情報保護學會論文誌
第14券 第5號, 2004. 10

DoS 공격에 강한 무선 랜 인증 프로토콜

김 민 현†, 이 재 욱‡, 최 영 근, 김 순 자
경북대학교

DoS-Resistance Authentication Protocol for Wreless LAN

Min-Hyun Kim†, Jae-Wook Lee‡, Young-Geun Choe, Soon-Ja Kim
Kyungpook University

요 약

무선 랜은 액세스 포인트를 경유하여 인터넷을 사용할 수 있기 때문에 접근 제어의 중요성을 가지고 있다. 또한 무선 랜을 이용하기 위해서는 EAP의 인증과정을 거치게 된다. 이러한 액세스 포인트 접근과 인증 과정에 대한 치명적인 공격 중의 하나가 DoS(Denial of Service) 공격이다. 즉 악의적인 공격자가 액세스 포인트의 접근을 막거나 또는 인증 과정에서 서버의 메모리 및 중앙처리장치의 계산 능력 등을 강제적으로 소비시킴으로써 합법적인 사용자가 서비스를 받지 못하게 한다. 본 논문에서는 무선 랜에 대한 DoS 공격을 접근 제어, 자원의 할당, 인증프로토콜 상에서의 공격으로 나누어 각 공격에 대한 방어법을 제시하였다. 액세스 포인트 접근에 대한 문제는 사전 검증 단계 및 보안 수준 변수에 의해, 자원의 할당에 대한 공격은 부분적인 stateless 프로토콜에 의해, 프로토콜상의 약점은 타임스템프와 접근 제한 변수에 의해 개선하였다.

ABSTRACT

A Wireless Lan has an importance of access control, because we can use wireless Internet via AP(Access Point). Moreover, to use wireless LAN, we will go through authentication process of EAP. DoS(Denial of Service) attack is one of the fatal attack about these AP access and authentication process. That is, if malicious attacker keeps away access of AP or consumes memory of server and calculation ability of CPU and etc. compulsorily in authentication process, legal user can't get any services. In this paper, we presents the way of protection against the each attack that is classified into access control, allocation of resource, attack on authentication protocol. The first thing, attack to access control, is improved by pre-verification and the parameter of security level. The second , attack of allocation of resource, is done by partial stateless protocol. And the weak of protocol is done by time-stamp and parameter of access limitation.

Keywords : *DoS attack, Wireless LAN, authentication*

Ⅰ. 서 론

PDA나 휴대폰 등 무선 인터넷 기술이 발달함에 따라 무선 인테넷을 통하여 상거래, 정보 교환, 실시간 증권 거래, 금융 업무 등 서비스 등의 이용이 증가하고 있다. 최근 무선 인터넷을 이용하기 위하여 많이 사용되고 있는 무선 랜은 액세스 포인트를 통하여 단말기의 인증이 이루어지므로 액세스 포인트에 대한 접근제어의 중요성을 가진다. 이러한 접근 제어를 방해하는 치명적인 공격중의 하나가 DoS

접수일 : 2004년 1월 20일 ; 채택일 : 2004년 8월 26일
* 본 논문 연구는 한국과학재단 지역대학(R05-2003-12083-0) 지원으로 수행하였습니다.
† 주저자 : bahn@palgong.knu.ac.kr
‡ 교신전자 : llkkllkk@palgong.knu.ac.kr

(Denial of Service) 공격이다.

DoS 공격은 악의적인 공격자가 서버의 하드용량, 메모리 등의 자원을 고갈 시켜 합법적인 사용자가 서비스를 받지 못하도록 하는 공격이다[1].일반적인 프로토콜에서는 이러한 문제를 해결하기 위해서 프로토콜의 초기부분에 인증 과정을 두어 인증이 완료된 사람만이 서버의 자원(resource)에 접근하도록 하고 있다. 그러나 인증 프로 보통의 프로토콜보다 더 많은 계산 량과 메모리 등의 자원을 필요로 한다[2]. 따라서 악의적인 공격자에 의해 인증 프로토콜에 대한 DoS 공격이 행하여 질 수 있다.

