디지털산업정보학회 논문지 제5권 제3호-2009년 9월

무선 메쉬 네트워크를 위한 인증 메커니즘에 관한 연구

김 태 경*

A Study on the Authentication Mechanism for Wireless Mesh Network

Kim, Tae Kyung

〈Abstract〉

Wireless mesh networks (WMNs) consist of mesh routers and mesh clients, where mesh routers have minimal mobility and form the backbone of WMNs. They provide network access for both mesh and conventional clients. The integration of WMNs with other networks such as the Internet, cellular, IEEE 802.11, IEEE 802.15, IEEE 802.16, sensor networks, etc., This paper presents a secure and efficient authentication mechanism for Wireless mesh network. The validity of proposed mechanism is provided by BAN logic and the efficiency of suggested mechanism is showed through the performance evaluation.

Key Words : Wireless Mesh Network, Authentication, Security

Ⅰ. 서론

무선 인터넷 서비스의 발달로 인해 3G, 4G 망과 같은 광대역 셀룰러 데이터 네트워크에서부터 이동 ad-hoc 네트워크, 무선 랜, 블루투스와 같은 다양한 무선 네트워크 기술들이 개발되고 있다. 이렇게 다양한 무선 네트워크들이 차세대 네트워크로 발전하면서 보다 좋은 서비스를 제공하기 위한 핵심 기술로 최근 무선 메쉬 네트워크가 제안되었다. 메쉬 네트워크는 옥외형 공간에서 AP와 AP간을 무선망으로 연결할 수 있는 공중망 무선 랜 기술로, 그동안은 와이파이와 와이맥스/와이브로 시장의 중간단계 또는 보완재 시장으로 평가받아 왔다. 그러나 AP간 전송 커버리지가 4~5㎞, 최대 10㎞로 확대되고 전송속도도 20Mbps급 이상으로 업그레이드되면서, U-시티 및 국가 단위의 모바일 프로젝트에 핵심 기술로 각광받고 있다.

무선 메쉬 네트워크는 케이블 설치 없이 여러 액세스 포인트를 하나의 무선 네트워크 혹은 핫 스팟(지역)에 연결해 방대한 무선 커버리지를 제공하며, 각 액세스 포인트는 사용자 기기의 접근을 제공함과 동시에 근접한 액세스 포인트에 무선 전송로를 제공해 라우팅이 가능하게 하는 네트워크이다. 무선 메쉬 네트워크는 여러 기반의 무선 통신 기술들과 연동이 가능하며, ad-hoc 네트워크 등의 제한점과 결점을 보완하여 네트워크 성능을 개선할 수 있다[1]. 일반 무선랜과 메쉬 네트워크의 차이점은 <표 1>과 같다.

* 서울신학대학교 교양학부 교수

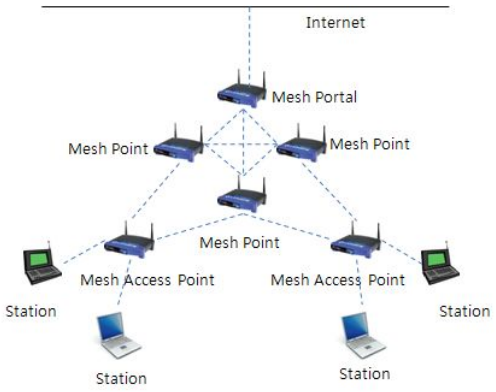
<표 1> 무선랜과 메쉬 네트워크의 특성 비교

항목	무선랜 네트워크	메쉬 네트워크
기능	단순 RF 처리	라우팅 정보를 활용하여 경로를 이중화
회선	AP까지 유선연결 필요	AP까지 유선연결 필요하지 않음
구성 형태	단독 구성	그물망 구조
장단점	AP 장애 시 서비스가 중단됨	메시 구조로 되어 있어서 하나의 AP 장애시에도 서비스 가능

무선 메쉬 네트워크는 메쉬 포인트들과 스테이션으로 구성되어 있으며, 다른 여러 종류의 네트워크와 통합이 가능한 네트워크 환경이다. 즉, 무선 메쉬 네트워크는 같은 종류의 네트워크뿐만 아니라 인터넷, 셀룰러, IEEE 802.11, IEEE 802.15, IEEE 802.16, 센서 네트워크 등을 메쉬 액세스 포인트에서 데이터 전송이 가능하도록 한다. 무선 메쉬 네트워크의 특징으로는 기존 ad-hoc 네트워크, WLANs(Wireless Local Area Networks), WPANs (Wireless Personal Area Networks) 그리고 WMANs (Wireless Metropolitan Area Networks)의 향상을 꾀할 수 있으며, 그 활용 분야는 더욱 확대되어질 것으로 예상되고 있다[2].

