무선랜 환경에서의 서버/클라이언트 보안통신 모듈 설계

전준상, 조명휘, 소우영
한남대학교 컴퓨터공학과

Design of Server/Client Security Communication Module on Wireless LAN

Jun-Sang Jeon, Myeong-Hwi Jo, Woo-Young Soh
Dept. of Computer Engineering, Hannam University

요 약

최근 용이한 이동성등의 장점으로 기존의 유선랜을 대체하고 있는 무선랜은 AP(Access Point)와 단말기 사이의 보안상 많은 취약성을 갖고 있다. 예를 들어, 동일한 AP에 접속한 공격자에 의해 스니핑된 패킷에서 원본 데이터를 추출 할 수 있는 문제점이 제기되었다. 본 논문에서는 무선랜 환경에서 세밀한 보안이 요구되는 서버/클라이언트 통신 시 스니핑에 의한 원본 데이터의 유출을 방지하여, 안전한 서버/클라이언트 통신이 가능한 보안 통신모듈을 설계하였다. 이 모듈을 사용할 경우 스니핑에 의해 패킷 데이터가 유출되어도 키 없이는 원본 데이터의 내용을 볼 수 없는 장점이 있다.

1. 서론

현재 인터넷 기술은 개인 또는 기업의 사용자들에게 보다 빠르고 편리하게 이용할 수 있는 최적의 환경을 제공하기 위한 방향으로 발전하고 있다. 이미 빠르고 안정적인 서비스를 제공하기 위해 전용회선, xDSL 등 다양한 고속의 인터넷 서비스가 등장하였다. 그러나 유선랜의 관리나 추가에 관한 기회비용 등을 고려하여 볼 때, 무선랜의 구축을 채택하고 있는 기업과 사용자의 수가 증가하고 있는 추세이다. 현재 무선망은 관공서, 학교, 기업 등의 사설무선랜과 개인이 이용할 수 있는 공중 무선랜 서비스인 넷스팟이나 스카이윈 등이 있다. 무선랜은 무선 AP(Access Point)와 무선 클라이언트 사이의 무선 통신에 의하여 데이터를 교환한다. 이러한 무선랜의 통신구간은 개방되어 있어 네트워크의 최대 관심사인 보안에 있어서는 유선랜에 비하여 매우 취약하다. 유선랜은 전송 신호가 유선이라는 한정된 물리 매체에서만 존재하므로 강력한 물리-접근 제어로 보호할 수 있다. 하지만 무선랜의 전송 매체는 전파이므로 수신기가 영역 내에 있으면 누구라도 접근 할 수 있도록 설계되어 있으므로 네트워크 스니핑에 완전히 노출되어 있다. 본 논문에서는 이러한 801.11 무선랜의 보안 취약점에 대하여 분석하고 Server/Client간의 보안 통신모듈을 이용하여 통신데이터를 보호하는 방법을 설계하였다. 2장에서는 무선랜의 전반적인 내용에 대해 설명하고 3장에서는 무선랜 환경에서의 보안기법 및 보안취약점에 대해 설명한다. 4장에서는 Server/Client간의 보안통신 모듈을 설계하였다.

본 연구는 과학기술부 지역협력연구사업
(R12-2003-004-01002-0) 지원으로 수행되었음

2. 무선랜의 구성

2.1 무선랜이란

무선랜(Wireless Local Area Network)이란 네트워크가 구축된 실내 또는 실외에서 클라이언트가 별도의 물리적인 매체 없이 무선으로 네트워크에 접속할 수 있는 환경을 말한다. 기본적인 무선랜 네트워크는 다른 무선 단말기나 유선랜으로 연결하기 위해 각 단말기 내에 설치되는 무선 NIC(Network Interface Card), 각 단말기와 유선랜간의 게이트웨이 역할을 담당하는 AP(Access Point), 그리고 건물과 건물 또는 분산된 네트워크 세그먼트 사이를 점-대-점 방식으로 연결하는 데 사용되는 무선 브리지 장비로 구성된다. 기술적으로 AP에서 무선랜어댑터까지 유선대신 RF전파나 적외선을 이용해서 네트워크를 구축하는 방식을

뜻하며, 일반적으로 30-150미터 정도의 거리에서 무선으로 1~54Mbps의 데이터를 고속으로 전송하는 네트워크를 가리켜 무선랜이라고 부르고 있다. 무선랜은 점차적으로 유선랜의 중요한 대체 매체로 되어가고 있으며, 이동성, 재배치성, 각 터미널간에 일시적으로 형성되는 Ad-Hoc 네트워킹 접속, 유선랜이 접속할 수 있는 허용 거리 등을 만족한다.

