한국산학기술학회논문지
Vol. 10, No. 9, pp. 2384-2389, 2009

홈네트워크를 위한 새로운 경량화된 상호인증 프로토콜

이기성[1*]
[1]호원대학교 컴퓨터·게임학부

A New Lightweight Mutual Authentication Protocol for Home Network

Gi-Sung Lee[1*]
[1]**Division of Computer and Game, Howon University**

요 약 본 논문에서는 안전하고 효율적인 홈 네트워크 서비스를 제공하기 위해 경량화 된 상호인증 프로토콜을 제안한다. Lee 등은 공개키 연산을 이용하여 홈네트워크 상에서 속성기반의 인증된 키 교환 프로토콜을 제시하였다. 이 프로토콜에서는 전 방향 안전성을 제공하고 있으나 티켓을 이용한 두드러진 연산의 오버헤드를 줄이지는 못하고 있다. 따라서 제안하는 프로토콜은 해시함수와 카운터만을 이용하여 효율성과 안전성을 제공했다. 또한 세션키 생성 후에는 사용자의 가전 제어 레벨을 체크함으로써 안전한 홈 네트워크 서비스를 제공할 수 있다.

Abstract In this paper, we propose a lightweight mutual authentication protocol for secure and efficient home network service. Lee et al. recently proposed an attribute-base authentication key agreement protocol using public key in home network. Its protocol provided forward secrecy but don't diminish conspicious overhead of operation using ticket. Therefore the proposed protocol provided the security and efficiency using hash function and counter. Also it can provide secure home network service by check consumer electronics control level of users after created session key.

Key Words : Secure home network protocol, Lightweight mutual authentication, User authentication

1. 서론

유비쿼터스 컴퓨팅과 네트워킹 기술의 발달로 인해 홈 네트워크에 많은 관심이 집중되고 있다. 홈 네트워크는 유·무선 망을 댁내로 연결시켜 원격지에서도 댁내의 정보가전을 제어할 수 있도록 하여 생활의 편리성을 증진시키는데 있다. 그러나 안전한 홈 네트워크를 구성하지 않을 경우 개인의 사생활 침해를 비롯하여 개인의 생명 및 자산의 피해 등이 발생할 수 있다. 따라서 홈네트워크 보안에 대한 표준화는 필수적이다. 홈네트워크의 표준화는 ISO에서 2005년에 홈네트워크 보안 요구사항과 댁내 및 댁외 보안에 대한 표준이 나오게 되었고 국내에서는 HNSF(Home Network Security Forum)와 TTA(Telecommunications Technology Association)를 중심으로 홈네트워크 보안에 관한 표준이 개발되고 있는데 2006년과 2007년에는 홈네트워크 보안 기술 프레임워크, 홈 네트워크 사용자 인증 메커니즘, 홈네트워크 보안 정책 기술 언어 등의 표준안이 제정되었다. 홈네트워크 보안에 있어서 가장 중요한 요소는 사용자 인증과 키교환이다. 인증 기법으로는 댁내 홈서비스를 위한 사용자 인증, 댁외에서 댁내 홈서비스에 대한 세가지 형태로 나눌 수 있다[1]. 이러한 세 가지 형태의 인증을 제공하기 위해 가장 많이 사용되고 있는 기법은 EAP-MD5(Extensible Authentication Protocol-MD5)이다. 하지만 EAP-MD5에서 인증서버는 사용자를 인증하지만 사용자는 인증 서버를 인증하지 않는 단방향 인증을 사용하고 키 생성을 제시하지 못한다. 그러므로 EAP-MD5는 중간자공격(Man-In-The-Middle attack)과 서비스 공격(Denial of Service)에 노출될 수 있다. 이러한 EAP-MD5의 취약점을 개선하기 위해 2006년 TTA에서 홈네트워크 사용자

이 논문은 2009년 호원대학교 교내연구비의 지원에 의하여 연구되었음
*교신저자 : 이기성 (ygslee@howon.ac.kr)
접수일 09년 07월 27일 수정일 (1차 09년 08월 25일, 2차 09년 09월 13일) 게재확정일 09년 09월 16일

인증 메커니즘인 EEAP-PW(Encrypted Extensible Authentication Protocol PW) 프로토콜을 표준화 하였다. 그러나 이 표준 역시 패스워드 테이블에 대한 공격 가능성이 존재하므로 Jeon외 1명은 2008년 속성기반의 인증 프로토콜을 제시하였다. 그러나 이 프로토콜은 인증과 키 생성을 위해 계산량이 많은 공개키 연산을 사용하고 있으며 티켓을 사용하여 연산의 오버헤드를 줄이려고 했으나 티켓의 효율성이 떨어진다[2].

