

논문 2007-44TC-5-8

# 무선 메쉬 네트워크의 패스워드 기반 인증 프로토콜

( A Novel Authentication Protocol based on the Password scheme for  
Wireless Mesh Network )

이 규 환\*, 이 주 아\*, 김 재 현\*\*

( Kyu-hwan Lee, Ju-a Lee, and Jae-hyun Kim )

## 요 약

본 논문에서는 무선 메쉬 네트워크에서 사용자의 편의를 위하여 패스워드 기반 방식의 인증 프로토콜을 제안한다. 제안하는 프로토콜의 성능 분석을 위해서 GNY Logic 분석, Security 분석, 전송지연시간 분석을 하였다. 우선 GNY logic 분석을 통하여 프로토콜의 신뢰성을 증명하였으며, 다양한 공격에 대한 Security 분석을 통하여 인증 프로토콜이 여러 가지 공격에 대하여 강한 면모를 가지고 있는 것을 보였다. 또한 전송지연시간 분석으로 제안하는 인증 프로토콜이 무선 메쉬 네트워크 내에서 데이터 전송 지연에 큰 영향을 미치지 않음을 증명하기 위해 Linux 시스템에서 구현하여 전송지연시간을 측정하였다. 이러한 세 가지 분석 결과 제안하는 인증 프로토콜은 무선 메쉬 네트워크의 성능에 큰 영향을 미치지 않으면서도 안전한 무선 메쉬 네트워크 환경을 제공한다는 것을 보였다.

## Abstract

We propose a novel authentication protocol for wireless mesh network. The proposed authentication protocol is based on the password scheme for convenience of users. The proposed protocol is evaluated through three analyses. The correctness of the proposed protocol is proved using the GNY analysis. By the security analysis, we show that the proposed protocol is resistant to various attacks. For the performance analysis, we implemented the protocol in Linux operating system based laptop and measured the transmission time. The analytic results show that the proposed protocol provides the secure wireless mesh network without considerable performance degradation.

**Keywords** : authentication protocol, wireless mesh network, password

## I. 서 론

현재 사용되거나 각광 받고 있는 무선 기술은 무선랜과 블루투스, UWB 등이 있다. 이러한 다양한 무선 네트워크의 원활한 통신과 무선 네트워크의 범위가 미치지 않는 음영 지역을 위해서는 무선 메쉬 네트워크가 지원이 되어야 한다. 무선 메쉬 네트워크는 유선 메쉬 네트워크에서와 같이 주변의 노드들을 그물과 같은 네

트워크로 구성하기 위해 멀티 홉 무선 통신을 지원한다. 무선 메쉬 네트워크는 노드의 이동에 제약이 없고, 네트워크를 동적으로 구성할 수 있는 장점이 있으며 일반적인 기반 망에 기초한 네트워크의 전개가 용이하지 않을 경우 사용될 수 있다. 그러나 동적인 토폴로지 변화, 중앙의 감시와 관리의 부족, 자원의 제약성, 무선 매체의 사용 등의 요인들로 다양한 공격에 노출되기 쉽다. 또한 노드의 신분이 서로에게 불확실한 경우가 많으며 멀티 홉 방식에 의해 라우팅을 할 경우 중간 노드에 의해 발생할 수 있는 데이터 보안 문제도 존재한다. 따라서 무선 메쉬 네트워크에서는 적합한 사용자임을 증명 받은 노드만이 네트워크 자원을 이용하게 해주는 인증 과정이 중요한 문제이다. 무선 메쉬 네트워크에서

\* 학생회원, \*\* 정회원, 아주대학교 전자공학과  
(Ajou University)

※ “이 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음” (IITA-2006-(C1090-0602-0011))

접수일자: 2007년5월1일, 수정완료일: 2007년5월14일

의 인증은 일반적인 기반 망에 기초한 네트워크와 달리 중앙 관리자가 존재하지 않음을 염두에 두어야 한다. 또한 멀티 홉 통신을 위하여 인증 프로토콜은 인증 과정이 복잡하지 않고 빠르게 처리될 수 있어야 하며 데이터를 중계해주는 중간 노드의 안전성도 증명되어야 한다. 이를 위해서는 데이터를 전송하기 전에 별도의 인증 과정을 거치는 것보다 라우팅 과정과 동시에 인증 과정을 수행하는 것이 효율적이다. 따라서 본 논문에서는 라우팅 과정에 기초하여 중앙 관리자 역할의 노드 없이도 빠르고 안전하게 인증을 할 수 있는 기법을 제안한다.

무선 메쉬 네트워크는 멀티 홉 통신에 의해 네트워크를 구성하기 때문에 빠르게 인증을 수행할 수 있는 패스워드 방식을 제안하며 사용자의 개입을 최소화 하고, 관리하기 쉽게 하기 위하여 기기 인증 방식을 제안한다. 또한 이러한 인증 기법을 홈 네트워크에 적용하고, 홈 네트워크의 특성을 고려하여 홈 네트워크의 소유자 뿐만 아니라 방문자도 사용할 수 있도록 하기 위해 호스트 인증과 더불어 게스트 인증 방식도 제안한다.

본 논문의 구성을 살펴보면 II장에서는 기존의 라우팅을 이용한 인증 프로토콜에 대하여 살펴보고, III장에서는 무선 메쉬 네트워크의 특성에 맞는 인증 프로토콜을 제안하며 IV장에서는 제안한 인증 프로토콜을 분석하며 V장에서 결론을 맺는다.