표 1 무선랜의 장단점

장점	단점
효율성	전파간섭
확장성	보안문제
이동성	
비용절감	

2.2 무선랜의 전송방식

미국 전기전자공학회(IEEE)의 802.11 표준안[1]은 무선랜의 국제 표준으로 인식되고 있으며, FHSS, DSSS의 두 가지 전송방식을 허용한다. 전파는 원형 형태로 공기를 통해 퍼져나간다. 무선랜 기술은 스프레드 스펙트럼 방식(Spread Spectrum-based)의 무선 커뮤니케이션 방식을 사용한다. 스프레드 스펙트럼 방식은 노이즈 캐리어 웨이브(Noise-like carrier wave)를 사용하여 원래 시그널보다 큰 대역폭에 퍼지도록 하기 위해서 시그널 안에 정보를 담아 보내는 방식을 사용한다. 큰 대역폭에 시그널을 실어 보내는 것이 표준 point-to-point 커뮤니케이션에 비해 데이터 비율 증가를 요구하지만 반면에 방해 전파를 더 잘 견디고 중간에 가로채거나 발견하는 것을 어렵게 하고 전파 전송 범위를 조절할 수 있었다.

표 2 무선랜의 전송 방식

	FHSS	DSSS
전파간섭	자동주파수변환 더욱 높은 투과력	수동 조작
확장성	시스템 수용량을 15배로 확장.	시스템 수용량의 3배까지 가능.
다중채널시스템	채널간 로밍가능.	로밍기능 없음.
실효범위	주파수 Hopping은 다중경로 효과로 최소화함.	다중경로 효과를 줄이기 위해 무선국을 이동해야함.

2.3 무선랜의 구성

무선랜은 유선랜과 독립적으로 무선 NIC를 장착한 복수의 단말기들끼리 단독으로 연결하는 Ad-Hoc망과 AP를 통해 단말기를 유선랜에 연결하는 Infra Structure 망방식으로 구성할 수 있다. Ad-Hoc 망은 일시적으로 형성되는 작업그룹 등에서 주로 사용하며, Infra Structure망은 유무선 연결장치인 AP를 통해서 무선 단말을 기존 유선랜에 연결한다. 이 때 AP를 중심으로 무선 셀 BSS(Basic Service Set)가 형성되는데, AP는 BSS내에 있는 모든 단말기들을 LAN에 연결하는 셀룰러 폰 기지국과 동일한 역할을 수행한다. 서로 중첩하지 않는 채널을 사용하는 여러 BSS를 모아 하나의 ESS(Extended Service Set)를 구성할 수도 있는데, 동일 ESS내의 서로 다른 BSS간에는 로밍에 의해 단말기의 이동이 가능하다.

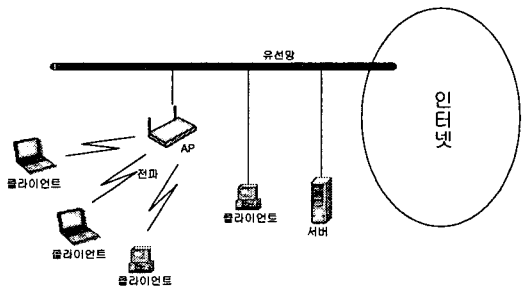


그림 1 무선랜의 구성

3. 무선랜 환경의 보안취약점 및 보안기법

3.1 무선랜 보안의 정의

무선랜 보안을 위한 요소는 유선랜 환경의 일반적인 보안 시스템이 지니는 것과 유사하다. 일반적인 보안 요소는 사용자 인증(Authentication), 접근제어(Access control), 권한 검증(Authorization), 데이터 기밀성(Privacy), 데이터 무결성(Integrity), 부인방지(Non-repudiation), 안전한 핸드오프(secure hand-off)로 정의할 수 있다. 정의한 결과는 표 3과 같다.

표 3 무선랜 보안요소

보안 요소	내용
사용자 인증	정당한사용자에 의한 정당한 인증.
접근제어	정당한사용자에 의한 정당한 접근.
권한 검증	정당한사용자에 의해 허가된 권한.
데이터 기밀성	정당한 데이터의 비밀 보장.
데이터 무결성	데이터의 훼손 없이 정당한 데이터 전달.
부인방지	전달된 데이터에 대한 수신 사실 부인 방지.
안전한 핸드오프	이동중인 사용자가 정당한 데이터를 비밀성이 보장되면서 중간에 훼손 없이 전달.