따라서 본 논문에서는 해시함수($h(), MAC(K, M)$)와 연접연산을 이용하여 경량화된 상호인증 프로토콜을 제안한다. 먼저 사용자(mobile phone, PDA, smart phone, laptop computer etc)는 서버(home server 또는 home gateway)에 off-line으로 ID, PW, C를 등록한다. 그런 후에 세션키 $K_{U-S} = h(ID_i \| PW_i \| C_i^{j+1} \| C_i^{j+2})$를 생성한다[3,4]. 제안하는 프로토콜에서는 [2]와 달리 공개키 연산을 전혀 사용하지 않기 때문에 계산량 측면에서 효율적이다. 또한 사용자와 홈서버는 초기 카운터값을 비교하여 메시지의 드롭여부를 결정하기 때문에 리소소 고갈 공격 및 연결 고갈 공격인 DoS공격에 강건하다. 반면에 매번 공개키 연산을 사용하는 [2]는 공격자가 타임스탬프를 획득한 후 $M_1 = ID_U, ID_H, A, T_U, sign_1(M_1), sign_2(M_1), \cdots, sign_i(M_1)$ 메시지를 생성하여 분산적으로 홈서버에 집중하여 전송할 경우 홈서버의 리소스를 독점하거나 정당한 사용자의 접속을 지연시킬 수 있다.

이 논문의 구성은 다음과 같다. 2장에서는 홈 네트워크 구성에 대해 살펴보고 기존에 제안된 홈 네트워크 인증 프로토콜을 살펴본다. 3장에서는 제안하는 프로토콜에 대해 자세히 기술하며 4장에서는 제안하는 프로토콜의 효율성과 안정성을 분석하고 마지막 5장에서는 결론과 향후 연구방향을 제시한다.

2. 관련연구

2.1 표기법

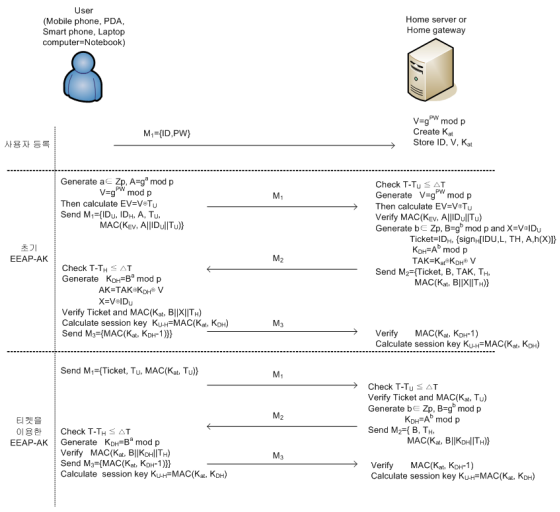
제안하는 프로토콜과 관련 연구에서 사용될 용어 및 표기는 표 1과 같다.

[표 1] 표기법

표기	의미
ID_i	i의 식별자
PW_i	i의 패스워드
C_i^j	i의 j시작 카운터
$Level_i$	i수준의 가전 제어 권한
K_i	i의 비밀키
K_{a-b}	a와 b사이의 세션키
K_{at}	속성기반의 비밀키
K_{DH}	Diffie-Hellman 비밀키
$h()$	충돌 회피 해시 함수($\{0,1^* \rightarrow 0,1^l\}$)
$MAC(k,m)$	비밀키 k를 이용한 메시지 m에 대한 메시지 인증 코드 값
$sign_i$	i의 전자서명
V	$g^{PW} \bmod p$
r_i	i의 랜덤 값($a \in Z_p$)
g,p	p는 매우 큰 소수, $g < p$이고 p와 서로소인 원시근
T_i	i의 타임스탬프
T	i가 생성한 타임스탬프 도착 시간
L	Lifetime
$f_K(M)$	비밀키 K를 이용한 메시지 M에 대한 pseudorandom function
$m_1 \| m_2$	메시지 m_1과 m_2의 비트결합