무선 메쉬 네트워크의 구성은 <그림 1>과 같다. 무선 메쉬 네트워크는 메쉬 포인트, 메쉬 액세스 포인트, 메쉬 포털 포인트, 스테이션의 네 가지 요소로 구성되어 있다.

- 메쉬 포인트(MP): WLAN 메쉬 서비스를 제공하는 요소
- 메쉬 액세스 포인트(MAP): 메쉬 포인트에 액세스 포인트의 기능을 추가, 메쉬 서비스와 AP 서비스를 동시에 지원
- 스테이션: 메쉬 액세스 포인트를 통하여 메쉬 네트워크에 액세스 할 수 있는 단말 장치
- 메쉬 포털 포인트(MPP): 무선 메쉬 네트워크 망이 다른 기반의 망이나 인터넷으로 연결을 유지시켜 주는 게이트웨이 역할을 수행



<그림 1> 무선 메쉬 네트워크 구성도

무선 메쉬 네트워크의 인프라 백본 구조는 다양한 무선 통신 기술과 IEEE 802.11에서 사용되고 있는 기술들에 의해서 구성되며, 이를 지원하기 위해서 메쉬 포인트는 자가 망 설정과 자가 망 복구를 제공하고, 게이트웨이 관련 기술을 통하여 인터넷에 연결되어 질 수 있다. 그러므로 이러한 방법을 통해 각각의 스테이션들을 위한 백본을 제공할 수 있게 되고, 메쉬 포인트에서 제공하는 게이트웨어/브리지 관련 기술을 통하여 존재하는 무선 네트워크를 무선 메쉬 네트워크로 결합을 가능하게 한다[3].

이러한 무선 메쉬 네트워크 환경에서 시스템에 대한 안전한 상호 인증은 필수 서비스로서 하나의 AP에 장애가 발생하면, 근접한 액세스 포인트에 무선 전송로를 제공해 라우팅이 가능해야 하며, 여러 기반의 무선 통신 기술들과 연동이 가능해야 하므로 효율적인 인증 서비스가 안전하게 제공되어야 한다. 그러므로 본 논문에서는 Kerberos[4]에서 사용되는 티켓을 이용한 인증방식을 제안하였다. 티켓의 가장 큰 장점은 재활용이 가능하다는 것이다. 기존의 인증방식은 핸드오프시 마다 인증서버와 상호작용을 필요로 하기 때문에 이를 개선한 인증 방식에 관한 연구를 수행하였다.

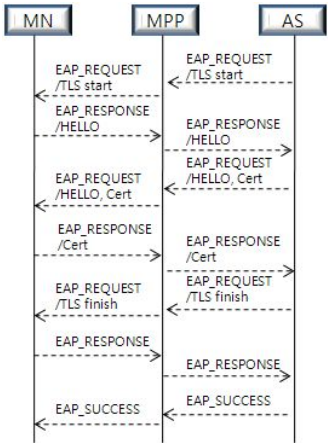
본 논문의 구성은 다음과 같다. 2장에서는 EAP-TLS와 Kerberos를 무선 메쉬 네트워크에 적용하는 방안에 대해서 기술하였으며, 3장에서는 제안한 인증 메커니즘에 대하여

설명하였다. 4장에서는 제안한 인증 메커니즘의 정형 명세 및 검증을 BAN로직을 이용하여 수행하였고, 5장에서는 EAP-TLS 방식과의 성능비교를 통해 그 효율성을 나타냈으며, 6장에서는 결론 및 향후 연구계획을 정리하였다.

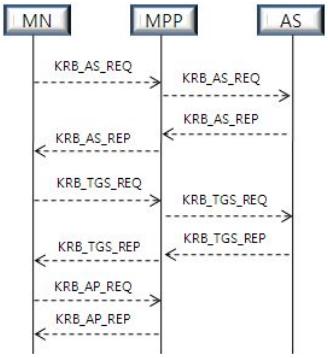
II. 다른 인증방식

2.1 무선 메쉬 네트워크에 EAP-TLS 적용

EAP-TLS(Transport Layer Security)는 널리 사용되는 인증 프로토콜로서, IEEE 802.11과 IEEE 802.16 등 대부분의 무선 네트워크들이 상호 인증 프로토콜로 사용하고 있다. EAP-TLS를 무선 메쉬 네트워크에 적용한 방안은 <그림 2>와 같다. EAP를 적용하는 방법은 AP에서 상호 인증을 위한 협상을 시작하기 위해 EAP request 메시지를 전송한다. EAP negotiation을 통하여 모바일 노드와 인증서버 간에 인증 프로토콜을 EAP-TLS를 사용하기로 결정하면, 모바일 노드와 인증서버는 상호인증을 수행하기 위해서 각자의 인증서와 키를 교환한다. 각 메시지에 대한 자세한 사항은 [5]에 제시되어 있다. EAP-TLS를 통해 인증서의 유효성 검증과 취소가 수행되어야 하며, 모



<그림 2> EAP-TLS 메시지 흐름



<그림 3> Kerberos 메시지 흐름

바일 노드는 새로운 네트워크로 이동하더라도 동일한 절차에 의해서 인증이 수행된다.