3.2 무선랜의 보안기능

먼저 가장 간단한 방법의 보안으로 MAC필터링이 있다. MAC필터링이란 기존의 유선랜에서와 같이 MAC주소를 이용하여 합법적인 클라이언트와 비합법적인 클라이언트를 구별하는 가장 간단한 방법이기는 하나 많은 허점을 가지고 있다. 프로토콜 필터링은 클라이언트의 접속을 제한하지는 않지만 위험을 줄일 수 있는 다른 방법이다. 그러나 필터링 룰을 정의하는데 매우 세심한 주위가 필요하다. 프로토콜 필터링이란 네트워크의 자원을 독점하거나 생산성에 나쁜 영향을 초래하는 트래픽을 제한하는 것을 말한다. 다른 의미로 공격자가 네트워크에 접속하여 많은 트래픽을 가중시켜 일종의 DOS공격과 같은 효과를 사전에 차단할 수 있는 방법이기도 하다. WEP(Wired Equivalent Privacy)인증은 두 가지 보안기능(비밀, 승인)을 제공한다. WEP기능은 전송 정보를 암호화하여 보내고, 암호 키를 가진 수신기만이 전송정보를 해독할 수 있다. WEP은 암호화 없음, 40비트 암호화, 128비트 암호화의 형태로 보안기능을 제공한다. 40비트 암호화 또는 128비트 암호화는 RC4 알고리즘에 의하여 클라이언트와 AP 사이에 전송되는 데이터를 암호화하는 것을 말한다. 그러나 RC4 암호화는 이미 1995년도에 깨어진 알고리즘이다. 폐쇄 시스템 설정은 클라이언트가 AP를 찾을 때 마치 존재하지 않는 것처럼 보이게 하는 것을 말한다. 클라이언트가 AP에 연결하기 위해서는 일반적으로 "any"라는 SSID를 가지고 허가 요청을 보낸다. 폐쇄 시스템에서는 "any"라는 SSID를 가진 클라이언트에게 응답하지 않거나 SSID를 클라이언트에게 브로드캐스트 하지 않도록 설정하는 방식이다. 기타 방식으로는 RADIUS인증, EAP-TLS인증, EAP-TTLS인증, EAP-SRP인증, EAP-MD5인증 등이 있다[2][3].

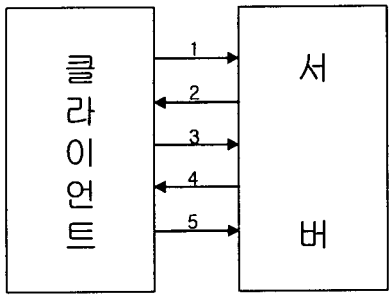
3.3 무선랜의 보안취약점

현재의 무선랜이 가지는 보안요소는 접근제어와 데이터의 기밀성 지원에 중점을 두고 있다. 접근제어는 사용자 인증을 통해 이루어지며 크게 3가지 방법이 있다. 첫째, 허가 받는 사용자와 AP가 동일한 공유키를 보유하여 접속 요청 시 공유 키 인증방식을 사용하는 방법, 둘째, 허가 받은 사용자의 무선랜카드 MAC주소를 AP에 직접 입력시켜 놓은 방법, 마지막으로 허가 받은 사용자가 자신의 인증정보를 가지고 인증서버와 인증절차를 수행하는 IEEE 802.1x인증 방법이다. 데이터 기밀성은 WEP알고리즘을 사용하여 지원되는데 이미 깨어진 알고리즘을 사용함으로써 현재의 무선랜 보안기능은 전면적으로 보완되어야 한다. 각각의 취약점을 살펴보면 모든 침입이나 공격의 시작점인 AP가 누구나 검색 가능하다는 점이다. AP는 NetStumbler라는 프로그램을 이용하면 정확한 위치까지 검색이 가능하다. 물론 패쇄시스템의 AP는 검색이 불가능하지만, 구축 시 설정해줘야 하고 사용자에게 불편을 주는 점이 문제가 된다. 그리고 MAC주소를 복제하여 침입하는 방식이다. MAC주소는 고유한 키 값이지만 얼마든지 복제가 가능하다. WEP도 취약점을 가지고 있는데 데이터를 스니핑하면 이미 깨어진 알고리즘이고 상용툴도 많이 나와 있는 실정이기 때문에 얼마든지 데이터를 수집할 수 있기 때문이다. 또한 데이터의 스니핑이 문제가 된다. 유선에서의 스니핑은 네트워크를 구성하는 물리적 전송 매체에 흐르는 패킷을 수집하는 형태를 말한다. 유선에서는 리피터나 허브 등의 장비에 연결해야 데이터를 수집할 수 있지만, 무선에서는 전파를 이용하기 때문에 네트워크 모니터링툴을 이용하면 손쉽게 데이터를 수집할 수 있게 된다.

