, 이동 통신사 정보를 사용하여 사용자 인증, AP 인증, 이동 통신사 인증을 통하여 안전한 무선 네트워크 서비스 환경을 제공한다.

본고의 2장에서는 기존의 인증 프로토콜을 살펴보고, 3장에서는 제안하는 프로토콜을 소개한다. 4장에서는 기존 시스템과 제안하는 시스템의 구현을 통해 성능분석 및 안전성 문석 결과를 기술 하였다. 마지막으로 5장에서는 결론을 통해 논문을 맺는다.

2. 관련연구

2.1 무선랜 보안 요소

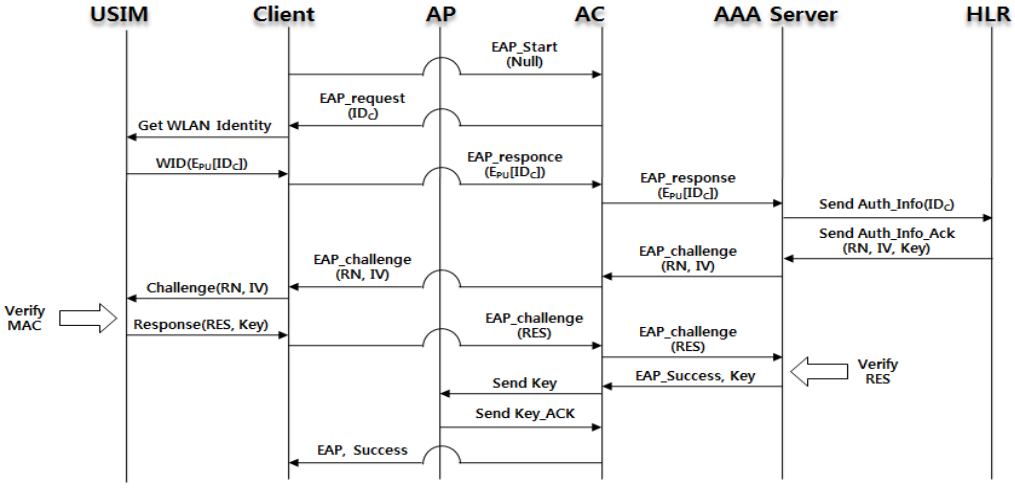
무선 LAN(Wireless Local Area Network) 보안을 위한 요소는 처리 대상인 정보의 속성에 따라 다양화 할 수 있지만, 일반적인 보안 요소는 사용자 인증(Authentication), 접근제어(Access control), 권한검증(Authorization), 데이터 기밀성(Privacy), 데이터 무결성(Integrity), 부인방지(Non-repudiation), 안전한 핸드오프(Secure hand-off)로 정리할 수 있다. 이중 가장 핵심이 되는 무선랜 환경에서의 보안은 사용자 인증과 데이터 암호화라 할 수 있다. 통신망을 통하여 단말기에 접속하는 사용자가 등록되어 있는 정당한 사용자인지의 확인하는 과정을 사용자 인증이라고 하며, 데이터들을 비인가자가 이해할 수 없도록 하는 것이 암호화라고 할 수 있다[3].

2.2 EAP-AKA 프로토콜

IETF의 표준인 EAP-AKA 인증은 3세대 이동통신망(WCDMA)의 사용자가 표준 인증인 AKA알고리즘을 이용하여 WLAN망에서 동일하게 이증될 수 있는 모델을 보여준다. EAP-AKA 인증은 기존 AKA 인증에 EAP 개념을 도입함으로써 사용자의 단일 인증을 통한 편의성, 호환성 및 보안이 한층 강화될 수 있는 장점은 있으나, 프로토콜의 오버헤드가 증가하는 단점을 지닌다[1][2].

[그림 1]은 EAP-AKA 인증이 이루어지는 전체 단계를 나타내며 인증 절차는 다음과 같다[1].

① 사용자는 AC에게 WLAN에 접속할 것을 요청한다.
② AC가 사용자의 IDC를 요구하면, 모바일기기에 장착된 USIM 카드는 칩에 저장된 사용자의 IDC를 AAA 서버의 공개키로 암호화하여 EAP_response / AKA_identity를 통해 AC로 보낸다.