## II. 관련 연구

무선 메쉬 네트워크에서 인증을 위한 방안은 신뢰된 노드를 이용하는 방식, 클러스터를 이용하는 방식, 라우팅을 이용하는 방식 등 여러 가지가 제안되었다. 그 중에서 제 3의 신뢰된 노드를 이용하는 방식<sup>[2],[3]</sup>은 인증을 원하는 모든 노드들이 언제나 신뢰된 노드와 연결이 가능해야 하므로 완전한 무선 메쉬 네트워크를 위한 인증 방식이라고 할 수 없다. 클러스터를 이용하는 방식<sup>[4]</sup>은 무선 메쉬 네트워크를 클러스터 단위로 구분한다. 각 클러스터의 클러스터 헤드가 신뢰된 노드의 역할을 하여 인증서를 발급하거나 공개키를 생성하기 때문에 클러스터에 속하는 모든 노드들은 언제든지 신뢰된 노드로의 접근이 가능하다. 그러나 클러스터 헤드가 공격을 받거나 제 역할을 못하면 해당 클러스터에 속한 노드들 모두에게 영향을 미치는 단점이 있다. 라우팅을 이용한 인증 방식들<sup>[5]-[8]</sup>은 무선 메쉬 네트워크(에드 혹 네트워크)의 노드들이 라우팅을 하는 동시에 인증을 수

행한다. 그 중 ARAN (Authenticated Routing for Ad hoc Networks) 프로토콜<sup>[5]</sup>은 인증서를 이용한 라우팅 기법이다. ARAN에서 소스 노드는 경로 발견 메시지를 브로드캐스트하며 각 경로 발견 메시지는 소스 노드에서 목적 노드로 이르는 각 홉에서 인증된다. 따라서 경로 요청과 응답 과정에서 모든 노드들은 라우팅 관련 작업을 수행하고 패킷을 전송할 때마다 자신의 인증서를 부가적으로 추가하여 전송해야 하는 단점이 있다. 또한 인증서를 이용한 인증 방식은 다른 방식보다 오랜 시간이 소요되며 각 노드는 언제나 인증 서버와 연결이 가능해야 한다<sup>[6]</sup>. SRP (Secure Routing Protocol) 프로토콜<sup>[7]</sup>은 임의의 두 단말 상에 공유된 비밀 키를 가정한다. SRP의 가장 큰 문제는 경로 요청 노드와 목적 노드 간에 존재하는 중간 노드에 대한 인증 과정이 없다는 것이다<sup>[8]</sup>.

앞에서 설명한 여러 가지 인증 방식 중에서 라우팅을 이용한 인증 기법은 호스트와 게스트가 존재하는 홈 네트워크 환경을 고려하지 않았다. 그리고 무선 메쉬 네트워크에서는 시간이 오래 소요되고 관리하기 어려운 인증서는 적당하지 않기 때문에 제안하는 인증 프로토콜에서는 빠르게 인증을 수행할 수 있는 패스워드 방식을 이용한다. 또한 본 논문에서는 중간 노드에 의한 공격을 방지하기 위하여 중간 노드에 대한 인증도 수행하도록 한다.

## III. 제안하는 인증 프로토콜

### 1. 가정 사항

기존의 인증 방식에서 사용자가 인증 설정을 위해서는 컴퓨터 지식이 있어야 하며 인증과 관련된 전문 용어를 알아야 했다. 그러나 이는 사용자의 보안 설정을 어렵게 하여 홈 네트워크 보안에 큰 공백을 야기할 수 있다. 이를 위하여 제안하는 인증 프로토콜에서는 사용자가 편리하게 인증 방식을 사용할 수 있도록 패스워드 방식을 사용하며 특정 창에서 키를 설정하는 것이 아니라 기기 인증을 통하여 자동으로 수행할 수 있도록 한다. 기기 인증은 사용자가 USB 같은 저장 장치를 기기에 연결하는 형태로 이루어질 수 있으며 근거리 무선 통신을 이용하여 이루어질 수도 있다.

기기 인증은 노드들에게 호스트 키와 인증을 위한 상수  $HC_n$ 을 안전하게 분배하기 위한 과정이다. 여기서  $n$ 은  $HC$ 의 수열을 의미하며 1부터  $m$ 까지 가능하고,  $m$ 은 상수의 최대 사용 개수이다. 노드  $i$ 는 여러 개의

$HC_n$  중에서 특정 상수 한 개를 선택하여 인증을 수행하도록 하며 이것을  $HC_i$ 라고 한다. 기기 인증 단계를 거친 노드  $i$ 는 다음 연산을 거쳐 무선 메쉬 네트워크의 소유자의 기기인 호스트를 인증하기 위하여 사용하는  $HAK_i$  (host authentication key)를 얻는다.

$$HAK_i = (K_H, MADDR_i), \quad (1)$$

여기서  $K_H$ 는 호스트 키를 의미하여  $MADDR_i$ 는 노드  $i$ 의 MAC 주소를 의미한다.  $hash(a, b)$ 는  $a$ 와  $b$ 를 입력 값으로 하는 해쉬 함수의 결과 값이다.

본 논문에서는 무선 메쉬 네트워크를 적용한 홈 네트워크를 가정하였으므로 인증 프로토콜은 홈 네트워크의 특성을 고려하여 홈 네트워크의 일시적인 방문자인 게스트에 대해서도 고려해야 한다. 게스트는 홈 네트워크 소유자의 노드가 아니면서 홈 네트워크를 일시적으로 방문하여 접속하기를 원하는 노드를 말한다. 게스트 키 정보는 홈 서버에서 주기적으로 변경시키며 홈 네트워크 내의 호스트 노드들에게 브로드캐스트하여 알려준다. 또는 호스트 인증 과정에서 인증 응답 메시지를 보낼 때 게스트 키에 관한 정보도 포함하여 전송한다.  $HAK_i$ 와 마찬가지로  $GAK_i$  (Guest Authentication Key)는 게스트 인증을 위하여 사용되며 다음과 같은 계산으로 얻을 수 있다.

$$GAK_i = (K_G, MADDR_i), \quad (2)$$

여기서,  $K_G$ 는 게스트 키를 의미한다.