2.2 무선 메쉬 네트워크에 Kerberos 적용

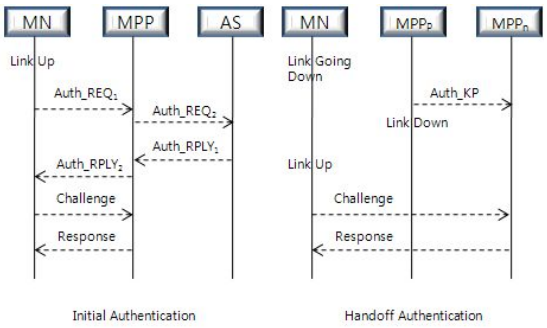
Kerberos는 분산 환경에 적용 가능한 인증서비스 이다[6]. 이 방식은 사용자가 자신의 ID와 비밀번호를 입력하면, 분산 서비스 서버의 다양한 서비스들을 이용할 수 있는 권한을 얻게 된다. Kerberos를 무선 메쉬 네트워크에 적용하기 위해서 메쉬 포털 포인트를 서비스 서버로 가정하면 적용이 가능하다.

<그림 3>은 Kerberos가 무선 메쉬 네트워크에 적용되는 것을 간략히 나타낸 것이다. 여기서는 티켓 부여(Ticket granting) 서버와 인증 서버(Authentication Server)가 동일한 개체에 있는 것으로 가정하였다. 좀 더 명확한 메시지의 의미는 [7]에 제시되어 있다. 여기서 모바일 노드는 이동시마다 티켓 부여 서버로부터 네트워크 서비스를 사용할 수 있는 권한을 허가받아야 한다.

III. 제안 인증 메커니즘

제안한 방식에서는 IEEE 802.21에서 2계층의 트리거(trigger) 기능을 사용한다는 것을 가정하였다[8]. 이 기능

은 모바일 노드가 다른 네트워크로 이동하였을 경우에 모바일 노드가 현재의 메쉬 포탈 포인트에 접속되어 있는 정보를 다른 메쉬 포탈 포인트로 전송하는 것을 가능하게 한다. 본 논문에서는 2개의 인증방식을 제안하였다. 첫 번째는 모바일 노드가 처음으로 무선 메쉬 네트워크에 접속할 때의 인증방법과 한 네트워크에서 다른 네트워크로 이동할 때인 핸드오프 인증방식이다.



<그림 4> 인증과정의 메시지 흐름

<그림 4>에서 초기 인증은 모바일 노드(MN)가 Link Up 되면 링크 계층의 트리거 기능에 의해 작업이 시작된다. 트리거 수행 후에는 모바일 노드, 메쉬 포탈 포인 (MPP), (AS) .
기능을 수행하기 위한 가정은 다음과 같다.

- 모든 모바일 노드와 메쉬 포탈 포인트는 IEEE 802.21 signaling이 가능
- 모바일 노드와 인증서버 간에 대칭키가 공유되어 있음
- 대칭키가 메쉬 포탈 포인트와 인증서버 간에 공유되어 있음
- 메쉬 포탈 포인트와 다른 메쉬 포탈 포인트 간에는 대칭키가 공유되어 있음
- 각각의 메쉬 포탈 포인트는 동기화 되어 있음
- 모바일 노드와 메쉬 포탈 포인트는 인증서버와 다른 메쉬 포탈 포인트에서 생성된 키를 신뢰함

3.1 초기 인증 메커니즘

<그림 4>의 초기 인증을 위한 메시지 흐름에 대한 설명을 위해 다음과 같은 기호를 정의하였다.

- ||: 연결(Concatenation) 관계
- $K_{A, B}$: A와 B의 대칭키는 K
- $E(Message)_K$: 메시지를 대칭키 K로 암호화

초기 인증에 대한 메시지의 설명은 다음과 같다.

- $Auth\_REQ_1$: $I_{MN}||I_{MPP}||Time||Nonce_1$
- $Auth\_REQ_2$: $Auth\_REQ_1||Nonce_2$
- $Auth\_RPLY_1$: $I_{MN}||Ticket||$ $E(K_{MN,\ MPP}||I_{MPP}||Time||Nonce_1)K_{MN,\ AS}||$ $E(K_{Auth}||I_{MPP}||Time||Nonce_2)K_{MPP,\ AS}$
- $Auth\_RPLY_2$: $I_{MN}||Ticket||$ $E(K_{MN,\ MPP}||I_{MPP}||Time||Nonce_1)K_{MN,\ AS}$
- Challenge: Ticket||Authenticator
- Response: $E(I_{MN}||Time||Nonce_3+1)K_{MN,\ MPP}$

여기에서 사용된 기호의 의미는 다음과 같다.