[그림 1] EAP-AKA 프로토콜의 인증과정
[Fig 1] EAP-AKA Protocol Authentication Process

③ AC는 사용자로부터 받은 IDC를 AAA서버로 전송하여 인증을 요청하면, AAA서버는 개인키로 IDC를 복호화한 후 HLR에 C의 IDC를 전송한다.
④ HLR은 IDC를 이용하여 RN과 IV 그리고 Key를 생성하여 RN과 IV는 EAP_request / AKA_challenge를 이용하여 AAA서버와 AC를 거쳐 USIM 카드로 전송되고 Key는 AAA서버에 저장한다.
⑤ USIM 카드는 메시지에 포함된 MAC(Message Authentication Code)값을 검증하여 결과가 성공적일 경우 결과 값(RES)을 AAA서버로 전송하고 실패하면 다시 접속 요청을 한다.
⑥ AAA서버는 수신된 RES 값을 자신이 가지고 있는 값과 비교하여 사용자에 대한 인증을 수행한다.
⑦ 인증이 성공적으로 끝나면 AC로 Key를 전송하고, 실패하면 일련의 작업을 중지시키고 사용자에게 재전송 요청을 한다.
⑧ AC는 AP로 Key를 보내고 AP는 수신된 Key가 올바른 Key라고 긍정의 신호를 보낸다.
⑨ AC는 사용자에게 WLAN에 접속할 수 있는 권한을 준다.

3. 제안하는 인증 메커니즘

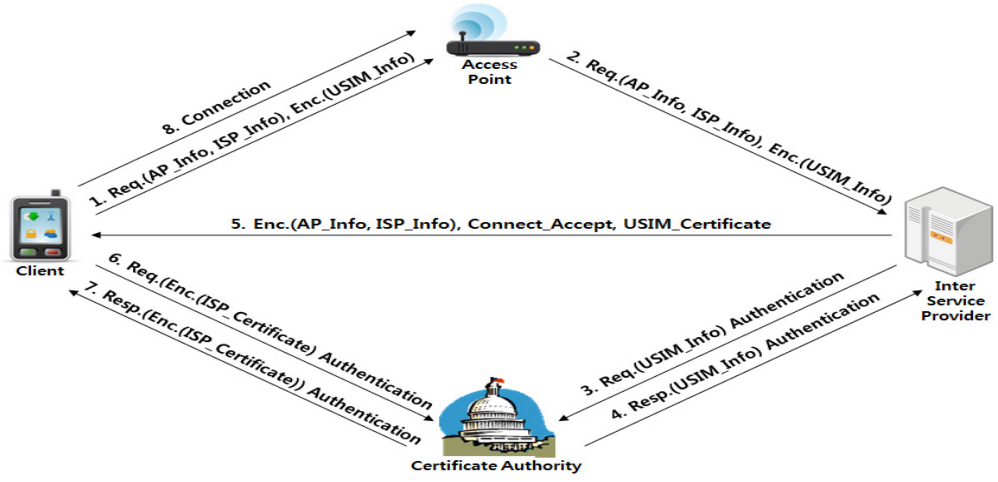
본 논문에서 제안하는 방식은 정상적인 AP를 가장한 불법 AP, 정상적인 사용자를 가장한 악의적인 공격자를 방지하기 위하여 사용자 인증, AP 인증, 이동 통신사 인증을 통해 스마트폰 환경에서 안전하게 이동 통신사 AP 접속을 하기 위한 신뢰기관 기반의 인증 방식이다. 제안하는 방식은 다음과 같은 조건을 만족해야 한다.

조건 1 : 제안한 방식에 필요한 구성원은 사용자와, AP, 이동 통신사 서버, 인증을 위한 인증기관(CA : Certificate Authority)이 필요하다.
조건 2 : 사용자와 이동 통신사 서버는 사전에 인증기관과 신뢰된 관계가 형성되어야 한다.
조건 3 : 이동 통신사 서버는 설치 되어있는 AP에 대한 정보를 가지고 있어야 한다.

3.1 제안 메커니즘 구성도

[그림 2]는 본 논문에서 제안하는 신뢰기관 기반의 인증 기법에 대한 전체 구성도로 단계별 설명은 다음과 같다.

① Client는 AP의 정보, 이동 통신사의 정보를 요청하고, Client의 개인 정보를 ISP와 사전에 공유하고 있는 대칭키로 암호화하여 보낸다.
② AP는 Client로부터 받은 정보들을 ISP에게 전송한다.
③ ISP는 AP로부터 받은 정보들 중에 Client의 개인 정보 값을 사전에 공유하고 있는 대칭키로 복호화하고, 정보를 확인하기 위해서 사전에 신뢰관계가 형성된 CA에게 유효성을 요청한다.
④ CA는 ISP로부터 받은 정보가 일치하는지 확인하고, 유효성 확인 응답을 ISP에게 전송한다.
⑤ ISP는 Client가 요청한 AP 정보를 사전에 공유하고 있는 대칭키로 암호화하고, 이동 통신사 정보에 대해서는 자신의 개인키로 전자 서명 하여 암호화한다. 동시



[그림 2] 시스템 구성도
[Fig 2] System Configuration

에 ISP로부터 전송받은 Client 정보 유효성 확인 값과 AP에 접속 연결을 할 것인지에 대한 메시지를 3G망을 통하여 전송한다.