## 2. 호스트 인증 기법

본 절에서는 홈 네트워크 소유자의 노드를 인증하기 위한 호스트 인증 기법을 제안한다. 그림 1에서와 같이 소스 노드 A, 중간 노드 B, 목적 노드 C가 있다고 가정한다. 호스트 인증 순서는 그림 1에서의 번호 순서대로 이루어지며 상세한 내용은 다음과 같다.

단계 1: 소스 노드 A는 라우팅 요청 메시지를 브로드캐스트하며 이 메시지를 전송할 때 다음과 같은 인증 요청 메시지를 함께 전송한다.

$$A \rightarrow \text{broadcast} : \text{host}, ID, \{HC_A, K_A, t_A\}_{HAK_A}, HMAC, \quad (3)$$

이때  $A \rightarrow \text{broadcast} : M$ 은 노드 A가 메시지 M을 브로드캐스트 했다는 것을 의미하며  $\{*\}_K$ 는  $*$ 을 키 K로 암호

화한 것을 의미한다.  $host$ 는 노드 A가 호스트 기기임을 의미하며,  $ID$ 는 노드 A에서 랜덤하게 생성한 메시지 ID이다.  $HC_A$ 는 기기 인증 과정에서 부여 받은 상수  $HC_n$  중의 하나로 노드 A가 랜덤하게 선택 한 값이다.  $HC_A$ 는 노드들이 동일한 비밀 정보를 공유하고 있는지를 확인하는데 사용한다.  $K_A$ 는 노드 A에서 랜덤하게 생성한 키이다.  $t_A$ 는 A에서의 시스템 시간이며 replay 공격을 방지하기 위해 사용한다.  $HC_A, K_A, t_A$ 는  $HAK_A$ 로 암호화되어 전송되며  $HMAC$ 은 Hashed Message Authentication Code로 라우팅 메시지를 포함한 전체 메시지의 해쉬 값으로 무결성을 확인하기 위해 사용된다.

단계 2: 메시지를 받은 이웃 노드 B는 라우팅 요청 메시지를 받으면 메시지에 실려 있는 노드 A의 MAC 주소를 얻어내고, 인증 메시지의 종류가 호스트인지 게스트인지를 확인한다. 호스트 인증이라면 기기 인증 때 부여 받은 호스트 키를 이용하여  $HAK_A$ 를 생성한다. 생성된  $HAK_A$ 를 이용하여 메시지를 복호화하여  $HC_A$  정보를 얻어내고 중간 노드 B가 기기 인증 때 부여 받은  $HC_i$ 와 비교하여 동일한 값이 존재하는지 찾아본다. 노드 B는 노드 A가 적합한 사용자라고 판단을 하면 노드 A가 보내 온  $ID, K_A, HC_A$  정보와 노드 A의 MAC 주소 정보를 라우팅 정보와 함께 유지하여 라우팅 응답 메시지를 보낼 때 사용하도록 한다.

단계 3: 중간 노드 B는 다시 인증 요청 메시지를 생성하여 브로드캐스트한다.

$$B \rightarrow \text{broadcast} : \text{host}, ID, \{HC_B, K_B, t_B\}_{HAK_B}, HMAC. \quad (4)$$

단계 4: 메시지를 받은 목적 노드 C는 동일한 방법으로  $HAK_B$ 를 생성하여 메시지를 복호화하고 중간 노드 B가 보내온 메시지를 인증한다. 목적 노드 C는 라우팅 알고리즘에 따라 효율적인 경로를 선택하고 라우팅 응답 메시지를 전송한다. 여기서는 A-B-C 경로를 가정한다.

단계 5: 목적 노드 C는 중간 노드 B에게 라우팅 응답 메시지를 전송할 때 다음과 같은 인증 응답 메시지를 함께 전송한다.

$$C \rightarrow B : \text{host}, ID, \{HC_C^{**}, t_C, L_C, K_G, T_G\}_{K_B}, HMAC, \quad (5)$$

여기서  $HC_C^{**}$ 는  $hash(HC_B, MADDR_C)$ 이고,  $ID$ 는 전송 받은 인증 요청 메시지의  $ID$ 이다. 만일 노드 C가 홈 네트워크 내에서 이미 인증된 노드이고, 홈 서버로부터 게스트 키 정보를 전송 받았다면 노드 C는 이러한 정보를 인증 응답 메시지를 통하여 다른 노드들에게 알려준다.  $L_G$ 는 게스트 키의 길이이며  $K_G$ 는 게스트 키,  $T_G$ 는 게스트 키의 유효 시간 정보이다. 이러한 정보는 인증 요청 메시지에 실려 있던 노드 B에서 랜덤하게 생성한 키인  $K_B$ 를 이용하여 암호화되어 전송한다.

단계 6: 인증 응답 메시지를 받은 노드 B는  $K_B$ 를 이용하여 메시지를 복호화하고  $HC_C^{**}$  정보가 올바른지 확인한다. 그리고 게스트 키 정보를 받아들이며 A에게 동일한 방법으로 인증 응답 메시지를 전송한다.

단계 7: 소스 노드 A는 마찬가지로  $HC_B^{**}$  정보와 게스트 키 정보를 확인하여 라우팅 과정을 마치고 이후에 전송되는 데이터는  $K_A$ 에 기반을 둔키를 생성하여 암호화한다.