- Ticket: $(K_{MN,\ MPP}||I_{MN}||Time)K_{Auth}$
- Authenticator: $(I_{MN}||Time||Nonce_3)K_{MN,\ MPP}$
- I_{MN}, I_{MPP}: MN과 MPP의 유일한 식별자
- Time: 대칭키와 Ticket의 유효시간

Auth_REQ와 Auth_RPLY 메시지를 통해 모바일 노드는 인증서버에 의해 인증이 수행되고, MPP에 제시할 티켓을 받게 된다. 또한 Challenge와 Response 메시지에 의해 모바일 노드와 메쉬 포탈 포인트가 서로 간에 인증을 하게 된다. 메쉬 포탈 포인트가 모바일 노드로부터 티켓을 받을 때마다 메쉬 포탈 포인트는 인증서버로부터 받은 K_{AUTH} 키를 이용하여 티켓 값을 복호화한다. 이러

한 작업은 모바일 노드가 다른 메쉬 포탈 포인트로 이동할 때마다 발생한다. 또한 Nonce의 값은 최신성이 보장되어야 하고, 랜덤하게 생성되어야 한다.

3.2 핸드오프 인증 메커니즘

핸드오프 인증은 한 메쉬 포탈 포인트에서 다른 메쉬 포탈 포인트로 이동할 때 발생하는 인증 방법으로, 모바일 노드는 초기 인증 때 받은 티켓을 이용한다. 이를 위해서 기존의 메쉬 포탈 포인트에서 이동할 메쉬 포탈 포인트로 K_{AUTH} 키가 <그림 4>의 핸드오프 인증 메커니즘의 Auth_KP 메시지에 의해 전송된다.

핸드오프 인증에 대한 메시지의 설명은 다음과 같다.

- Auth_KP: $E(K_{AUTH}, I_{MN}, Time)K_{MPPp,\ MPPn}$
- Challenge: Ticket||Authenticator
- Response: $E(I_{MN}||Time||Nonce_4+1)K_{MN,\ MPP}$

링크 계층으로부터 Link Going Down 트리거 이후에 Auth_KP 메시지가 전송된다. 현재의 메쉬 포탈 포인트가(MPPp) 모바일 노드의 핸드오프를 확인하였을 때, 이동할 메쉬 포탈 포인트(MPPn)로 K_{AUTH}를 전송하여, 새로운 메쉬 포탈 포인트가 모바일 노드의 티켓 값으로 모바일 노드를 인증할 수 있도록 한다. 메시지의 최신성을 확인하기 위해서 Time의 값이 사용되었으며, 모든 MPP 사이에는 동기화가 되어있어야 한다.

IV. 유효성 검증

4.1 초기 인증 메커니즘 정형 명세 및 검증

제안한 알고리즘의 유효성을 제시하기 위해서 BAN 로직을 사용하였다. 인증 프로토콜의 기술을 위해 전통적인 보안 명세에서는 주체 사이에 단순히 메시지만을 나열하거나 상징적으로 보내는 사람, 받는 사람, 메시지의 내용들을 보여주는 것에 치중하였다. 그러나 이러한 명세는 로직에서 조작하기 힘들 뿐 아니라 메시지에 포함된 내용으로부터 명백한 의미를 얻어낼 수 없다. 따라서 보안 명세를 통해 프로토콜의 정확한 의미뿐만 아니라 주고받는 메시지의 의미를 명확히 나타낼 필요가 있다[9]. 그러므로 본 논문에서는 BAN 로직[10]을 이용하여 제시한 메커니즘을 정형 명세하고, 검증하고자 한다.

BAN 로직은 분산 네트워크 환경에서 개체들의 인증에 관한 프로토콜의 검증과 분석을 위하여 만들어진 로직이다. 정형명세를 위해서 사용된 표시들은 [13]에 제시된 표현을 사용하였다. 초기 인증의 목적을 BAN 로직을 이용하여 표현하면 다음과 같다.

<표 2> 초기 인증의 보안 목표

① $MN| \equiv MN \xleftrightarrow{K_{MN,MPP}} MPP$

② $MPP| \equiv MN \xleftrightarrow{K_{MN,MPP}} MPP$

③ $MN| \equiv MPP| \equiv MN \xleftrightarrow{K_{MN,MPP}} MPP$

④ $MPP| \equiv MN| \equiv MN \xleftrightarrow{K_{MN,MPP}} MPP$

초기 인증의 보안 목표는 MN과 MPP가 MN과 MPP의 대칭키인 $K_{MN,\ MPP}$로 암호화 하는 것을 서로 신뢰하는 것을 목표로 한다. 초기 인증을 위한 가정은 <표 3>과 같다.