무선 랜 인증 프로토콜 상에서의 DoS 공격의 취약성은 크게 세 부분으로 나누어서 생각할 수 있다. 먼저 프로토콜을 진행하면서 할당되는 자원에 의한 DoS 공격의 위험이 있다. 공격자가 인증 서버의 자원을 무한히 할당받도록 하여 자원을 소비함으로써 합법적인 사용자가 서비스를 받지 못하게 하는 방법이다. 또한, 인증 과정의 구조적인 원인에 의한 DoS 공격의 취약점이 있다. 기존의 인증 프로토콜은 사용자가 인증을 요구하면 사용자에 대한 확인 없이 서버의 자원을 할당하고 인증 프로토콜을 진행하게 된다[2]. 따라서 악의적인 공격자에게도 자원을 할당하게 되는 문제점이 있다. 마지막으로 프로토콜상의 문제점이 있다. 기존의 인증 프로토콜의 표준에서는 패킷의 잃어버림 등이 발생할 때 올바른 패킷이 전송 되도록 하기 위해서 재전송을 보장하고 있다[3]. 이점을 이용하여 악의적인 공격자가 고의적으로 잘못된 패킷을 전송하거나 패킷을 잃어버림으로써 서버의 자원을 소모시킬 수 있다.

본 논문에서는 무선 랜 인증 프로토콜 진행 변수를 프로토콜의 진행 과정에서 데이터와 함께 보내는 stateless 프로토콜을 적용하여 자원의 할당에 의한 공격의 위험을 줄였다[4]. 인증 구조에 의한 위험은 사전 검증단계를 두어서 사용자가 먼저 자신의 자원을 할당하여 사전 검증과정을 하도록 인증구조를 변화 시켰으며, 마지막으로 프로토콜상의 문제점을 해결하기 위해서 접속을 제한하는 접속 제한 변수, 타임 스템프를 인증프로토콜에 적용하였다.

본 논문의 구성은 다음과 같다. 2장에서는 기존의 무선 인증 프로토콜과 문제점에 대해서 살펴본다. 3장에서는 이런 문제점을 해결한 프로토콜을 제안하고 4, 5장에서는 제안하는 프로토콜의 안정성과 효율성을 분석한 뒤 6장에서 결론을 맺는다.

II. 기존의 무선 랜 인증 프로토콜

802.1x에서는 무선 랜에서 단말기와 인증 서버간의 인증 기법과 무선 접속구간 보안에 필요한 마스터 세션 키를 생성하는 방법을 정의한다. 또한 EAP를 인증을 위한 데이터 전송의 표준 프로토콜로 사용하고 있다.

이러한 EAP 인증 프로토콜 진행단계를 살펴보면, 최초 단말기가 액세스 포인트를 통하여 인증 서버에 인증 요청을 보내게 되고, 인증서버는 단말기에 아이덴터티를 요청한다. 단말기는 이 요청에 대하여 응답만 하면 인증 및 키교환 프로토콜이 바로 실행된다. 따라서 악의적인 공격자의 무차별적인 인증 요청에 대한 대책이 없다. 즉 액세스 포인트를 통한 인증서버에 대한 접근 제어의 문제점을 가진다.

또한 프로토콜이 진행됨에 따라 서버는 프로토콜의 진행 과정에 필요한 클라이언트의 아이덴터티 등 필요한 파라미터의 값 등의 상태 변수(state)를 저장한다[4]. 악의적인 공격자가 프로토콜 시작을 반복적으로 요청한 뒤 그 연결을 완전히 끝내지 않는 상태로 놓아둔다면 자원은 계속해서 소비하게 될 것이고 따라서 다른 합법적인 사용자들이 서비스를 받지 못하게 된다[2]. 근본적으로 이런 일이 발생 할 수 있는 원인은 처음 프로토콜을 시작할 때 상대에 대한 정확한 인증 없이 처음부터 익명의 사용자에게 자원을 할당하는데 있다.