⑥ Client는 대칭키로 AP 정보를 복호화하고, 이동 통신사 정보는 ISP의 공개키로 복호화 하여 두 값이 일치하는지 확인한다. 두 값이 일치한다면 CA에게 ISP로부터 받은 이동 통신사 정보가 CA에 등록되어 있는 정보와 일치하는지 여부를 확인하기 위해 CA의 공개키를 이용해 암호화 하여 인증 요청을 한다.

⑦ CA는 Client로부터 받은 값을 자신의 개인키를 이용해 복호화 하여 일치 여부를 확인하고 일치한다면 Client의 공개키를 이용해 암호화 하여 확인 응답 값을 전송한다.

⑧ Client는 자신의 개인키로 CA에게 받은 값을 복호화 하여 이동 통신사 정보 일치 확인 값일 경우 AP에 접속을 한다.

3.2 제안 메커니즘에 사용되는 파라미터

[표 1]은 본 논문에서 제안하는 인증 메커니즘에 사용되는 파라미터이다.

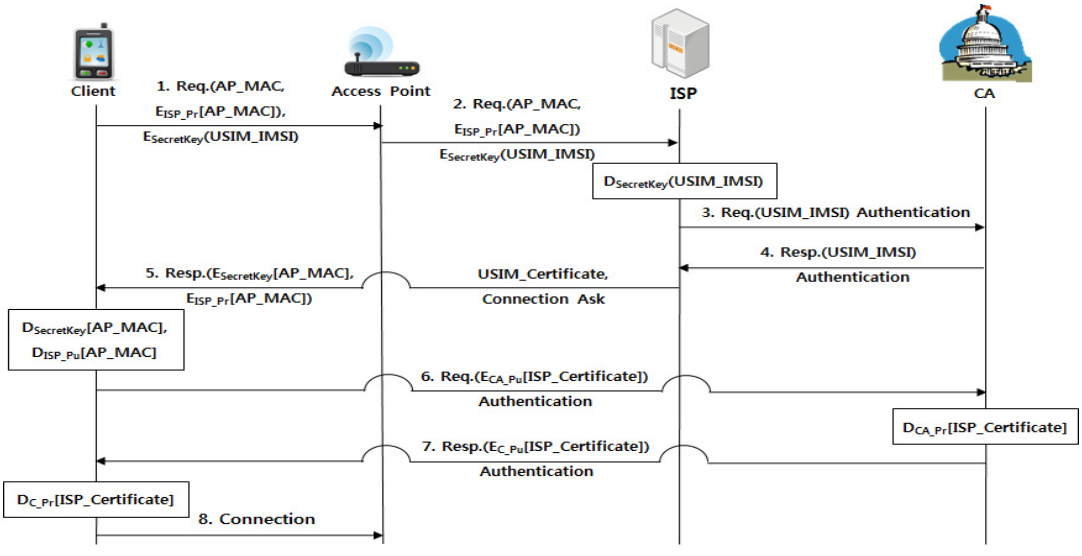
[표 1] 메커니즘에 사용되는 파라미터
[Table 1] Parameters

기호	내용
AP_MAC	AP의 맥주소
$SecretKey$	Client와 ISP가 사전에 공유한 값
$IMSI$	USIM에 들어있는 국제 모바일 가입자 인증 번호
$E_{ISP\_pr}[AP\_MAC]$	ISP의 개인키로 AP의 맥주소를 전자 서명한 이동 통신사 정보 값
$E_{CA\_Pu}[ISP\_Certificate]$	Client에서 이동 통신사 정보의 인증을 CA에게 요청하기 위해 CA의 공개키로 암호화한 값
$E_{C\_Pu}[ISP\_Certificate]$	CA에서 통신사 정보의 인증을 Client에게 응답하기 위해 Client의 공개키로 암호화한 값

3.3 제안 메커니즘 상세 프로토콜

[그림 3]은 본 논문에서 제안하는 신뢰기관 기반의 인증 기법에 대한 상세 프로토콜로 단계별 설명은 다음과 같다.

① Client는 ISP에게 AP_MAC와 $E_{ISP_pr}[AP_MAC]$을 요청하고, Client는 개인 정보 값인 단말 안에 있는 USIM 정보 중에 IMSI 값을 사전에 공유하고 있는 $SecretKey$로 암호화하여 전송한다.



[그림 3] 프로토콜
[Fig 3] Protocol

② AP는 Client로부터 받은 정보들을 ISP에게 전송한다.

③ ISP는 AP로부터 받은 정보들 중에 $D_{SecretKey}[USIM_IMSI]$와 같이 복호화 하고, Client의 개인 정보 값을 확인하기 위해서 $Req.(USIM\_IMSI)Authentication$ 같이 CA에게 유효성 검사를 요청한다.
ISP는 Client의 개인 정보 값을 확인하기 위해서 사전에 신뢰관계가 형성된 CA에게 $USIM\_IMSI$ 값의 유효성 검사를 요청한다.