<표 3> 초기 인증을 위한 가정

① $MN| \equiv MN \xleftrightarrow{K_{MN,AS}} MPP$

② $MPP| \equiv MPP \xleftrightarrow{K_{MPP,AS}} AS$

③ $MN| \equiv (AS| \sim MN \xleftrightarrow{K_{MN,MPP}} MPP)$

④ $MPP| \equiv (AS| \sim MN \xleftrightarrow{K_{MN,MPP}} MPP)$

⑤ $MPP \mid \equiv (AS \mid \sim MPP \overset{K_{AUTH}}{\longleftrightarrow} AS)$
⑥ $MN \mid \equiv \#(Nonce_1)$
⑦ $MPP \mid \equiv \#(Nonce_2)$
⑧ $MPP \mid \equiv \#(Nonce_3)$
⑨ $MPP \mid \equiv \#(Time)$

초기 인증 메커니즘을 BAN 로직을 이용하여 표현하면 <표 4>와 같이 나타낼 수 있다.

<표 4> 초기 인증 메시지

① Auth_REQ1: $I_{MN}, I_{MPP}, Nonce_1$
② Auth_REQ2: $I_{MN}, I_{MPP}, Nonce_1, Nonce_2$
③ Auth_RPLY1:
MPP$\lhd \{MPP \overset{K_{AUTH}}{\longleftrightarrow} AS, Nonce_2\} K_{MPP,AS}$
④ Auth_RPLY2:
MN$\lhd \{MN \overset{K_{MN,MPP}}{\longleftrightarrow} MPP, Nonce_2\} K_{MN,AS}$
⑤ Challenge:
MPP$\lhd (\{MN \overset{K_{MN,MPP}}{\longleftrightarrow} MPP, Time\} K_{AUTH}$,
$\{MN, None_3\} K_{MN,MPP})$
⑥ Response: MN$\lhd \{Nonce_3 + 1\} K_{MN,MPP}$

제시한 초기 인증 알고리즘을 증명하기 위해서 BAN 로직에 있는 Message-meaning rule, Nonce-verification rule 그리고 Jurisdiction rule을 사용하였다.

<표 4>의 초기 인증 메시지에서 ①과 ②는 단순히 정보만을 전송하므로, ③의 Auth_RPLY$_1$에 대해서 살펴보면, <표 3>의 ②의 규칙과 Message-meaning rule을 적용하면 다음과 같은 값을 얻을 수 있다.

$$MPP \mid \equiv AS \mid \sim (MPP \overset{K_{AUTH}}{\longleftrightarrow} AS, Nonce_2) \quad (1)$$

(1)의 수식에 Nonce-verification rule과 <표 3>의 가정 ⑦을 적용하면

$$MPP \mid \equiv AS \mid \equiv (MPP \overset{K_{AUTH}}{\longleftrightarrow} AS, Nonce_2) \quad (2)$$

(2)의 수식에 Elimination rule을 적용하면,

$MPP \mid \equiv AS \mid \equiv MPP \overset{K_{AUTH}}{\longleftrightarrow} AS$이고,

여기에 Jurisdiction rule을 적용하면, (3)을 얻을 수 있다.

$$MPP \mid \equiv MPP \overset{K_{AUTH}}{\longleftrightarrow} AS \quad (3)$$

Auth_RPLY$_2$에 대해서도 동일한 과정을 적용하면 다음과 같은 값을 얻을 수 있다.

$$MN \mid \equiv MN \overset{K_{MN,MPP}}{\longleftrightarrow} MPP \quad (4)$$

그러므로 <표 2>의 목표 중 ①의 값을 만족시킨다.

또한, Challenge 메시지에 Nonce-verification rule, Jurisdiction rule과 Elimination rule을 적용하면 (5)와 (6)을 얻을 수 있다.

$$MPP \lhd \{MN \overset{K_{MN,MPP}}{\longleftrightarrow} MPP, Time\} K_{AUTH} \quad (5)$$

$$MPP \lhd \{MN, Nonce_3\} K_{MN,MPP} \quad (6)$$

(3)의 식과 (5)의 식에 Message-meaning rule을 적용하면 (7)을 구할 수 있으며,

$$MPP \mid \equiv AS \mid \sim (MN \overset{K_{MN,MPP}}{\longleftrightarrow} MPP) \quad (7)$$