2.2 EEAP-AK 프로토콜[2]

홈 네트워크에서 홈서버 또는 홈 게이트웨이는 댁내로 접근하는 모든 사용자를 검사하고 제어하는 인증서버 역할을 수행한다. 홈 네트워크 시스템에서 인증 처리는 크게 댁내에서 댁내 홈 서비스를 제공하기 위한 사용자 인증, 댁내에서 댁외 서비스를 위한 사용자 인증, 댁외에서 댁내 홈서비스를 위한 사용자 인증으로 나눌 수 있다[2]. Lee 등은 TTA의 표준인 EEAP-PW의 문제점을 해결하기 위해 제안된 속성기반의 인증된 키교환 프로토콜은 그림 1과 같다. 프로토콜은 크게 초기 EEAP-AK 프로토콜과 티켓을 이용한 EEAP-AK로 나눌 수 있다.



[그림 1] EEAP-AK 프로토콜

사용자는 먼저 랜덤 값 $a \in Z_p$를 선택하고 $A = g^a \bmod p$를 계산한 후 $V = g^{PW}$와 $EV = V \oplus T_U$를 계산하여 홈서버 H에게 $M_1 = ID_U, ID_H, A, T_U, MAC(K_{EV}, A \| ID_U \| T_U)$을 전송한다. 이 때, 사용자(핸드폰, PDA, Smart phone, etc)가 처리해야 할 계산량을 구해보면 A와 V값을 구하기 위한 지수연산 2번($2 * 3028K(cycles/byte)$)과 해시연산 1번($0.026K(cycles/byte)$)을 수행한다. 한정된 배터리를 이용하는 단말기로서는 적지 않은 계산량이다[2]. 홈서버는 먼저 $T - T_U \leq \Delta T$ 연산을 통해 적법한 시간 범위에 메시지가 보내졌는지 확인한다. 홈서버는 V와 EV를 계산하고 MAC값을 검증하여 적법한 사용자 여부를 확인한 뒤, 랜덤 값 $b \in Z_p$를 선택하여 $B = g^b \bmod p$와 $X = V \oplus ID_U$을 계산한 후 티켓을 서명하여 발급한다. 그리고 $MAC(K_{at}, B \| X \| T_H)$와 $K_{DH} = A^b \bmod p$ 및 $TAK = K_{at} \oplus K_{DH} \oplus V$를 계산하여 사용자에게 M_2메시지를 전송한다. 먼저 홈서버의 총계산량을 계산해보면 2번의 Diffie Hellman 키 계산($2 * 3028K(cycles/byte)$, 1번의 서명($1 * 62000K$)과 2번의 해시연산($2 * 0.026K(cycles/byte)$)이 필요하다. 이는 적지 않은 계산량이지만 서버라는 점에서는 가능하다고 볼 수 있다.

사용자는 M_2 메시지를 받은 후 $T - T_U \leq \Delta T$의 적법성을 체크하고 $K_{DH} = B^a \bmod p$를 계산하여 $TAK \oplus K_{DH} \oplus V = K_{at}$를 유도한다. 사용자는 속성기반 비밀키 K_{at}를 이용하여 $MAC(K_{at}, K_{DH} - 1) = M_3$를 계산하고 서버에게 전송한다. 이 단계에서도 1번의 Diffie-Hellman 키 계산($1 * 3028K(cycles/byte)$)과 3번의 해시연산($3 * 0.026K(cycles/byte)$)이 필요하다[3].

티켓을 이용한 키교환을 살펴보면 사용자가 티켓을 홈서버에게 전송하면 홈 서버는 티켓 안의 사용자 Diffie-Hellman 공개키를 이용하여 키동의($K_{DH} = A^b \bmod p$)를 수행한다. 티켓의 주역할은 이것인데 이는 서버에서 티켓을 발행하지 않고 초기 키교환 단계에서 계산한 A값을 사용자가 저장하고 있다가 티켓 대신에 $M_1 = A, T_U, MAC(K_{at}, A \| T_U)$을 서버에게 전송하는 것이 전체적인 계산 측면에서는 더욱 효율적이다. 왜냐하면 서버에서 굳이 티켓을 발행할 필요가 없으며 발행시 서명에 대한 계산 부담도 줄여줄 수 있기 때문이다.