④ CA는 ISP로부터 받은 $USIM\_IMSI$ 정보가 일치하는지 확인하고, 유효성 확인 응답을 ISP에게 전송한다.

⑤ ISP는 $E_{SecretKey}[AP\_MAC]$, $E_{ISP_pr}[AP_MAC]$와 같이 암호화와 전자 서명한 값을 생성하여 Client에게 전송한다. 동시에 CA로부터 전송받은 Client 정보 유효성 확인 값과 AP에 접속 연결을 할 것인지에 대한 메시지를 3G망을 통하여 전송한다.
ISP는 Client가 요청한 AP_MAC을 사전에 공유하고 있는 $SecretKey$로 암호화 하여 $E_{SecretKey}[AP_MAC]$을 생성한다.
ISP는 개인키로 AP_MAC을 전자 서명하여 이동 통신사 값인 $E_{ISP_pr}[AP_MAC]$을 생성한다.

⑥ Client는 $D_{SecretKey}[AP\_MAC]$, $D_{ISP_pu}[AP_MAC]$과 같이 ISP 에게 받은 값을 복호화 하여 두 값이 일치하는지 확인한다. 두 값이 일치한다면 $E_{CA_Pu}[ISP_Certificate]$과 같이 암호화한 값을 생성하여 CA에게 인증 요청을 한다.
Client는 ISP로부터 전송 받은 $E_{SecretKey}[AP_MAC]$을 $SecretKey$로 복호화 한다.
Client는 ISP로부터 전송 받은 $E_{ISP_pr}[AP_MAC]$을 ISP의 공개키로 복호화 한다.
Client는 CA에게 ISP로부터 받은 이동 통신사 정보가 CA에 등록되어 있는 정보와 일치하는지 여부를 확인하기 위해 CA의 공개키를 이용하여 암호화한 $E_{CA_Pu}[ISP_Certificate]$을 생성하여 인증 요청을 한다.

⑦ CA는 $D_{CA_Pr}[ISP_Certificate]$와 같이 복호화 하여 등록되어 있는지 일치 여부를 확인하고 $E_{C_Pu}[ISP_Certificate]$과 같이 암호화한 값을 생성하여 Client에게 확인 응답을 전송한다.
CA는 Client로부터 받은 $E_{CA_Pu}[ISP_Certificate]$을 개인키로 복호화 한다.
CA는 Client의 공개키를 이용하여 암호화한 $E_{C_Pu}[ISP_Certificate]$을 생성하여 Client에게 전송한다.

⑧ Client는 다음 $D_{C_Pr}[ISP_Certificate]$과 같이 복호화 하여 이동 통신사 정보 일치 확인 값일 경우 AP에 접속을 한다.
Client는 CA로부터 전송 받은 $E_{C_Pu}[ISP_Certificate]$을 개인키로 복호화 한다.

4. 구현 및 비교 분석

4.1 구현 환경

본 논문에서 제안하는 기법의 성능 평가를 위해 구현된 시스템은 OPNET v14.5와 Visual C++ 6.0을 이용하여 시뮬레이션 및 구현하였고, 데이터의 암·복호화는 AES 대칭키 알고리즘과 공개키 기반 구조(Public Key Infrastructure: PKI)를 적용한 RSA 공개키 알고리즘을 사용하였고, 전자서명에는 SHA-1 해시 알고리즘을 사용하였다.

단말기의 연산능력은 현재 스마트폰으로 판매되고 있는 IPhone 3GS가 600Mhz~833Mhz 클럭을 지원하는 것을 감안해 850Mhz의 CPU로 설정하였고, 하드웨어는 Intel(R) Core(TM)2 Duo CPU E8400 3.00Ghz, RAM 2GB 환경에서 구현하였다.

4.2 구현

네트워크 시뮬레이터 툴인 OPNET을 이용하여 네트워크 구조를 설계하고 기존의 EAP-AKA 프로토콜과 본 논문에서 제안한 프로토콜을 비교분석 하였다.

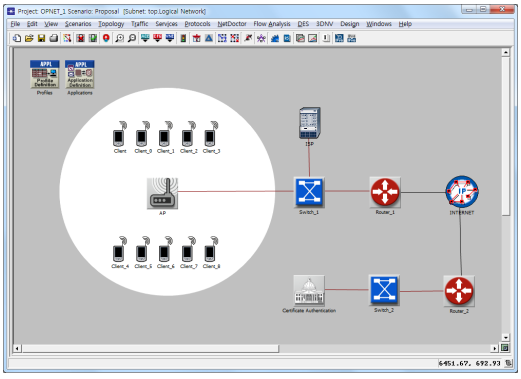
다양한 분석을 위해 어플리케이션 별 특성, 특정 망, 구간의 트래픽 등 다양한 트래픽을 측정하는 수동(passive) 측정 방식인 패킷 기반 방식을 사용한다. 이 방식은 측정지점에서 목적지까지 송·수신되는 모든 트래픽을 수집하는 방식이다.