현재 표준화 중인 EAP 인증 프로토콜은 EAP-MD5, EAP-SRP[9], EAP-TLS, EAP-TTLS[8], 가 있으며 각각의 특징은 다음과 같다. EAP-MD5는 단방향의 단말기 인증만 가능하며 마스터 키 생성이 이루어지지 않는다. 마스터키 생성 과정이 TLS에 기반을 두는 EAP- TLS는 상호 인증시 단말기와 인증서버 모두 자신의 인증서를 사용한다. EAP-TLS의 확장이라할 수 있는 EAP-TTLS는 인증 서버가 단말기를 인증할 때 단말기의 인증서를 사용하게 되는데 이러한 인증서의 부담을 줄이기 위해서 패스워드를 사용한다. 또한 EAP-SRP는 단말기와 인증서버 모두 패스워드를 이용한다[5].

위의 인증 프로토콜 중 EAP-SRP 및 EAP-TTLS는 기본적으로 사용자의 패스워드를 서버가 저장하여야 하므로 서버는 인증 프로토콜과 관계없이 자원을 할당하여야 한다. 또한 EAP-TLS나 EAP-TTLS 방식의 무선 랜 인증 프로토콜은 공개키 암호 시스템을 기반으로 하기 때문에 많은 계산량과 자

표 1. 기존의 무선랜 인증 프로토콜 비교

구 분	서버의 단말기 인증	단말기의 서버 인증	키 생성	접근 제어의 문제점	서버의 자원할당		재전송에 대한 DoS 공격
					인증프로토콜 실행전	인증프로토콜 실행중	
EAP-MD5	Password	no	불가능	o	사용자의 Password	요청시 무조건적 할당	o
EAP-SRP	Password	Password	가능	o	사용자의 Password	요청시 무조건적 할당	o
EAP-TLS	Certificate	Certificate	가능	o		요청시 무조건적 할당	o
EAP-TTLS	Certificate	Password	가능	o	사용자의 Password	요청시 무조건적 할당	o

원의 할당이 필요하다[2]. 따라서 악의적인 공격자가 인증 프로토콜 실행 과정 중 연속적인 재전송을 시도한다면 서버는 단말기의 인증을 위해 계속적인 연산이 실행된다. 또한 종료되지 않은 상태로 프로토콜의 연결 상태를 유지하기 위해서 서버는 자원을 할당해야 한다. 따라서 재전송에 대한 제한을 가할 수 있는 효율적인 인증 프로토콜 설계가 필요하다. 표 1은 기존의 무선랜 인증 프로토콜의 특징과 DoS 공격에 대한 위험 요소를 나타낸다.

Ⅲ. 프로토콜 설계

무선랜에서 적용될 수 있도록 EAP를 기반으로 하고 크게 인증 초기단계와 인증 실행 단계 그리고 최종단계 세부분으로 나누어 살펴본다. 표 2는 사용될 기호들의 정의를 나타낸 것이다.

3.1 인증 초기단계

3.1.1 보안 수준 변수 k

기존의 EAP 인증 프로토콜에서는 단말기의 인증을 위해 먼저 인증 서버가 사용자의 아이디(identity)를 요청하는 메시지를 보내면서 프로토콜이 시작된다. EAP-TLS의 경우 사용자는 자신의 아이디를 액세스 포인트를 거쳐서 인증 서버에 보내고 되고 이 후 그림 1과 같은 인증 및 키 교환 과정을 거치게 된다. with warrant) 대리 서명 프로토콜에 대해서 살펴본다[3,4].

단말기가 서버에 보내는 2번 메시지에서 단말기의 난수를 보내게 되고 서버는 단말기의 인증 및 키 교환을 위하여 3번 메시지를 단말기로 보내게 된다. 이때 서버는 자신이 생성한 난수, 모듈 값, 공개 키 값을 계산하고 서명한 값을 단말기에 보내게 된다. 이러한 인증과정에서 악의적인 공격자가 계속적인 접근 요청과 함께 난수를 서버에 보내게 되면, 인증 서버는 요청에 대한 불필요한 암호학적 연산을 계속적으로 행하게 된다. 따라서 이러한 인증 및 키 교환 과정에서 보다 능동적인 대처 방안이 필요하다. 즉 인증서버가 인증 요청에 대하여 제어를 할 수 있는 방법이 필요하다.