3. 제안하는 프로토콜

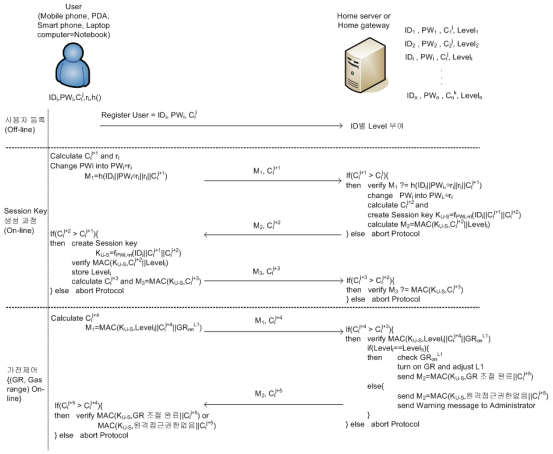
본 장에서는 안전하고 효율적인 홈네트워크 서비스를 제공하기 위해 제안한 경량화된 상호 인증 프로토콜에 대해 설명한다. 프로토콜은 크게 사용자 등록 단계, 세션키 생성 단계와 가전 제어 단계로 나누어진다. 사용자 등록 단계는 통신상에서 존재할 수 있는 공격이 접근할 수 없는 안전한 off-line상에서 수행되고 세션키 생성 단계는 on-line상으로 수행되는데 서비스 거부 공격을 방지하기 위해 초기 카운터 값을 체크하여 메시지의 드롭여부를 판별한다. 마지막으로 가전 제어 단계에서는 세션키를 생성한 후 서버로부터 수신한 수준별 가전 제어 값으로 가전 제어 여부를 판별하여 차별화된 홈 네트워크 서비스를 제공한다.

3.1 사용자 등록 단계

사용자 등록은 안전한 off-line상에서 진행되며 홈 네트워크 서비스를 이용하는 사용자는 가족 구성원들(관리자, 성인, 어린이, 노인 등)과 원격 관리자들(수도, 전기, 가스 검침 및 관리)이 있을 수 있다[2]. 먼저 사용자는 자신의 아이디(ID_i)와 패스워드(PW_i) 및 카운터(C_i^j)를 홈서버에 등록한다. 관리자는 홈서버에 등록된 사용자의 나이 및 가전 제어 능력을 고려해서 가전 제어 수준($Level_i$)을 지정한다. 이 때, 등록된 패스워드는 매번 홈서버에 접속할 때마다 변경되기 때문에 공격자의 홈서버 해킹으로 인한 PW노출에도 안전하다.

3.2 세션키 생성 단계

이 단계는 on-line상으로 진행되는데 먼저 사용자는 자신의 ID,PW를 이용해 홈서버의 인증을 받는다. 홈서버는 변경된 사용자의 $PW_i \oplus r_i$를 키로 이용하는 pseudorandom function을 이용하여 세션키를 생성한다. 이때, 카운터는 초기 DoS공격을 방지하기 위해 사용된다. 전체적인 프로토콜은 그림 2와 같으며 프로토콜의 상세한 수행과정은 다음과 같다.



[그림 2] 경량화된 상호 인증 프로토콜

$M_1(User \rightarrow Home\ Server)$: 먼저 사용자는 카운터 값 C_i^{j+1}을 계산하고 변경된 패스워드 $PW_i \oplus r_i$와 아이디 ID_i 및 카운터 값을 포함한 메시지를 해시한 후 홈서버에 접속을 위해 메시지 M_1을 전송한다.