시뮬레이션 하는 구간은 단말기와 AP 사이인 무선망의 전체 트래픽에 대한 지연율 및 처리율을 분석한다. 각 항목은 유·무선망 종단간 전체 트래픽에 대한 Delay(sec), Load(packets/sec), Throughput(packets/sec)와 AP, ISP, CA 단일 노드에 대한 Delay(sec), Load(packets/sec), Throughput(packets/sec)이 있다.

4.2.1 Network Modeling

[그림 4]와 같이 한 이동 통신사 AP내에는 무선 인터넷을 사용하기 위한 단말기가 존재하고, 이동 통신사 서버인 ISP와 신뢰기관인 CA가 존재한다.

각 단말기에서 어플리케이션 별로 트래픽을 발생시키며 단말기는 10명의 사용자를 가정하고 설정마다 각각의 시나리오를 구성하여 비교분석을 진행한다.

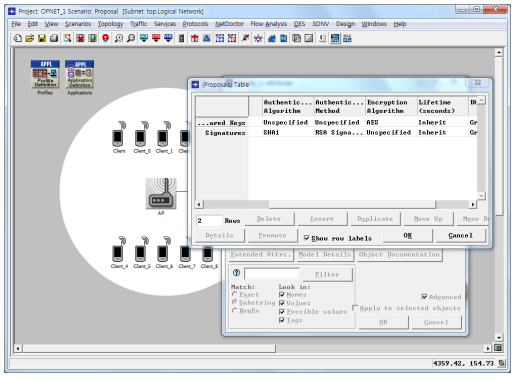


[그림 4] Network Model
[Fig 4] 네트워크 모델

4.2.2 암 · 복호화 모듈 설계 및 적용

OPNET에서는 각종 라이브러리를 C, C++ 컴파일러 기반으로 제공하고 있다. 보안 항목의 IPsec 설정에서는 Tunnel이나 Transport 모드를 위해 암호화 및 키 교환 알고리즘, 전자서명, 해시함수를 지원한다.

[그림 5]는 보안 항목에서 지원되는 암호화 모듈 목록을 나타낸다.



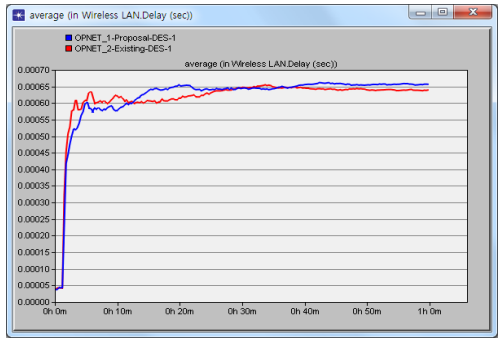
[그림 5] 암호화 모듈 정의
[Fig 5] cryptography Module

4.3 구현 결과

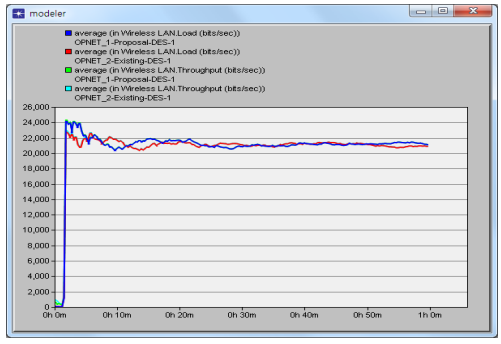
시뮬레이션 Parameter 항목으로 전체 트래픽을 분석하는 Global Statistics(Delay, Load, Throughput)와 각 노드의 오버헤드를 테스트하기 위해 단일 노드의 분석 값을 확인할 수 있는 Node Statistics(Delay, Load, Throughput)를 선택한다. DES Result Chart는 각 적용된 프로필의 결과 값의 그래프와 값을 나타낸다.

4.3.1 결과 차트1

[그림 6], [그림 7]은 전체 트래픽을 분석하는 Global Statistics(Delay, Load, Throughput) 시뮬레이션 차트를 나타낸다.