### 3. 게스트 인증 기법

게스트 인증은 홈 네트워크를 일시적으로 사용하기 원하는 노드를 인증하기 위한 인증 기법이다. 소스 노드 A는 게스트 노드이며 홈 네트워크에 접속하기 위해서는 홈 네트워크 소유자가 직접 게스트 키 정보를 입력해주어야 한다. 게스트 키는 홈 서버에서 주기적으로 생성하여 홈 네트워크 내의 노드들에게 알려주며 홈 네트워크 소유자가 알 수 있도록 화면에 출력해주는 형태가 되어야 한다. 중간 노드 B와 목적 노드 C는 호스트 노드이며 호스트 인증 과정을 통하여 게스트 키를 알거나 또는 홈 서버로부터 주기적으로 게스트 키 정보를 전송 받는다. 게스트 인증에서는 호스트 인증 과정에서 사용되던  $HAK_i$ 와  $HC_i$ 를 대신하여  $GAK_i$ 와  $GC$ 를 사용한다. 여기서  $GC$ 는 게스트 키를 해쉬한 값이다.

그림 1에서와 같이 소스 노드 A, 중간 노드 B, 목적 노드 C가 있다. 노드 A는 게스트 노드이고 노드 C는 호스트 노드로 가정하고, 게스트 인증의 순서는 그림 1에서와 같고 자세한 설명은 아래에 기술되어 있다.

단계 1: 소스 노드 A는 라우팅 요청 메시지를 브로드캐스트하며 이 메시지를 보낼 때 다음과 같은 인증 요청 메시지를 함께 전송한다.

$$A \rightarrow broadcast: guest, ID, \{GC, K_A, t_A\}_{GAK_A}, HMAC, \quad (6)$$

여기서  $guest$ 는 인증을 요청하는 노드가 게스트 노드임을 의미한다.

단계 2: 메시지를 받은 이웃 노드 B는 라우팅 요청 메시지를 받으면 메시지에 실려 있는 노드 A의 MAC 주소를 얻어내고, 인증 메시지의 종류가 호스트인지 게스트인지를 확인한다. 게스트 인증이라면  $GAK_A$ 를 생성한다. 생성된  $GAK_A$ 를 이용하여 메시지를 복호화하여  $GC$  정보를 얻어내고 B가 계산한  $GC$ 와 동일한지를 비교한다. 중간 노드 B는 소스 노드 A가 적합한 사용자라고 판단을 하면 노드 A가 전송한  $ID$ ,  $K_A$  및 노드 A의 MAC 주소 정보를 유지하여 라우팅 응답 메시지를 보낼 때 사용하도록 한다.

단계 3: 중간 노드 B는 동일한 방법으로 인증 요청 메시지를 생성하여 브로드캐스트한다.

단계 4: 메시지를 받은 목적 노드 C는 메시지를 복호화하고 B가 보내온 메시지를 인증한다. 목적 노드 C는 라우팅 알고리즘에 따라 효율적인 경로를 선택하고 라우팅 응답 메시지를 전송한다. 여기서는 A-B-C 경로를 가정한 것이다.

단계 5: 노드 C는 노드 B에게 라우팅 응답 메시지를 전송할 때 다음과 같은 인증 응답 메시지를 함께 전송한다.

$$C \rightarrow B: guest, ID, \{GC_C^{**}, t_C\}_{K_B}, HMAC, \quad (7)$$

여기서  $GC_C^{**}$ 는  $hash(K_C, MADDR_C)$ 이고,  $ID$ 는 전송 받은 인증 요청 메시지의  $ID$ 이다.

단계 6: 인증 응답 메시지를 받은 노드 B는  $K_B$ 를 이용하여 메시지를 복호화하고  $GC_C^{**}$  정보가 올바른지 확인한다. 그리고 노드 A에게 동일한 방법으로 인증 응답 메시지를 전송한다.

단계 7: 소스 노드 A는 마찬가지로  $GC_B^{**}$  정보를 확인하여 라우팅과정을 마치고 이후에 전송되는 데이터는  $K_A$ 를 이용하여 암호화한다.

#### IV. 성능 평가

##### 1. GNY 분석

제안한 인증 프로토콜의 신뢰성을 분석하기 위하여 GNY logic을 이용한다. GNY logic은 암호화 프로토콜의 수행을 이해하기 위한 체계적인 방법으로 GNY logic에 대한 상세한 검증 방법은 [9]에 기술되어 있다.

본 논문에서 제안하는 인증 프로토콜은 기본적으로 인증을 요청하는 노드와 인증 요청에 대한 응답을 보내는 노드 간의 메시지 교환이다. 따라서 두 노드 간의 인증 프로토콜의 검증 결과만 보이기로 하겠다.

GNY logic을 통한 검증을 위해서는 먼저 프로토콜을 이상화된 프로토콜로 표현하여야 하며 제안하는 프로토콜을 표현하면 다음과 같다. 이때 노드 A에서 랜덤하게 생성한 키를  $K_A$ 로 표기하지 않고  $K$ 로 표현하도록 한다.

이상화된 프로토콜 (Idealized protocol)

$$\begin{aligned} B \triangleleft * host, * ID, \\ * \{ * HC_A, * K, * t_A \}_{HAK_A}, * HMAC \\ \hookrightarrow A \mid \equiv A \xleftrightarrow{K} B \end{aligned}$$

$$\begin{aligned} A \triangleleft host, ID, * \{ * HC_B^{**}, * t_B, * L_G, \\ * K_G, * T_G \}_K, * HMAC \\ \hookrightarrow B \mid \equiv B \xleftrightarrow{K} A \end{aligned}$$

GNY 로직을 통하여 검증 하고자는 인증의 목적은 다음 네 가지이다. 즉, 상대방과 자신이 각각 안전한 세션키를 공유하고 있음을 믿고 상대방이 그런 믿음을 가지고 있음을 믿는 것까지를 인증의 목적으로 한다.