$M_2(Home\ Server \rightarrow User)$: 홈서버는 먼저 $C_i^{j+1} > C_i^j$ 연산을 통해서 사용자를 인증한다. 이는 DoS공격의 초기 방지를 위함이다. 그런 후에 해시 값을 검증하고 데이터베이스에 저장된 사용자의 PW_i를 $PW_i \oplus r_i$으로 변경한다. 홈서버는 카운터 값을 증가시키고 사용자와 일정 세션동안 사용할 세션키 $K_{U-S} = f_{PW_i \oplus r_i}(ID_i \parallel C_i^{j+1} \parallel C_i^{j+2})$를 pseudo-random function $f_K(M)$을 이용하여 생성한다. 마지막으로 생성된 세션키를 이용하여 메시지 $M_2 = MAC(K_{U-S}, C_i^{j+2} \parallel Level_i)$을 사용자에게 전송한다. 이 때, $Levei_i$는 사용자별 가전 제어를 차별화하기 위한 값으로서 예를 들어, 노약자나 어린이의 경우 화재 위험이 있는 가스렌즈 접근 권한은 외부에서 제한할 수 있다.

$M_3(User \rightarrow Home\ Server)$: 사용자 역시 $C_i^{j+2} > C_i^{j+1}$을 체크하여 홈서버를 인증하고 세션키 $K_{U-S} = f_{PW_i \oplus r_i}(ID_i \parallel C_i^{j+1} \parallel C_i^{j+2})$를 생성한다. 그런 후에 가전 제어 수준 $Level_i$ 값을 안전한 곳에 저장한다. 마지막으로 카운터 값 C_i^{j+3}으로 증가하고 $M_3 = MAC(K_{U-S}, C_i^{j+3})$을 홈서버에 전송한다. 홈 서버는 먼저 카운터 값을 체크하고 MAC값을 검증한다.

3.3 가전 제어 단계

사용자는 세션키 생성단계에서 홈서버로부터 획득한 가전 제어 수준 값을 이용하여 차별화된 가전 제어를 할 수 있다. 가전 제어 과정은 다음과 같다.

$M_1(User \rightarrow Home\ Server)$: 사용자는 카운터 값 C_i^{j+4}을 계산하고 가스렌즈를 조절하기 위한 변수 $GR_{on}^{L_1}$를 선택한다. 이때 $GR_{on}^{L_1}$는 가스렌즈를 1단으로 켜는 변수이다. 그런 후에 세션키를 이용하여 $MAC(K_{U-S}, Level_i \parallel C_i^{j+4} \parallel GR_{on}^{L_1})$을 계산하고 홈서버에게 전송한다.

$M_2(Home\ Server \rightarrow User)$: 홈서버는 먼저 카운터 값의 정당성을 체크한 후 세션키를 이용하여 MAC값을 검증한다. 그런 후에, 사용자로부터 수신한 $Level_i$값과 가스렌즈 접근 레벨 $Level_5$와 같은지 확인하고 같을 경우 원격으로 가스렌즈를 1단으로 켜고 사용자에게 GR 조절 완료 메시지를 포함한 MAC값을 보낸다. 그렇지 않을 경우에는 “원격 접근 권한 없음”메시지를 포함한 MAC값을 사용자에게 보내고 또한 관리자에게도 경고 메시지를 보낸다.

4. 성능분석

4.1 안전성 분석

제안하는 프로토콜에서 off-line상으로 진행되는 사용자 등록시에는 어떤 공격도 받지 않는다고 가정한다. 공격자에 대한 프로토콜의 침해는 on-line상으로 진행되는 세션키 생성 단계와 가전 제어 단계로 국한하여 여러 공격 시나리오를 통해 본 프로토콜의 안전성을 분석한다.

4.1.1 제안하는 프로토콜

■공격 시나리오 I (패스워드 추축 공격): 패스워드는 사용자들이 쉽게 기억할 수 있는 비밀값으로 설정하는 것이 대부분이다. 제안하는 프로토콜에서 공격자가 홈서버를 해킹하여 사용자의 패스워드를 획득하여도 세션키 생성단계에서 사용자는 홈서버 초기 인증시 패스워드 PW_i를 매번 변경하여 홈서버에 접근하기 때문에 패스워드 추축공격은 어렵다. 그럼에도 불구하고 공격자가 사용자의 패스워드를 $PW_i \oplus r_i^{'}$로하고 홈서버에 접근하려 해도 공격자는 일방향 해시함수를 계산할 수 없기 때문에 홈서버 접속에 대한 어려움이 따른다.