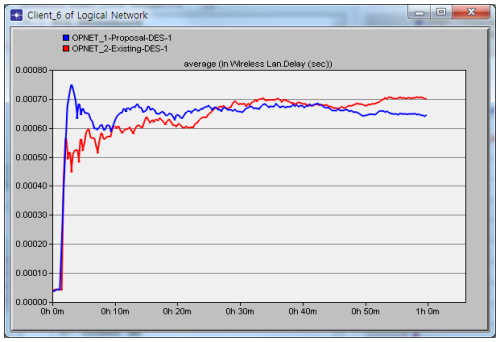
[그림 6] 전체 트래픽 분석 (Delay)
[Fig 6] Global Statistics (Delay)



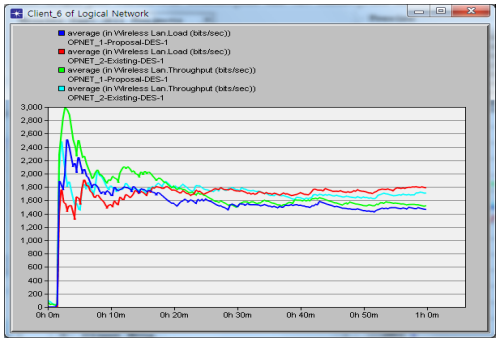
[그림 7] 전체 트래픽 분석 (Load, Throughput)
[Fig 7] Global Statistics (Load, Throughput)

4.3.2 결과 차트2

[그림 8], [그림 9]는 Client의 Node Statistic(Delay, Load, Throughput)을 비교분석 한 것을 나타낸다. 실험 결과 각 Client 마다는 미세한 차이가 있는 것으로 나타났다. 본 논문에서는 10명의 Client중 한명씩을 골라서 비교분석 하였다.



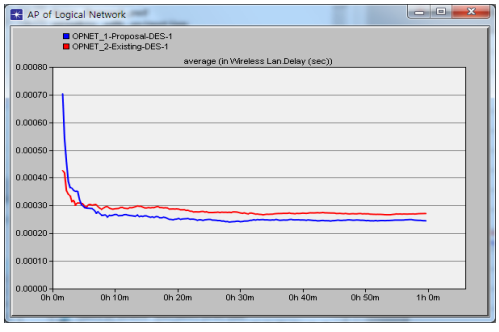
[그림 8] 클라이언트 노드 분석 (Delay)
[Fig 8] Client Node Statistic Compare (Delay)



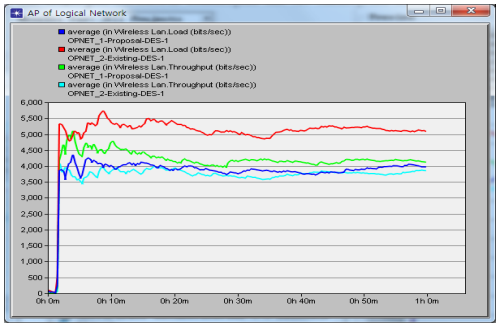
[그림 9] 클라이언트 노드 분석 (Load, Throughput)
[Fig 9] Client Node Statistic Compare (Load, Throughput)

4.3.3 결과 차트3

[그림 10], [그림 11]은 AP의 Node Statistic (Delay, Load, Throughput)을 비교분석 한 것을 나타낸다.



[그림 10] AP 노드 비교 분석 (Delay)
[Fig 10] AP Node Statistic Compare (Delay)



[그림 11] AP 노드 비교 분석 (Load, Throughput)
[Fig 11] AP Node Statistic Compare (Load, Throughput)

4.4 비교분석

4.4.1 분석결과 수치 분석1

[표 2], [표 3]은 제안하는 기법과 기존 기법의 전체 트래픽에 대한 시뮬레이션 분석결과 수치를 나타낸다.

전체 Wireless LAN 트래픽은 평균 Delay 0.0000173 (sec), 최대 0.0000445(sec), 최소 0.0000007(sec), 평균 Load 215(bits/sec), 최대 10769(bits/sec), 평균 Throughput 221(bits/sec), 최대 10769(bits/sec)로 비슷한 속도를 보여주었다.

[표 2] 제안하는 기법의 전체 트래픽 분석 결과
[Table 2] Global Statistic Summary (Delay, Load, Throughput)

Statistic (Proposal)	Average	Maximum	Minimum
Wireless LAN Delay(Sec)	0.0006566	0.0010221	0.0000380
Wireless LAN Load(bits/sec)	21,099	162,589	0
Wireless LAN Throughput (bits/sec)	21,105	162,589	0

[표 3] 기존 기법의 전체 트래픽 분석 결과
[Table 3] Global Statistic Summary (Delay, Load, Throughput)

Statistic (Existing)	Average	Maximum	Minimum
Wireless LAN Delay(Sec)	0.0006393	0.0010666	0.0000373
Wireless LAN Load(bits/sec)	20,884	151,820	0
Wireless LAN Throughput (bits/sec)	20,884	151,820	0

4.4.2 분석결과 수치 분석2

[표 4], [표 5]는 제안하는 기법과 기존 기법의 Client 단일 노드 분석결과 수치를 나타낸다.