(7)의 수식에 <표 3>의 ⑨의 가정과 Nonce-verification rule을 적용하고, <표 3>의 ④의 가정과 Jurisdiction rule을 적용하면, (8)과 (9)의 값을 얻게 된다.

$$MPP \mid \equiv AS \mid \equiv (MN \overset{K_{MN,MPP}}{\longleftrightarrow} MPP) \quad (8)$$

$$MPP \mid \equiv MN \overset{K_{MN,MPP}}{\longleftrightarrow} MPP \quad (9)$$

즉 (9)의 수식이 <표 2>의 ②의 목적을 달성하는 것을 알 수 있다. (6)의 식에 Message-meaning rule과 Nonce-verification rule을 적용하면, (10)의 식을 얻을 수 있다.

$$MPP \mid \equiv MN \mid \equiv MN \overset{K_{MN,MPP}}{\longleftrightarrow} MPP \quad (10)$$

(10)의 수식은 <표 2>의 ④의 목적을 달성하는 것을 알 수 있다. <표 4>의 ⑥인 Response 메시지에

Message-meaning rule과 Nonce-verification rule을 적용하면, (11)의 식을 구할 수 있다.

$$MN| \equiv MPP| \equiv MN \xleftrightarrow{K_{MN,MPP}} MPP \quad (11)$$

(11)의 수식은 ③의 조건을 만족하므로, <표 2>의 모든 조건이 만족하는 것을 증명하였다.

4.2 핸드로프 인증 메커니즘 정형 명세 및 검증

핸드로프 인증 메커니즘의 보안 목적은 모바일 노드가 새로운 네트워크로 이동하였을 경우에 새로운 네트워크에서 인증이 되도록 하는 것이다. 이동할 메쉬 포탈 포인트를 MPPn라 하고, 이동하기 전의 메쉬 포탈 포인트를 MPPp라 하면, 핸드오프 인증 목적은 <표 5>와 같이 나타낼 수 있다.

<표 5> 핸드오프 인증의 보안 목표

① $MN| \equiv MN \xleftrightarrow{K_{MN,MPPn}} MPPn$

② $MPPn| \equiv MN \xleftrightarrow{K_{MN,MPPn}} MPPn$

③ $MN| \equiv MPPn| \equiv MN \xleftrightarrow{K_{MN,MPPn}} MPPn$

④ $MPPn| \equiv MN| \equiv MN \xleftrightarrow{K_{MN,MPPn}} MPPn$

<표 5>의 핸드오프의 보안 목적은 모바일 노드와 새로 이동한 메쉬 포탈 포인트간에 안전한 인증을 수행하는 것이다. 핸드오프 인증을 위한 가정은 <표 6>과 같다.

<표 6> 핸드오프 인증을 위한 가정

① $MPPn| \equiv MPPp \xleftrightarrow{K_{MPPp,MPPn}} MPPn$

② $MPPn| \equiv (MPPp| \sim MPPn \xleftrightarrow{K_{AUTH}} AS)$

③ $MPPn| \equiv (AS| \sim MN \xleftrightarrow{K_{MN,MPPn}} MPPn)$

④ $MPPn| \equiv \#(Time)$

<표 6>의 내용은 이동전 메쉬 포탈 포인트(MPPp)와 이동후의 메쉬 포탈 포인트(MPPn) 간에 공유 비밀키가 수립되어 있어야 하며, 인증서버(AS)와 MPPn 그리고 모바일 노드(MN)와 MPPn의 비밀 공유키가 설정되어 있다는 것을 가정한 것이다. BAN 로직을 이용하여 핸드오프 인증 메커니즘을 나타내면 <표 7>과 같다.

<표 7> 핸드오프 인증 메시지

① Auth_KP:
MPPn◁ $\{MPPn \xleftrightarrow{K_{AUTH}} AS, Time\} K_{MPPp,MPPn}$

② Challenge:
MPPn◁ $(\{MN \xleftrightarrow{K_{MN,MPPn}} MPPn, Time\} K_{AUTH},$
$\{MN, None_3\} K_{MN,MPPn})$

③ Response:
MN◁ $\{None_3 + 1\} K_{MN,MPPn}$

MN과 MPPn 사이에 사용된 키는 초기 인증시에 사용된 키와 같다. 즉 $K_{MN, MPP}$가 $K_{MN, MPPn}$으로 사용이 되며, 키의 생명주기가 끝날 때까지 모바일 노드의 인증에 사용이 된다. 핸드오프 인증 메커니즘의 메시지의 Challenge와 Response 메시지는 초기 인증시에 사용된 방법과 동일하며, 여기에서 중요한 기능은 MPPp에서 MPPn으로 K_{AUTH}를 전송하는 방법과 MPPn이 K_{AUTH} 값을 신뢰할 수 있어야 한다.