■공격 시나리오 II(재전송 공격): 재전송 공격은 프로토콜상에서 유효 메시지를 골라 복사한 후 일정 시간 후에 재전송함으로써 정당한 사용자로 가장하는 공격으로 여러 가지 방법(타임스탬프와 도전 응답 및 카운터 값)을 통해 대응할 수 있다. 제안하는 프로토콜에서는 카운터 값을 이용하는데 공격자가 M_1, C_i^{j+1}을 복사한 후 일정 시간 후 홈서버에 전송하여도 홈서버는 초기 정당한 사용자로부터 M_1, C_i^{j+1}을 수신하여 검증한 후 카운터 값 C_i^{j+1}을 C_i^{j+2}으로 이미 변경하였기 때문에 초기 카운터 값의 정당성 체크 $C_i^{j+1} > C_i^{j+2}$시에 메시지가 차단되게 된다. 다른 메시지 복사의 경우에도 위와 동일한 결과가 된다. 따라서 재전송 공격에 안전하다.

■공격 시나리오III(위장공격): 공격자가 사용자의 패스워드를 전송 메시지 M_1과 M_2를 통해서 획득하는 것은 불가능하다 또한 공격자가 홈서버를 해킹하여 사용자의 패스워드를 획득하였다고 하여도 매번 변경되는 패스워드를 추축하여 정당한 사용자로 위장하는 공격은 불가능하다. 공격자가 홈서버로 위장하였다고 가정해도 사용자로부터 전송되는 M_1 메시지를 해시하여 사용자의 변경된 패스워드 $PW_i \oplus r_i$을 획득할 수 없기 때문에 정당한 세션키 K_{U-S}를 생성할 수 없다. 따라서 올바른 M_2 메시지를 생성할 수 없기 때문에 정당한 홈서버로 위장할 수 없다.

■공격 시나리오IV(DoS 공격): 도스 공격은 크게 리소스 고갈공격과 연결 고갈 및 지연 공격을 들 수 있다. 홈서버의 경우 리소스에는 제한이 없다고 볼 수 있기 때문에 이 공격은 배제하고 연결 고갈 공격을 수행했다고 가정하자. 제안하는 프로토콜에서는 초기 카운터 값만을 비교하여 메시지의 드롭 여부를 결정하기 때문에 신속하게 처리될 수 있다. 따라서 연결 고갈 및 지연을 큰 부담이 되지 않는다.

[표 2] 프로토콜의 성능분석

			EEAP-AK[2]		**제안하는 프로토콜**
			초기	티켓발행 후	
메시지 수			3	3	3(가전제어 메시지 제외)
사용자	암/복호화		0K	0K	0K
	RSA	서명	0K	0K	0K
		검증	1*3019K	0K	0K
		Diffie-Hellman	3*3028K	1*3028K	0K
	MAC(CBCMAC-Rijindael)		4*0.026K	4*0.026K	4*0.026K
합계			**12103.104K**	**3028.104K**	**0.104K**
홈서버	암/복호화		0K	0K	0K
	RSA	서명	1*62000K	0K	0K
		검증	0K	1*3019K	0K
		Diffie-Hellman	3*3028K	2*3028K	0K
	MAC(CBCMAC-Rijindael)		4*0.026K	4*0.026K	4*0.026K
합계			**71084.104K**	**9083.104K**	**0.104K**
총합계			**83187.208K**	**12111.208K**	**0.208K**

4.1.2 Lee외 1명[2]

패스워드 추축 공격와 위장공격의 경우 전송되는 메시지 M_1과 M_2메시지로 사용자의 패스워드를 추축할 수는 없다. 그러나 만일 공격자가 홈서버를 해킹하였다고 가정하면 공격자는 ID, V, AK를 획득할 수 있다. 그럴 경우 공격자는 M_1메시지의 T_U와 홈서버에서 획득한 V를 이용해 EV를 계산할 수 있다. 그럴 경우 공격자는 정당한 사용자의 M_1 메시지를 생성할 수 있게 되어 정당한 사용자로 위장할 수 있다. 또한 DoS공격의 경우 공격자는 M_1메시지의 타임스탬프를 중간에서 획득하는 것은 어려운 일이 아니다. 공격자는 타임스탬프를 획득한 후 $M_1 = ID_U, ID_H, A, T_U, sign_1(M_1), sign_2(M_1), \cdots, sign_i(M_1)$ 메시지를 생성하여 분산적으로 홈서버에 집중하여 전송할 경우 홈서버의 리소스를 독점하거나 정당한 사용자의 접속을 지연시킬 수 있다. 이는 $T - T_U \leq \triangle T$시간을 만족하는 메시지이기 때문에 홈서버는 서명 메시지의 정당성을 검증하게 된다.