분석 목적 (Goal)

$$\begin{aligned} A \mid \equiv A \xleftrightarrow{K} B \quad B \mid \equiv B \xleftrightarrow{K} A \\ A \mid \equiv B \mid \equiv B \xleftrightarrow{K} A \quad B \mid \equiv A \mid \equiv A \xleftrightarrow{K} B \end{aligned}$$

가정 사항 (Assumptions)

$$\begin{aligned} A \ni ID \quad A \ni K \quad A \ni t_A \quad A \ni HC_A \\ A \ni K_H \quad A \ni MADDR_A \quad A \ni HAK_A \\ B \ni K_H \quad B \ni MADDR_B \quad B \ni HC_B^{**} \\ B \ni t_B \quad B \ni L_G \quad B \ni K_G \quad B \ni T_G \end{aligned}$$

$$A \mid \equiv B \mid \rightarrow B \mid \equiv * \quad B \mid \equiv A \mid \rightarrow A \mid \equiv *$$

$$A \mid \equiv \#(t_A) \quad B \mid \equiv \#(t_B)$$

$$A \mid \equiv \#(ID) \quad A \mid \equiv \#(K)$$

$$B \mid \equiv \#(HC_B^{**}) \quad A \mid \equiv \phi(K)$$

$$A \mid \equiv \phi(ID) \quad B \mid \equiv \phi(HC_A)$$

$$A \mid \equiv A \xleftrightarrow{K} B \quad B \mid \equiv A \mid \rightarrow A \xleftrightarrow{K} B$$

$$A \mid \equiv A \xleftrightarrow{HAK_A} B \quad B \mid \equiv A \xleftrightarrow{HAK_A} B$$

로직 분석 (logical Analysis)

메시지 1: 노드 B는 소스 노드 A로부터 메시지를 수신하면 MAC 헤더를 통하여 노드 A의 MAC 주소를 알 수 있다. 따라서  $B \ni MADDR_A$ 이며 가정  $B \ni K_H$ 와 P2 규칙을 적용하면,  $B \ni HAK_A$ 가 나오며 노드 B는  $B \mid \equiv A \xleftrightarrow{HAK_A} B$ 이라 믿는다. 규칙 T1을 적용하면 다음과 같다.

$$B \triangleleft host, ID, \{ HC_A, K, t_A \}_{HAK_A}, HMAC. \quad (8)$$

식 (8)에 다시 T3과 P1을 적용하면 식 (9)와 같다.

$$B \triangleleft host, ID, HC_A, K, t_A, HMAC. \quad (9)$$

식 (9)에 규칙 R1과 가정  $B \mid \equiv \phi(HC_A)$ 를 적용하면 노드 B는 메시지를 인식할 수 있다.

$$B \mid \equiv \phi(host, ID, HC_A, K, t_A, HMAC). \quad (10)$$

노드 B는  $HC_A$ 가 자신이 가지고 있는  $HC_n$ 중에 존재하는지 확인을 한다. 또한, 노드 B는 P4에 의하여  $HMAC$ 을 확인하여 메시지의 무결성을 체크할 수 있다. 메시지의 암호화된 부분에 가정  $A \mid \equiv \#(t_A)$ 와  $A \mid \equiv \#(K)$ 에 F1을 적용하고, I1을 적용하면 식 (11)을 얻을 수 있다.

$$B \mid \equiv A \mid \sim (HC_A, K, t_A). \quad (11)$$

식 (11)은 메시지가 노드 A로부터 전송된 사실을 확증하여 노드 A를 인증하였음을 의미한다. 식 (11)에 J2를 적용하면 다음과 같은 목표를 이끌어 낼 수 있다.

$$B \mid \equiv A \mid \equiv A \xleftrightarrow{K} B. \quad (12)$$

식 (12)에 다시 J1을 적용하면 다음 식 (13)을 이끌어낼 수 있다. (13)식은 노드 B는 노드A와 노드B가 서로 같은  $K$ 를 소유하고 있음을 믿는다는 것을 의미한다.

$$B| \equiv A \xleftrightarrow{K} B \quad (=B| \equiv B \xleftrightarrow{K} A. \quad (13)$$

메시지 2: 식 (13)에 의하여 P3을 적용하면  $B \ni K$ 가 되며 다시 T1, T3, P1을 적용하면 다음과 같은 결과를 얻는다.

$$A \ni \text{host}, ID, HC_B^{**}, t_B, L_G, K_G, T_G, HMAC. \quad (14)$$

노드 A는 노드 B로부터 메시지를 수신하면 노드 B의 MAC 주소를 알 수 있다. 따라서  $A \ni MADDR_B$ 이고,  $HC_B^{**}$ 를 계산할 수 있다. P3에 의하여  $A \ni HC_B^{**}$ 이므로 노드 A는 자신이 계산한  $HC_B^{**}$ 과 전송 받은  $HC_B^{**}$ 가 일치하는지 계산하여 메시지를 인증할 수 있다. 따라서 제안하는 인증 프로토콜은 상호 인증을 검증할 수 있다. 노드 A와 노드 B가 서로 상호 인증을 했다는 것을 수식적으로 나타내면 다음과 같다.