이러한 문제점을 해결하기 위해 인증 서버는 사용자에게 간단한 문제(puzzle)을 내고 사용자는 그 문제를 해결할 경우에만 인증 프로토콜을 실행하게 한다. 문제의 구조는 다음과 같이 구성된다.

표 2. 파라미터

기 호	설 명	기 호	설 명
ID_P	사용자의 아이덴터티(identity)	$h()$	해쉬함수
k, l	보안 수준 변수, 접근 제한 변수	$E_K()$	키 값이 K인 대칭키 암호함수
$state_V$	V의 프로토콜 진행에 필요한 설정값	X	사전검증에 사용하는 값
$Cert_M$, T_V	M 객체의 인증서, 타임스템프	v, c	서버 및 사용자의 비밀키
K_A	인증 서버의 대칭 비밀키	$h_K()$	키가 K인 해쉬함수
K_{AP}	사용자와 서버 사이에 만들어지는 세션키	r_a, r_c	서버와 사용자가 생성하는 랜덤변수

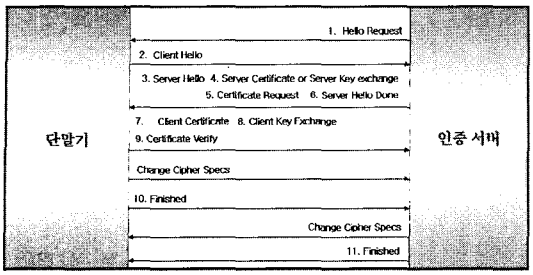


그림 1. EAP-TLS 인증 및 키 교환 프로토콜

$$h(ID_C, N_S, N_C, X) = 00\cdots\cdots00Y$$

N_C는 사용자의 난수, N_S는 서버의 난수를 나타내며, Y는 해쉬한 값에서 k만큼의 "0" 비트를 제외한 나머지 비트를 나타낸다. 일반적으로 MD5의 해쉬 함수에서 k가 0일 경우 단말기는 연산을 하지 않고 k가 128일 경우 X 값을 찾을 수가 없다. 따라서 인증서버는 보통 k를 0에서 64 사이의 값을 사용한다[2]. 이러한 보안 수준 변수 k는 인증서버의 현재 상태에 따라 유동적으로 값을 책정할 수 있다. 즉 연속적인 인증 요청이 들어오거나, 서버의 자원의 여유가 부족할 때 k를 증가 시킨다.

3.1.2 프로토콜

인증서버는 현재 상태에 대한 k를 결정하고 랜덤변수 N_S를 생성하여 사용자에게 보낸다. k 값에 따라 사용자는 랜덤변수 N_C를 생성하고 해쉬 함수를 이용하여 X를 계산한다[2]. 서버는 사전인증 과정이 필요한 사용자의 응답을 받으면 먼저 사용자가 보낸 값을 증명하고 올바른 값이면 다음 단계의 프로토콜을 실행하게 된다. 그림 2는 인증 초기 단계를 나타낸다.