<표 7>의 ①의 메시지에 <표 6>의 가정 ①, ④와 Message-meaning rule, Nonce-verification rule을 적용하면 (12)의 식을 얻을 수 있다.

$$MPPn| \equiv MPPp| \equiv MPPn \xleftrightarrow{K_{AUTH}} AS \quad (12)$$

(12)의 식에 <표 6>의 가정 ②와 Jurisdiction rule을 적용하면, (13)의 식을 얻을 수 있다.

$$MPPn| \equiv MPPn \xleftrightarrow{K_{AUTH}} AS \quad (13)$$

즉, MPPn은 AS로부터 안전하게 K_{AUTH}의 값을 얻을

수 있다. <표 5>의 핸드오프의 보안 목적을 만족시키기 위한 증명방법은 4.1의 증명방법과 유사하다.

Ⅴ. 성능평가

제시한 알고리즘 성능을 평가하기 위해서 EAT-TLS와 제안한 알고리즘의 적용시의 성능을 비교분석하였다. 성능평가는 Square-shaped 네트워크 모델에서 fluid-flow 이동 모델[11]을 이용하였다. MPP의 영역을 d, AS의 영역을 D라고 하면, 각각의 영역이 교차될 확률 r_m(MPP)과 r_a(AS)은 다음과 같이 나타낼 수 있다.

$$r_m = \frac{\rho v d}{\pi},\ r_a = \frac{\rho v D}{\pi}$$

단, ρ는 균일하게 분포되어 있는 모바일 노드의 밀집도를 나타내며, v는 $[0,2\pi]$ 상에서 균일하게 분산된 방향으로 움직이는 모바일 노드의 속도를 표시한다. 성능평가에 사용된 인자의 정의와 시뮬레이션에 사용된 값은 다음의 <표 8>과 같다.

<표 8> 성능평가를 위한 인자설정

설명	기호	값
암호화 비용	C_e	1
복호화 비용	C_d	1
키 생성 비용	C_k	1
한 홉당 전송 비용	C_t	10
인증서 유효성 검증	C_c	10
유선구간의 전송 비용	T_c	1
무선구간의 전송 비용	T_w	1.5
MPP와 AS간의 홉 수	$H_{MPP,AS}$	5
MPP와 MPP간의 홉 수	$H_{MPP,MPP}$	1
MPP 영역의 경계 값	d	120
MPP의 개수	n	100

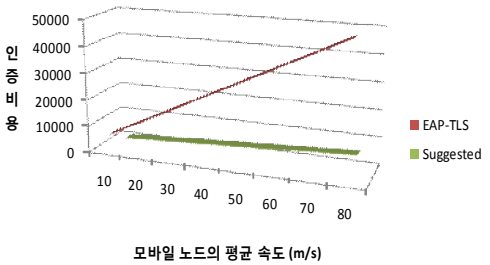
<그림 2>에서 제시된 바와 같이 EAP-TLS를 통한 인증에서는 8번의 유선과 무선구간의 전송이 일어나며, 모바일 노드와 인증서버에서 인증서 확인 작업과 키 생성 작업이 발생한다. 이를 수식으로 나타나면 다음과 같이 나타낼 수 있다.

$$T_{EAP-TLS} = [8(T_w + T_c H_{MPP,AS})C_t + 2C_c + 2C_k]r_m n$$

제안한 알고리즘(T_{sug})에 대해서도 수식적으로 표현이 가능하다. 제안한 알고리즘은 초기 인증과 핸드오프 인증으로 구성되어 있으며, 초기 인증은 모바일 노드가 처음으로 메쉬 포탈 포인트에 접속할 때 발생하고, 핸드오프 인증은 모바일 노드가 다른 네트워크로 이동할 때 발생하게 된다. 이를 정리하면 다음과 같다.

$$T_{sug} = [(4T_w + 2T_c H_{MPP,AS})C_t + 5(C_e + C_d) + 2C_k]r_a$$
$$+ [(2T_w + T_c H_{MPP,MPP})C_t + 3(C_e + C_d)](r_m n - r_a)$$

제안한 알고리즘과 기존 EAP-TLS의 성능을 비교하기 위해서 $n = 100, \rho = 0.0003$인 경우에 모바일 노드의 속도에 따른 인증비용에 대한 분석을 수행하였다. 수학적 분석을 수행한 결과는 <그림 5>와 같다.