4. Server/Client 간의 보안통신모듈 설계

본 논문에서 설계하고자 한 통신모듈은 유닉스 기반 시스템에서 사용하는 SSH통신모듈[4]과 유사하다. 그러나 SSH는 유닉스환경이라는 단점이 존재하기 때문에WINDOWS 기반의 환경에서 SSH통신모듈과 유사한 환경을 제공하며, 무선랜 환경에서의 데이터 스니핑을 원천적으로 봉쇄하는 것이 아니라 스니핑을 하여도 원본 데이터를 볼 수 없도록 하는 것에 목표를 두었다. 전체적인 구성을 보면 서버와 클라이언트 사이에서의 통신은 서버의 에이전트와 클라이언트의 에이전트가 담당한다. 서버의 에이전트는 데이터가 인증된 사용자의 데이터인지 파악하고, 데이터를 암호화, 복호화 하여 송수신하기 위해 사용되며 암호화키 리스트를 관리하게 된다. 클라이언트의 에이전트는 송수신 데이터를 암호화, 복호화하고 암호화키 리스트를 관리한다. 통신과정을 살펴보면 클라이언트는 최초에 서버 측에 접속을 요청하게 되고 서버는 적합한 사용자인지 파악한 후 승인과 함께 생성한 암호화키 리스트를 에이전트에 저장하여 다운로드 링크를 에이전트에 알려준다. 클라이언트는 에이전트를 다운로드받아 설치한 후 서버에 접속하면 서버는 암호화키 리스트 중 사용할 암호화키의 인덱스 번호를 클라이언트에게 알려주고 두 암호화키가 동일한 키인지 알아보기 위

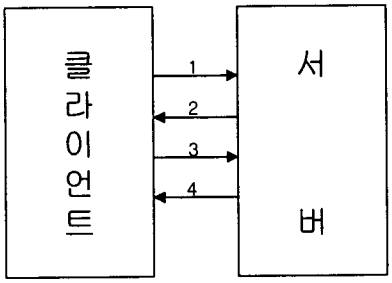
해 테스트 데이터를 전송한다. 전송한 데이터가 동일한 값인지 확인한 후 서버와 클라이언트는 통신을 실행한다.



1 접속요청
2 사용자확인
암호화키 리스트
에이전트 전송
3 에이전트 설치
암호화키 인덱스전송
4 테스트데이터생성전송
5 데이터확인후 통신시작

그림 2 서버와 클라이언트 통신순서

서버와 클라이언트는 정기적으로 암호화키의 인덱스를 회전시킨다. 전용프로토콜을 사용하여 서버나 클라이언트 양쪽에서 요청에 의해 이루어진다.



1 키교환요청
2 요청승인
새로운 암호화키인덱스전송
4 테스트데이터생성전송
5 데이터확인후 통신시작

그림 3 암호화키의 회전 순서

암호화된 데이터패킷은 다른 무선랜에서 사용하는 일반적인 무선랜의 패킷 모양과 같지만 패킷의 내용 부분에는 암호화된 데이터가 들어가 있기 때문에 스니핑을 하여 데이터를 추출하여도 암호화된 데이터이기 때문에 원본 데이터의 추출을 막을 수 있다.

5. 결론 및 향후 연구 과제

무선랜은 사용자들에게 많은 편리함을 제공한다. 본 논문에서는 편리함 되에 숨겨진 무선랜의 보안 취약성에 대하여 논의하고 스니핑이란 취약성의 대처방안에 대한 보안통신모듈을 설계하였다.

무선랜의 신뢰성을 위해서는 AP와 단말기사이의 보안에 더욱 신경을 써야 하지만 본 논문에서 설계한 통신모듈을 사용하여 비용을 줄일 수 있을 것이다.

이러한 모듈을 사용하게 되면 서버나 클라이언트 측에서의 데이터 송수신에 많은 부하가 걸릴 수도 있다. 그러한 문제점을 보완하여 더욱 완벽한 보안통신모듈을 설계하여야 하는 것이 추후 연구 과제이다.

6. 참고문헌

[1] ANSI/IEEE Std 802.11, "Wireless LAN Medium Access Control(MAC) and Physical Layer(PHY) Specifications," 1999.

[2] C. Rigney, "Remote Authentication Dial In User Service(RADIUS)," IETF RFC 2865, June 2000.

[3] D. Nessett, "Serial Authentication Using EAP-TLS and EAP-MD5," IEEE, 802.11-01/400r22, July 2001.

[4] http://kdsoo.com/file/seminar/4/ssh.pdf