우선, R1과 가정  $A| \equiv \phi(ID)$ 식 (14)에 적용하면 다음과 같다.

$$A| \equiv \phi(\text{host}, ID, HC_B^{**}, t_B, L_G, K_G, T_G, HMAC). \quad (15)$$

또한,  $A \ni HC_B^{**}$ 이므로  $A| \equiv \phi(HC_B^{**})$ 가 되고, R1을 적용하면 식 (16)과 같다.

$$A| \equiv \phi(HC_B^{**}, t_B, L_G, K_G, T_G). \quad (16)$$

식 (16)에 I1을 적용하면 식 (17)과 같음을 확인할 수 있다.

$$A| \equiv B| \sim (HC_B^{**}, t_B, L_G, K_G, T_G). \quad (17)$$

식 (17)에 다시 J2를 이용하여 최종적으로 식 (18)을 유도할 수 있다. 식 (18)은 노드 A와 노드 B가 둘 다 서로 같은  $K$ 를 공유하고 있음을 믿는다는 것을 의미하고, 이는 노드 A와 노드 B가 서로 상호 인증 됐음을 나타낸다.

$$A| \equiv B| \equiv B \xleftrightarrow{K} A. \quad (18)$$

메시지 1에서와 마찬가지로 노드 A는 P4에 의하여 메시지의 무결성을 확인할 수 있다. 게스트의 인증 기법 역시 호스트 인증 기법과 동일한 결과를 얻을 수 있다. 식 (12), (13), (18)과 가정  $A| \equiv A \xleftrightarrow{K} B$ 가 GNY 분석을 통하여 얻으려는 최종 결과이다. 이러한 결과를 종합하면 먼저 노

드 A가  $K$ 를 생성하였으므로 가정에 의하여 노드 A가  $K$ 를 소유하고 신뢰하는 것은 분명하다. 또한 노드 B 역시  $K$ 를 소유하고 신뢰하게 됨을 검증 결과로 알 수 있으며, 노드 A에서 요청한 인증 메시지를 확인하고 인증할 수 있다. 노드 A도 노드 B와 같이 노드 B에서 전송한 인증 응답 메시지를 인증할 수 있으며 노드 A와 노드 B 서로가 상대방이 키  $K$ 를 신뢰하고 있음을 알 수 있다. 이 결과로 인증과 키 분배가 잘 이루어졌음을 알 수 있다.

## 2. Security 분석

본 절에서는 다양한 공격 유형들을 고려하고, 제안한 무선 메쉬 네트워크 인증 프로토콜이 이러한 공격들을 어떻게 방어할 수 있는지에 서술하여 제안한 프로토콜의 안전성을 평가한다.

도청 (Eavesdropping): 도청은 무선으로 전송되는 데이터의 내용을 공격자가 가로채어 살펴보는 것을 의미한다. 그러나 제안하는 프로토콜에서 인증 메시지는 암호화되어서 전송되기 때문에 공격자가 메시지를 도청할 수 없다.

Replay 공격 (Replay Attack): replay 공격은 노드 간에 이미 전송된 메시지를 가로채어 수집하여 두었다가 공격자가 이를 그대로 사용하는 공격 유형이다. 제안한 프로토콜에서는 인증 메시지에 메시지를 전송하는 노드의 MAC 주소 정보가 포함되어 있다. 따라서 메시지 내의 MAC 주소와 메시지를 전송하는 노드의 MAC 주소가 동일하지 않으면 수신 노드는 인증 메시지가 공격 메시지라는 것을 알 수 있다. 또한 타임스탬프 값을 이용하여 제한된 시간 내에서만 인증 메시지가 유효하도록 하여 replay 공격을 방지한다.

패스워드 추측 공격 (Brute Force): 패스워드 추측 공격은 공격자가 추측한 패스워드를 이용하여 메시지를 복호화하는 방법이다. 그러나 제안한 프로토콜에서 암호화되는 부분 중에 고정된 값은 존재하지 않는다. 예를 들어, 호스트 인증 요청 메시지를 보면  $HC_n$ 의 개수는 한정되어 있기는 하지만 노드가 메시지를 전송할 때마다 계속 변화된다. 또한  $K$  값은 랜덤한 값이며, 정확한 타임스탬프 값을 공격자가 알아내기 어렵다. 게스트 키도 주기적으로 변경되는 값이며 노드마다 암호화하는 키가 다르기 때문에 여러 개의 노드들이 보낸 메시지를 동시에 복호화하여 같은  $HC_n$  또는  $GC$  값을 찾아내기 어렵다.

메시지 변조 (Message Modification): 공격자가 임의로 메시지의 일부분을 수정하는 공격 유형을 생각해볼 수 있다. 그러나 제안하는 프로토콜에서는 *HMAC*을 사용하기 때문에 메시지의 일부분에 수정이 가해지는 것을 알아낼 수 있다. 만일 공격자가 메시지의 일부만 수정하면 *HMAC* 값이 전혀 달라지기 때문이다.

### 3. 전송 지연 시간 성능 분석

제안한 메시 인증 알고리즘의 성능 분석을 위하여 본 절에서는 데이터 전송 지연 시간을 분석한다. 실험 환경인 홈 네트워크는 소규모 네트워크이므로 1 홉과 2 홉에 대해서만 전송 지연 시간을 측정하였다. 인증 프로토콜을 리눅스 기반의 랩톱에서 구현을 하여 실제 데이터를 전송하고 이때, 전송 시간을 측정 하였다. 기본 개발 환경은 표 1과 같다.<sup>[10]</sup> 구현 사용된 키 값은 16byte이며 인증을 위한 상수  $HC_n$ 은 2byte씩 총 5개를 사용하였고, AES(Advanced Encryption Standard) 암호화 알고리즘 방식과 MD5 해시 알고리즘을 사용하였다.