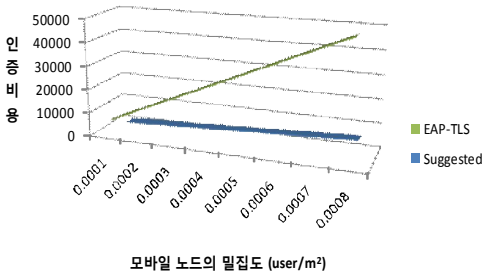


<그림 5> 모바일 노드의 속도에 따른 인증비용의 비교

<그림 5>에 제시된 바와 같이, 성능평가를 수행한 결과를 보면, 무선 메쉬 네트워크에 EAP-TLS를 적용하는 것보다는 본 논문에서 제안한 인증 알고리즘을 적용하는

것이 비용효과적인 측면에서 우수한 것을 알 수 있다. 또한 모바일 노드의 평균 속도가 높아질수록 인증 비용 측면에서 제안한 알고리즘의 성능이 좋아지는 것을 알 수 있다.

<그림 6>은 동일한 공간과 속도($n=100, v=30$)에서 모바일 노드의 밀집도를 변화시켜 가면서 인증비용을 비교한 것이다. 모바일 노드의 밀집도가 높아질수록 제시한 알고리듬이 인증비용 측면에서 더 우수한 것을 알 수 있다. 단, 제시한 알고리즘에서는 메쉬 포탈 포인트간에 동기화가 되어있어야 한다는 전제 조건을 가지고 있다.



<그림 6> 모바일 노드의 밀집도에 따른 인증비용의 비교

VI. 결론

무선 메쉬 네트워크는 최근 주요 이슈가 되고 있는 네트워크 기술로서 그 활용분야가 더욱 확대될 것으로 예상되고 있다. 그러므로 본 논문에서는 무선 메쉬 네트워크 환경에서 안전하고 효율적으로 시스템을 인증할 수 있는 인증 방안에 대한 연구를 수행하였다.

본 논문에서 제시한 인증 알고리즘의 안전성을 제시하기 위해 BAN 로직을 이용하여 그 유용성을 증명하였으며, 성능평가를 통해 기존에 사용하던 인증 알고리즘보다 인증비용 측면에서 더 효율적임을 수학적인 분석을 통해 제시하였다.

향후 연구계획으로는 QoS 측면에서 메쉬 무선 네트워크의 성능을 분석하여 유비쿼터스 환경에서 효율적으로 작업이 수행될 수 있는 주요 성능 인자 및 관리 방안에 대한 연구를 수행할 것이다.

참고문헌

[1] IEEE Wireless LAN Edition, A compilation based on IEEE std 802.11tm. 1999(R2003) and its Amendments, IEEE, 2003.

[2] IEEE P802.11S/D1.0: Draft Amendment to Standard for Information Technology-Telecommunications and Information Exchange Between Systems -LAN/MAN Specific Requirements - Part II: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Amendment: ESS Mesh Networking, Nov. 2006.

[3] 조규철, 한기준, "유비쿼터스 메쉬 네트워크 경로 재설정 기법", 인터넷정보학회지 제9권 2호, 2008년 6월.

[4] Web page of Krb Working Group: http://www.ietf.org/html.charters/krb-wg-charter.html.

[5] D. Simon, B. Aboba, and R. Hurst, "The EAP-TLS Authentication Protocol", RFC 5216, Mar. 2008.

[6] W. Stallings, "Cryptography and Network Security Principles and Practices", 2006.

[7] C. Neuman, T. Yu, S. Hartman, and K. Raeburn, "The Kerberos Network Authentication Service(V5)", RFC 4120, July 2005.

[8] V. Gupta, D. Johnston, "IEEE 802.21 A Generalized Model for Link Layer Triggers", IEEE 802.21 Media Independent Handoff Working Group, March 2004.

[9] 김영갑, 문창주, 박대하, 백두권, "OSGi 서비스 플

랫폼 환경에서 서비스 번들 인증 메커니즘의 검증 및 구현", 정보과학회 논문지 31권 1호, 2004년 2월.
[10] M. Burrows, M. Abadi, R. Needham, "A Logic of Authentication", ACM Transactions on Computer Systems, Feb. 1990.
[11] S. Park, N. Kang, and Y. Kim, "Localized Proxy-MIPv6 with Route Optimization in IP-Based Network", IEICE Transaction Communication, Dec. 2007.

■ 저자소개 ■

김 태 경
Kim, Tae Kyung

2008년 3월~현재
서울신학대학교 교양학부 교수
2006년 3월~2008년 2월
서일대학 정보기술계열
정보전자전공 교수
2005년 8월 성균관대학교
전기전자및컴퓨터공학과(공학박사)
2001년 8월 성균관대학교
전기전자및컴퓨터공학과(공학석사)
1997년 2월 단국대학교 수학교육과 (이학사)

관심분야 : 네트워크보안, 그리드 네트워크, USN
E-mail : tkkim@stu.ac.kr

논문접수일 : 2009년 8월 13일
수 정 일 : 2009년 9월 3일
게재확정일 : 2009년 9월 10일