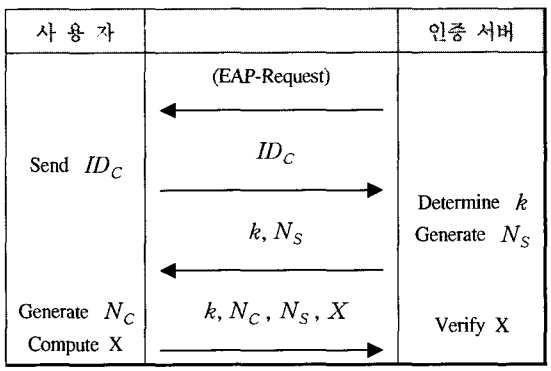


그림 2. 인증 초기 단계

3.2 인증 실행 단계

실질적인 인증 과정이 수행되는 부분으로 AsPect 프로토콜을 기본으로 하여 설계하였다[7]. 사용자는 자신의 랜덤변수 r_c을 생성하여 자신의 임시 공개키 g^{r_c}을 계산하여 인증 서버에 보낸다. 인증서버는 랜덤 변수 r_a를 생성하고 자신의 임시 공개키 g^{r_a}을 계산한 후, 자신이 생성한 타임스탬프와 공개키에 대한 인증서 그리고 상태 정보 $state_A$를 자신의 개인키로 암호화한 값과, $state_A$를 자신의 비밀키 K_A로 해쉬한 값과 같이 보낸다. $state_A$에 포함되는 값은 세션아이디, 타임스탬프, 사용자의 아이디, 접근 제한 변수(l) 등 서버가 다음 프로토콜 진행에 알아야 하는 값들이다. 타임스탬프는 고의적인 패킷 잃어버림을 방지하기 위한 것이고, 접근 제한 변수는 잘못된 패킷을 방지하기 위한 것이다. 즉 접근 제한 변수를 일정한 값으로 정해두고 잘못된 패킷이 들어올 때마다 값을 감소시킨다. 접근 제한 변수값이 0이 되면 서버는 인증 프로토콜을 종료하게 된다.

사용자는 서버로부터 받은 공개키 인증서로부터 서버의 공개키 g^v를 추출하여, 서버의 공개키 및 임시 공개키, 자신의 임시 비밀키(r_c)와 비밀키 (c)를 이용하여 $K_{AP} = h((g^v)^{r_c}, (g^{r_A})^c)$을 계산한다. 또한 세션 키와 자신의 ID를 입력 값으로 하는 $h(K_{AP}, ID_c)$을 계산한 후 자신의 공개키 인증서, 타임스탬프, 서버로부터 받은 상태 정보와 함께 서버에 보낸다.

서버는 사용자로부터 받은 공개키 인증서로부터 사용자의 공개키 g^c를 추출하여 사용자와 동일한 방법으로 $K_{AP} = h((g^{r_c})^v, (g^c)^{r_a})$를 생성한다. 이 때 필요한 파라미터는 상태 정보를 복호화하여 얻을 수 있다. 생성된 세션 키의 검증을 위해 사용자로부터 받은 $h(K_{AP}, ID_c)$과 비교한다. 또한 $h(K_{AP}, ID_a)$을 생성한 후 사용자에게 보낸다. 동일한 방법으로 사용자는 서버의 세션키를 검증한다. 그림 3은 인증 실행 단계를 나타낸다.