제안하는 인증 프로토콜이 데이터 전송 지연에 미치는 영향을 측정하기 위하여 제안하는 인증 프로토콜을 구현했을 때와 구현하지 않은 메시 네트워크에서의 데이터 전송 지연 시간 차이를 비교하였다. 인증 시간은 데이터 크기에 영향을 받지 않으며 고정되어 있기 때문에 ping을 통하여 전송 시간을 측정 하였으며 1 홉과 2 홉에서 각각 총 100회를 측정하였다. 1 홉 실험에서는 노드 A와 노드 C를 15m 간격으로 배치하여 실험을 하였으며, 2 홉에서의 성능을 측정하기 위하여 노드 A와 노드 B, 노드 C를 각각 15m 간격으로 배치하여 노드 A에서 ping을 통하여 전송 시간을 측정 하였으며 1 홉과 2 홉에서 각각 총 100회를 측정하였다. 1 홉 실험에서는 노드 A와 노드 C를 15m 간격으로 배치하여 실험을 하였으며, 2 홉에서의 성능을 측정하기 위하여 노드 A와 노드 B, 노드 C를 각각 15m 간격으로 배치하여 노드 A에서 노드 C로 ping 메시지를 전송하였다. 실험 결과는 그림 2 및 그림 3과 같으며 그림에서 보듯이 제안하는 인증 프로토콜이 데이터 전송 지연에 큰 영향을 미치지 않음을 알 수 있다. 1 홉에서 인증 프로토콜을 사용하지 않을 때의 평균 ping 전송 시간은 4.94ms이며 인증 프로토콜을 사용할 경우는 평균 5.04ms로 100 $\mu$ s의 차이를 보였다. 이러한 결과는 무선의 상태에 따라 전송 시간 범위 차이가 큰 것을 감안하면 인증 프로토콜을 사용한다고 하더라도 실제 데이터 전송 시간에 미미

표 1. 기본 개발 환경

Table 1. The basic environment.

항목	개발 환경	버전	비고
운영체제	Linux Fedora Core 5	커널 2.6.15	
무선 기기	Intel Pentium 4, 280 GHz CPU, 1 GB RAM		노드 A
	Ralink Tech RT2571w 모델 무선 랜 카드 802.11b/g 지원	1.0.3.6	
	Intel Celeron M, 1.5 GHz CPU, 256 MB RAM		노드 B
	Ralink Tech RT2571w 모델 무선 랜 카드 802.11b/g 지원	1.0.3.6	
	Intel Petium M 745, 1.8 GHz CPU, 1 GB RAM		노드 C
	Intel ipw2200 모델 무선 랜 카드 802.11b/g 지원	1.1.3	

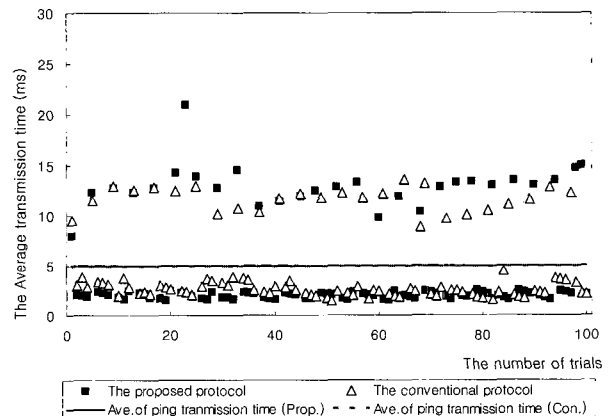


그림 2. 1 홉에서의 ping 전송 지연 시간 비교

Fig. 2. Comparison of the transmission time of ping message between the conventional routing protocol and the proposed protocol for one-hop.

한 영향만이 있다는 것을 알 수 있다. 2 홉에서는 인증 프로토콜을 사용하지 않을 경우의 평균 전송 지연 시간은 10.57ms 이며 인증 프로토콜을 사용할 경우는 11.28ms로 710 $\mu$ s의 차이를 보였다. 제안하는 인증 프로토콜을 사용함으로써 지연되는 이론적인 시간을 구해보면 약 2.7 $\mu$ s의 시간이 소요된다. 이러한 경우는 리눅스 커널 2.4.21 운영 체제에서 AMD 1.6GHz의 프로세서를 사용할 경우 1홉에서 지연되는 시간이다.

제안하는 인증 알고리즘은 빠른 인증을 수행하기 위하여 인증서 방식이나 공개키 방식이 아닌 패스워드 방

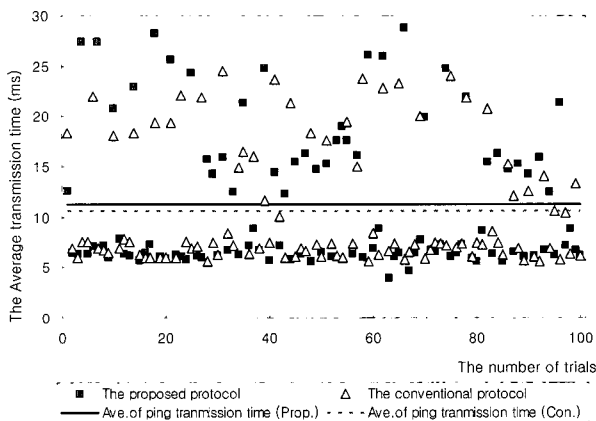


그림 3. 2 홉에서의 ping 전송 지연 시간 비교

Fig. 3. Comparison of the transmission time of ping message between the conventional routing protocol and the proposed protocol for two-hop.