10명의 Client 단일 노드에 대한 평균치를 계산하여 분석한 결과 CPU Utilization 0.001205(%), Delay 0.000010824(sec), Load 133.58(bits/sec) 증가하였고, Throughput 5.28(bits/sec) 감소하는 수치를 보였다.

[표 4] 제안하는 기법의 클라이언트 노드 분석 결과
[Table 4] Client Node Statistic Summary (Delay, Load, Throughput)

Statistic (Proposal)	Delay	Load	Throughput
Client	0.00066147	1,662.3	1,687.8
Client_0	0.00058543	1,928.2	2,028.5
Client_1	0.00062541	1,640.1	1,613.2
Client_2	0.00067106	1,648.5	1,855.7
Client_3	0.00064898	1,766.5	1,745.9
Client_4	0.00065545	1,629.5	1,581.4
Client_5	0.00066803	1,776.0	1,603.8
Client_6	0.00064409	1,463.7	1,516.7
Client_7	0.00070774	1,807.2	1,719.4
Client_8	0.00061998	1,806.6	1,631.3

[표 5] 기존 기법의 클라이언트 노드 분석 결과
[Table 5] Client Node Statistic Summary (Delay, Load, Throughput)

Statistic (Existing)	Delay	Load	Throughput
Client	0.00059930	1,352.0	1,407.8
Client_0	0.00060533	1,613.7	1,615.7
Client_1	0.00066883	1,867.4	2,002.2
Client_2	0.00060357	1,341.1	1,621.5
Client_3	0.00066890	1,540.9	1,692.6
Client_4	0.00068137	1,696.7	1,842.9
Client_5	0.00057613	1,602.2	2,000.7
Client_6	0.00070050	1,787.8	1,709.0
Client_7	0.00066077	1,437.4	1,511.7
Client_8	0.00061470	1,553.6	1,632.4

4.4.3 분석 결과 수치 분석3

[표 6], [표 7]은 제안하는 기법과 기존 기법의 AP 단일 노드 분석결과 수치를 나타낸다.

AP 단일 노드에 대한 분석 결과 Delay 0.00002609 (sec), Load 1120.8(bits/sec)만큼 감소하였으나 Throughput의 수치가 266.6(bits/sec) 증가하였다.

[표 6] 제안하는 기법의 AP 노드 분석 결과
[Table 6] AP Node Statistic Summary (Delay, Load, Throughput)

Statistic (Proposal)	Value
Wireless Lan Delay(sec)	0.00024476
Wireless Lan Load(bits/sec)	3,970.4
Wireless Lan Throughput(bits/sec)	4,121.3

[표 7] 기존 기법의 AP 노드 분석 결과
[Table 7] AP Node Statistic Summary (Delay, Load, Throughput)

Statistic (Existing)	Value
Wireless Lan Delay(sec)	0.00027085
Wireless Lan Load(bits/sec)	5,091.2
Wireless Lan Throughput(bits/sec)	3,854.7

4.4.4 암호학적 분석

제안 시스템은 기밀성, 무결성, 부인방지를 보장하며 사용자, AP, 이동 통신사 간의 상호 인증을 가능하게 하는 보안 기술을 적용하였다.

(1) 기밀성

제안 시스템은 Client에서 개인 정보 값인 $IMSI$를 ISP에게 전송할 때와 ISP에서 AP 정보 값인 AP_MAC을 Client에게 전송 할 때 서로 사전에 공유하고 있는 값을 이용하여 대칭키 암호화 알고리즘의 안전성을 기반으로 하기 때문에 기밀성을 보장한다.

(2) 무결성

ISP에서 Client에게 이동 통신사 정보 값인 $E_{ISP_pr}[AP_MAC]$을 전송 할 때 전자 서명을 사용하여 전송하는 값에 대한 인증, 무결성을 보장한다.

(3) 부인방지

Client는 이동 통신사 정보 값에 대해 CA에게 확인 요청, 응답 과정을 거치기 때문에 부인방지를 보장한다. 또한 ISP에서 이동 통신사 정보 값인 $E_{ISP_pr}[AP_MAC]$을 Client에게 전송할 때 사용되는 전자서명은 무결성 뿐만 아니라 부인방지도 보장한다.

5. 결론

본 논문에서는 IEEE 802.1x, EAP-AKA의 서비스 거부 공격, 스푸핑, 중간자 공격, Evil Twin Access Point 공격 등에 대한 취약성을 보완하여 강화된 인증과 안전한 서비스를 제공할 수 있는 신뢰기관 기반의 무선랜 보안 시스템을 제안하였다. 스마트폰의 급속한 이용증가와 무선랜 기술이 확산되는 시점에서 제안하는 시스템은 스마트폰 환경에서 사용자가 이동 통신사 AP 접속을 통하여 무선 인터넷을 이용할 때 USIM에 있는 사용자 고유정보와 AP 정보, 통신사 정보를 사용하여 사용자 인증, AP 인증, 통신사 인증을 함으로써 각종 공격에 대한 취약성을 보완하여 안전한 무선 네트워크 서비스 환경을 제공한다.