3.3 최종단계

최종적으로 프로토콜의 끝을 알리는 메시지를 보낸다. 단말기는 EAP-Response를 보내고 인증 서

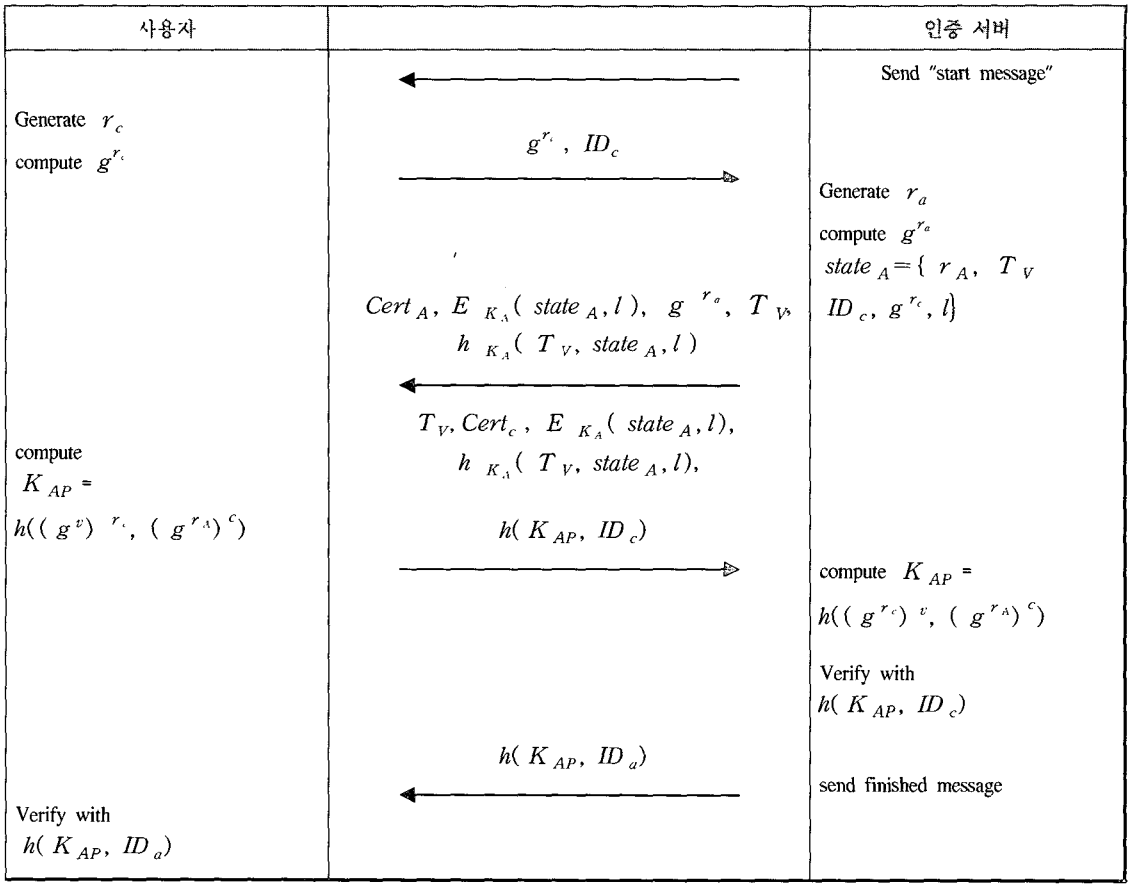


그림 3. 인증 실행 단계

버는 인증이 무사히 끝났음을 알리는 EAP-Success 메시지를 보냄으로써 인증을 완료한다. 인증 과정에서 생성된 세션 키는 인증과정 후의 프로토콜에서 마스터 세션 키로 사용한다.

Ⅳ. 안정성 분석

제안하는 인증 프로토콜의 초기 단계에서는 서버가 프로토콜이 진행될 때 마다 서버의 난수와 k를 다르게 함으로써 단말기는 미리 X 값을 계산 할 수 없다. 또한 인증 실행 단계에서는 서버는 단말기의 인증 및 키교환에 필요한 파라미터를 자신의 비밀키 K_A로 암호화하여 단말기에 보내게 되고, 이 값을 다시 단말기로 되돌려 받음으로써 단말기에 의한 파라미터 수정이 불가능하게 된다. 또한 세션 키 생성 시 이산 대수 문제를 기반으로 하기 때문에 3자에 의한 키 생성은 이루어 질 수 없다. 즉 $E_{K_A}(state_A, l)$, $h_{K_A}(T_V, state_A, l)$와 같이 설정변수들을 서버의 비밀키 K_A로 암호화하고, 해쉬 함으로써 이 변수들에 대한 기밀성과 무결성을 보장하고 있다. 이러한 설정변수는 공격자나 다른 사용자들에게 공개되어서는 않되는 서버만의 비밀로 블록 암호화하여 정보를 숨기고 자신의 비밀키 K_A로 해쉬하여 정보의 수정을 방지한다.

Ⅴ. 효율성 분석

4.1. 접근제어

기존의 프로토콜에서는 초기에 사용자의 아이디만 요청하고 그 아이디를 받으면 다음 단계의 프로토콜이 진행되었다. 이와 같은 방식은 인증프로토콜은 검증되지 않은 사용자일지라도 프로토콜의 시작을 요청하면 인증서버는 자신의 자원을 할당하고 인증 프로

토콜을 진행하는 구조를 가지고 있다. 이러한 점을 이용하여 DoS 공격이 가능하게 된다.

제안하는 프로토콜에서는 인증 초기 단계에서 보안 수준 변수 k를 두어 사용자의 무차별적인 인증 서버의 접근을 서버가 조절 가능하게 하였다. 즉 k를 증가시키면 사용자는 X를 찾기 위한 연산량이 많아지기 때문에 무차별적인 접근을 막을 수 있다. 또한 서버는 난수 생성과 해쉬만을 이용하기 때문에 DoS 공격에 효율적으로 방어할 수 있다.