4.2 효율성 분석

효율성은 프로토콜에 참여하는 각 단말의 계산량과 통신량을 통해 분석할 수 있는데 통신량은 일정하다고 가정하고 각 노드의 계산량만으로 프로토콜을 분석한다[5]. 분석 결과는 표 2와 같다.

EEAP-AK[2] 프로토콜에서 초기시 사용자는 홈서버의 서명을 확인하기 위한 한번의 검증과 Diffie-Hellman 키 동의에 필요한 지수연산 3번을 포함해서 대략 $12103Kbyte$의 계산량이 필요하며 티켓을 이용할 경우에는 그보다는 적은 $3028Kbyte$의 계산량이 필요하다. 이에 반해 제안하는 프로토콜에서는 공개키 연산을 전혀 사용하지 않기 때문에 $0.104Kbyte$의 계샨량이면 충분하다. 홈서버의 경우에는 초기와 티켓의 사용할 경우를 대략 비교해보면 $71084Kbyte/9083Kbyte$이 필요하다. 티켓을 이용할 경우가 비교적 적은 양의 계산량이 필요하지만 제안하는 프로토콜의 계산량 $0.104Kbyte$에 비하면 많은 연산 차이를 보인다.

5. 결론

본 논문에서는 Lee등[2]이 제안한 속성기반의 인증된 키교환 프로토콜의 많은 계산량과 이에 따른 공격에 대한 취약성을 보였다. 이를 해결하기 위해 제안하는 프로토콜에서는 공개키 연산을 전혀 사용하지 않고 해시연산만을 이용하여 안전하고 경량화된 세션키 생성을 했으며 이를 통한 가전제어 과정을 보였다. 또한 안전성과 효율성은 초기 카운터 값의 비교로 인해 리소스나 연결을 고갈 시킬 수 있는 DoS공격에 강건함을 보였으며 각 노드에서 처리해야 할 계산량 역시 Lee등의 프로토콜과 비교했을 때 많은 차이를 보였다.

참고문헌

[1] 이덕규, 김도우, 한종욱, “홈네트워크 보안 기술 및 표준화 동향”, ETRI 전자통신동향 분석, 제23권, 제4호, pp. 89-101, 2008.

[2] 이원진, 전일수, “홈네트워크 상에서 속성기반의 인증된 키교환 프로토콜”, 한국정보보호학회논문집, 제18권, 제5호, 2008.

[3] 구중두, 이기성, "네트워크 이동성 지원을 위한 인증된 경로 최적화 프로토콜", 한국산학기술학회 논문집, 제8권, 제4호, pp. 781-787, 2007.

[4] 이기성, "안전한 WiBro 서비스를 위한 PSD(Power Support Device) 기반 인증 프로토콜", 한국산학기술학회 논문집, 제9권, 제3호, pp. 727-733, 2008.

[3] Jung-Doo Koo and Dong-Chun Lee, “Extended Ticket-Based Update (ETBU) Protocol for Mobile IPv6 (MIPv6) Networks,” IEICE Transactions on Communications, vol.E90-B, no.4, pp.777-787, 2007.

이 기 성(Gi Sung Lee) **[종신회원]**

- 1993년 2월 : 숭실대학교 컴퓨터학과 (공학사)
- 1996년 2월 : 숭실대학교 컴퓨터학과 (공학석사)
- 2001년 8월 : 숭실대학교 컴퓨터학과 (공학박사)
- 2001년 9월 ~ 현재 : 호원대학교 컴퓨터·게임학부 교수

<관심분야>
이동통신, 네트워크 보안, 데이터베이스관리, 멀티미디어