OPNET 시뮬레이터를 이용하여 기존 시스템과 제안 시스템의 전체 트래픽과 각 노드 간의 트래픽 성능분석 결과 전체 Wireless LAN 트래픽은 평균 Delay 2.7%, 평균 Load 1.1%, 평균 Throughput 1.1% 증가하였고, 나머지 각 노드 항목들의 증가, 감소수치가 전체적으로 비슷하게 나타났다. 하지만 제안 시스템은 암호학적 비교분석 결과 각종 공격으로부터 기존 시스템 보다 안전하다는 것을 확인하였다.

향후 연구방향으로는 이동 통신사 AP가 설치된 카페, 공공기관 등에 적용을 시키며, 각종 공격으로부터 안전하도록 보안강도를 증가시키되 인증시간을 단축 시켜 인증 시스템의 효율성 면에서 최선의 결과를 나타내는 추가적인 연구가 필요할 것 이다.

References

[1] Kang Bong-Geun, “A Study on Home Network Authentication using USIM caed", Daejeon University, 2010.02.

[2] Y.S.Kim, J.W.Lee, J.H.Han, J.A.Shin. S.I.Jun, “Trends of Interworking Security Technologies for the Wireless Networks", Electronics and Telecommunications Trends, 2005.02.

[3] Park DongHyun, “A Study on Intrusion Patterns and Countermeasures in Wireless LAN Environment", Graduate School of Industry & Technology Chonnam National University, 2006.08.

[4] H. Chaouchi, Securite Dans Les Reseaux Sans Fil Et Mo, “Wireless and Mobile Networks Security", Willey-Iste 2009.06.

[5] 3GPP TS 35.206 v9.0.0, 2009.12.

[6] Hoyoung Hwang, Namyun Kim, "Personal Information Protection System for Web Service", Journal of The Institute of Webcasting, Internet and Telecommunication, VOL.11, No.6, pp. 267-273, December, 2011.

[7] YeWang, Xiao-LeiZhang, WeiweiChen, Jang-Geun Ki, Kyu-Tae Lee, "Comparative study of an integrated QoS in WLAN and WiMAX", Journal of The Institute of Webcasting, Internet and Telecommunication, VOL.10, No.3, pp. 103-110, June, 2010.

[8] Eun Cheol Kim, Seo Sung Il, Jin Young Kim, "Performance of Tactics Mobile Communication System Based on UWB with Double Binary Turbo Code in Multi-User Interference Environments", Journal of The Institute of Webcasting, Internet and Telecommunication, VOL.10, No.1, pp. 39-50, February, 2010.

[9] Ju phil Cho, Sang-In Cho, Kyu-Min Kang, Heon-Jin Hong, "Analysis on Characteristics for Sharing Co-channel between Communication Systems", Journal of The Institute of Webcasting, Internet and Telecommunication, VOL.11, No.4, pp. 251-256, August, 2011.

[10] Young-Hoon Choi, Yoon-Hyun Kim, Jin-Young Kim, Jung-Hoon Lee, Jae-Sang Cha, "Comparison of Spectrum Sensing Algorithms for Cognitive Radio Systems", Journal of The Institute of Webcasting, Internet and Telecommunication, VOL.11, No.4, pp. 195-201, August, 2011.

이 기 성(Gi Sung Lee) **[정회원]**

- 1996년 8월 : 숭실대학교 컴퓨터학과 (공학석사)
- 2001년 8월 : 숭실대학교 대학원 컴퓨터학과 (공학박사)
- 2001년 9월 ~ 현재 : 호원대학교 컴퓨터게임학부 교수

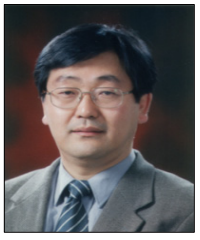
<관심분야>
정보통신, 통신보안, 암호이론

민 대 기(Dae-Gi Min) **[정회원]**

- 2009년 2월 : 숭실대학교 전산원 인터넷통신학과 (학사)
- 2011년 2월 : 숭실대학교 일반대학원 통신 (공학석사)
- 2011년 3월 ~ 현재 : 숭실대학교 일반대학원 통신 (박사과정)

<관심분야>
정보통신, 통신보안, 암호이론

전 문 석(Moon-Seog Jun) **[정회원]**



- 1989년 2월 : University of Maryland Computer Science 공학박사
- 1989 ~ 1991년 : New Mexico State University physical Science Lab 책임 연구원
- 1991년 ~ 현재 : 숭실대학교 정교수

<관심분야>
인터넷 보안, 멀티미디어 보안, 인증 시스템