4.2 자원의 할당 및 통신량

DoS 공격은 서버의 자원 소비를 비정상적으로 소비 시켜서 합법적인 사용자가 서비스를 이용하지 못하게하는 공격법이다. 따러서 이 자원을 할당을 최소화 시켜서 이러한 공격의 위험을 최소화 시킬수 있다. 기존의 프로토콜에서는 프로토콜 진행과정에서 프로토콜 진행에 필요한 랜덤변수 r_a, r_c, 타임스탬프 T_V, 아이디 ID_c, 사용자의 공개키 g^m, 접속 제한변수 l, 등이 서버의 메모리에 저장되어야 한다. 그림 2 에서 보듯이 제안된 프로토콜에서는 이런 정보들이 서버에 직접 저장되지 않고 프로토콜의 메시지들과 함께 $E_{K_A}(state_A, l)$, $h_{K_A}(T_V, state_A, l)$ 형태로 직접 사용자에게 전달되고 이것은 다시 사용자가 서버에게 보내는 메시지와 함께 되돌아오는 형태로 진행된다. 따라서 서버는 자신의 메모리의 사용을 최소화 할 수 있게 되고 이것을 통해서 DoS 공격의 위험을 줄일 수 있게 된다.

그러나 서버의 저장 공간의 효율성을 위해 사용한 stateless 프로토콜은 기존의 메시지에 $E_{K_A}(state_A, l)$, $h_{K_A}(T_V, state_A, l)$ 첨가되므로 전달되는 패킷의 길이가 커지고 더 많은 대역폭을 사용하게되는 단점이 있다. 또한 기존의 인증 프로토콜에는 존재하지 않는 인증 초기 단계를 둠으로써 서버에 저장되는 정보 Ns와 추가적인 통신량이 발생한다. 표 3은 EAP-TLS에서 서버에 저장되는 정보와 추가적인 통신량을 제안하는 프로토콜과 비교한 것이다.

4.3 프로토콜상의 취약점 개선

프로토콜상 보장된 재전송에 의한 공격은 따로 접속 제한 변수 l를 두고 타임 스탬프 T_V를 사용하여 횟수 및 시간상의 제약을 둠으로 해결하였다. 보통 접속 제한 변수를 0에서 5의 값을 가지게 하고 서버의 현재 서버의 상태에 따라 유동적으로 값을 변화시킨다. 즉 서버의 자원이 많이 남아 있을 때는 5를, 접속자 수가 많으면 l를 작게하여 잘 못된 패킷이 들어올 때 값을 감소 시켜 0이 될 때 는 자동으로 패킷을 폐기한다. 그리고 타임스탬프를 사용하여 일정 기간 이상이 지난 패킷은 폐기하여 재전송의 위험을 감소 시켰다.

V. 결 론

무선 랜에서 인증을 위한 인증 서버의 접근은 사용자의 ID 만으로 가능하다. 따라서 이러한 약점을

표 3. 자원의 할당 및 통신량 비교

구 분		EAP-TLS	제안하는 프로토콜
인증 초기 단계	서버에 저장되는 정보	no	NS (24bit)
	추가적인 통신량	no	k(6bit), Nc(24bit), Ns(24bit), X(24bit)
	메시지 전송횟수	no	3회
인증 실행 단계	서버에 저장되는 정보	사용자의 난수(32bit), 서버의 난수(32bit), 사용자의 ID(8bit), 타임스탬프(8bit), 접속제한변수(8bit)	no
	추가적인 통신량	no	$E_{K_A}(state_{A,l})$ (1024bit) $h_{K_A}(T_{V,state_{A,l}})$ (160bit)
	메시지 전송횟수	4회	4회

이용하여 악의적인 공격자에 의한 무차별적 인증 서버 접근은 인증서버의 자원을 고갈시키는 결과를 가져온다. 또한 인증 프로토콜 실행 단계에서 패킷의 잃어버림, 잘못된 패킷의 전송 등을 처리하기 위한 재전송은 결국 서버의 연산량의 측면과 저장 공간의 고갈을 가져온다.