식을 사용하였다. 따라서 결과에서 보는 바와 같이 제안하는 인증 프로토콜이 데이터 전송 지연에 큰 영향을 미치지 않으면서도 네트워크 보안을 강화하며 공격자로부터 안전한 데이터 전송을 보장할 수 있다. 또한, 상호 인증과 메시지 암호화에 서로 다른 키를 사용하여 보안을 향상시켰다. 또한, 라우팅 과정에서의 인증으로 홉 수가 늘어날수록 전달되는 메시지의 양이 증가하지 않는다.

## V. 결 론

본 논문에서는 무선 메쉬 네트워크를 적용한 홈 네트워크에서 사용자의 편의성과 멀티 홉 통신에서의 빠른 인증을 위해 패스워드 기반의 인증 프로토콜을 제안하였다. 제안한 인증 프로토콜은 reactive 라우팅 프로토콜에 기반하여 사용될 수 있으며 특정 라우팅 프로토콜을 구분하지 않는 장점이 있다. 그리고 홈 네트워크에서의 적용을 고려하여 호스트 인증과 게스트 인증을 구별하였기 때문에 보다 안전한 인증을 수행할 수 있다.

인증 프로토콜의 성능의 분석을 위해 GNY logic을 이용한 프로토콜 검증과 Security 분석, 그리고 전송 지연 시간 성능 분석을 하였다. GNY logic을 이용한 일반적인 증명을 통하여 프로토콜의 신뢰성을 증명하였고, 다양한 공격 유형에 대하여 제안한 인증 프로토콜이 어떠한 강점을 갖는지 분석하였다. 또한 실제 전송 지연 시간을 측정하여 인증 프로토콜이 네트워크의 성능저하에 큰 영향을 미치지 않음을 증명했다. 따라서 본 연구에서 제안한 인증 프로토콜은 무선 메쉬 네트워크에서

안전하고 효율적인 인증 프로토콜로 사용될 수 있을 것으로 기대한다.

## 참 고 문 헌

- [1] <http://www.itu.int/ITU-T/studygroups/com17/index.asp>
- [2] A. A. Pirzada and C. McDonald, "Kerberos Assisted Authentication in Mobile Ad-hoc Networks", in Proc. the 27th Australasian Computer Science Conference (ACSC'04), pp. 41-46, Dunedin, New Zealand, Jan. 18-22, 2004.
- [3] H. Deng, A. Mukherjee, and D. P. Agrawal, "Threshold and Identity-based Key Management and Authentication for Wireless Ad Hoc Networks", in Proc. the Information Technology: Coding and Computing (ITCC'04), vol. 1, pp. 107-111, Las Vegas, U.S.A., Apr. 5-7, 2004.
- [4] M. Bechler, H.-J. Hof, D. Kraft, F. Phlke, and L. Wolf, "A Cluster-Based Security Architecture for Ad Hoc Networks", in Proc. INFOCOM 2004, vol. 4, pp. 2393-2403, Hong Kong, Mar. 12-13, 2004.
- [5] K. Sanzgiri, D. Laflamme, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, "Authenticated Routing for Ad Hoc Networks", IEEE Journal on Selected Areas in Communications, Vol. 23, no. 3, Mar. 2005, pp. 598-610.
- [6] M. M. Islam, R. Pose, and C. Kopp, "Suburban Ad-hoc Networks in Information Warfare", in Proc. 6th Australian InfoWar Conference, Geelong, Australia, Nov. 24-25, 2005.
- [7] P. Papadimitratos and Z. J. Haas, "Secure Routing for Mobile Ad hoc Networks", in Proc. the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), pp. 193-204, San Antonio, TX, Jan. 27-31, 2002.
- [8] S. Carter and A. Yasinsac, "Secure Position Aided Ad hoc Routing Protocol", in Proc. the International Conference on Communications and Computer Networks (CCN) pp. 329-334, Mass, U.S.A., Nov. 4-7, 2002.
- [9] L. Gong, R. Needham, and R. Yahalom, "Reasoning about Belief in Cryptographic Protocols", in Proc. IEEE Symposium on Research in Security and Privacy, pp. 234-248, Oakland, CA, May 1990.
- [10] , , "홈 네트워크 내에서의 멀티 홉 통신을 지원하는 인증 프로토콜," JCCI 2007, 평창, 2007년 5월



---

 저 자 소 개
 

---



이 규 환(학생회원)  
 2007년 2월 아주대학교  
 전자공학부 졸업.  
 2007년 3월~현재 아주대학교  
 대학원 전자공학과  
 <주관심분야: WPAN에서의 보  
 안.인증, Ad-hoc, Mesh network>



이 주 아(학생회원)  
 2005년 2월 아주대학교  
 전자공학부 졸업.  
 2007년 2월 아주대학교  
 전자공학과 공학석사.  
 2007년 3월 삼성전자 무선사업부

<주관심분야 : 무선 LAN 보안, 센서 네트워크,  
 Ad-hoc 인증 >



김 재 현(정회원)  
 1991년 2월 한양대학교  
 전자계산학과 졸업  
 1993년 2월 한양대학교  
 전자계산학과 공학석사  
 1996년 8월 한양대학교  
 전자계산학과 공학박사

1997년 7월~1998년 6월 UCLA 전기과  
 Postdoc 연구원

1997년 7월~1998년 9월 IRI Corp. CA, USA

1998년 11월~2003년 2월 Bell Labs, Lucent  
 Tech. NJ, USA

2003년 3월~현재 아주대학교 정보통신대학  
 전자공학부 부교수

<주관심분야 : 무선 인터넷 QoS, MAC 프로토콜,  
 IEEE 802.11/15/16/20>