본 논문에서는 이러한 문제들을 해결할 수 있는 방법으로 자원 할당 이전에 실행되는 사전 검증 단계에 보안 수준 변수를 사용하여 사용자의 서버 접근을 서버가 능동적으로 방어할 수 있게 하였다. 또한 프로토콜의 진행에 필요한 정보를 서버에 직접 저장하지 않고 프로토콜의 메시지와 함께 보내는

stateless 프로토콜을 사용하여 서버의 자원의 효율성을 가져왔다. 접속 제한 변수와 타임 스탬프를 이용하여 패킷의 잃어버림, 잘못된 패킷의 전송에 대한 문제점을 해결하였다. 그러나 stateless 프로토콜과 초기 인증 단계를 사용하기 때문에 패킷 길이 및 대역폭 증가의 문제점을 가지고 있다.

참 고 문 헌

[1] J. Leiwo, "Towards Network Denial of Service Resistant Protocol," SEC-2000, pp. 301-310, 2000.

[2] T. Aura, P. Nikander, and J.Leiwo, "DOS-resistant authentication with Client puzzles", In Proc. Security Protocols Workshop, pp. 178-181, 2000.

[3] L. Blunk, J. Vollbrecht, B. Aboba, J. Carlson and H. Levkowetz,"Extensible Authentication Protocol," http://www.ietf.org/internet-drafts/draft-ietf-eap-rfc2284bis-06.txt, Sept. 2003.

[4] T. Aura and, P. Nikander, "Stateless Protocol," In ICICS'97, LNCS 1334. Springer-Verlag, 1997.

[5] B.H. Jung et al, "Technology Trends on Authentication and Key Management in Public WLAN Networks," 전자통신동향분석, pp.1-15, 2002.

[6] P. Eronen,"Denial of service in public key protocols,"Helsinki Univ. of Technology's Seminar on Network Security, course Tik-110.501, 24000.

[7] K.M. Martin and C.J. Mitchell, "Evaluation of authentication protocols for mobile environment value-added services", IEEE Transactions on Vehicular Technology, pp. 383-392, 2002.

[8] P. Calhoun and C. Perkins, "PPP EAP TLS Authentication Protocol," IETF RFC 2794, 2000.

[9] J. Arkko et al., "EAP AKA Authentication," http://www.ietf.org/internet-drafts/draft-arkko-pppext-eap-aka-03.txt, 2002.

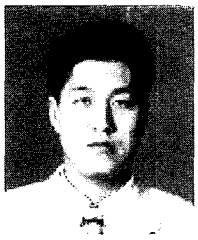
[10] 정종민 등, "공개키 기반 구조에서 빠른 핸드오프를 위한 무선랜 인증 기법 설계," 정보보호학회논문지, 2003.

[11] 박영만 등, "공중 무선랜에서의 이중요소 인증된 키교환 프로토콜," 정보보호학회논문지, 2003.

〈著者紹介〉

김 민 현 (Min-hyun Kim) 학생회원
2002년 2월 : 경북대학교 전자공학과 학사
2002년 3월 : 경북대학교 전자공학과 석사
〈관심분야〉 무선랜보안, 정보보호

이 재 욱 (Jae-wook Lee) 학생회원
2001년 2월 : 경북대학교 전자공학과 학사
2003년 2월 : 경북대학교 전자공학과 석사
2003년 3월~현재 : 경북대학교 전자공학과 박사과정
〈관심분야〉 무선랜 보안, XTR 암호 시스템, 정보보호



최 영 근 (Young-Geun Choe) 학생회원
1995년 2월 : 경북대학교 전자공학과 졸업
2001년 2월 : 경북대학교 전자공학과 석사 졸업
2001년 3월~현재:경북대학교 전자공학과 박사과정
〈관심분야〉 정보보호 및 보안 기술, 정보 보호 응용 기술

김 순 자 (Soon-Ja Kim) 정회원
1975년 2월 : 경북대학교 수학 교육학과 학사
1977년 2월 : 경북대학교 수학과 석사
1988년 2월 : 계명대학교 수학과 박사
1993년 4월~현재 : 경북대학교 전자·전기 공학부 교수
〈관심분야〉 정보보호 및 보안 기술, 정보 보호 응용 기술