논문 2009-46TC-2-11

# 유비쿼터스 네트워크 환경에서 커뮤니티 멤버간 인증 및 세션키 교환 기법

## ( Session Key Exchange and Authentication Scheme between Communication Members in Ubiquitous Networks )

노 효 선*, 정 수 환**

( Hyosun Roh and Souhwan Jung )

요 약

본 논문은 유비쿼터스 네트워크 환경에서 커뮤니티 멤버 ID를 이용하는 비대화형 키 분배 알고리즘을 적용한 세션키 교환 및 인증 기법을 제안한다. 유비쿼터스 네트워트 환경에서는 언제, 어디서나 사용자들이 필요로 하는 서비스를 제공해주기 위해 다양한 상황인식 정보들이 수집되고 활용된다. 그러나 유비쿼터스 네트워크 환경의 경우 공격자에 의해 상황인식 정보가 위조 및 도용되어 악의적인 목적으로 사용될 수 있다. 제안하는 기법은 커뮤니티 사용자 ID 정보를 이용한 커뮤니티 멤버들 간의 상호 인증 및 세션키 교환 기법을 제안하여 안전한 정보 전달을 수행할 수 있도록 하였다. 또한 AAA 인증 서버 기반 기법과의 비교 분석을 통해 상호 인증 및 세션키 교환 과정에서 발생하는 통신 오버헤드와 인증 지연시간이 감소함을 확인하였다.

Abstract

This paper proposed a session key exchange and authentication scheme on non-interactive key distribution algorithm using a community member's ID in ubiquitous networks. In ubiquitous network environment, User's context-awareness information is collected and used to provide a context-awareness service for someone who need it. However, in ubiquitous network environment, this kind of the Context-awareness information could be abused by a malicious nodes. The proposed scheme using the community member ID provides a session key exchange and mutual authentication between community members, and supports secure data communication. Also, when exchanging the session key and authenticating each other, this scheme reduces communication overhead and authentication delay compared to the AAA server scheme.

**Keywords :** 커뮤니티 네트워크, 유비쿼터스, ID 기반, 세션키 교환, 인증, Ad-hoc

## Ⅰ. 서 론

최근 무선네트워크 기술은 급속도로 발전하고 있으며, 더불어 네트워크 사업자들은 사용자들에게 최적의 인터넷 서비스를 제공해 주기 위한 다양한 네트워크 기술들을 개발하고 있다. 그중 최근 활발하게 연구 진행되고 있는 유비쿼터스 네트워크는 사용자들이 필요로 하는 다양한 서비스를 네트워크를 통해 언제, 어디서든 제공해 줄 수 있는 가능성을 열어주었다. 이러한 유비쿼터스 네트워크 환경에는 사용자들이 필요로 하는 서비스를 최적의 네트워크 상태로 제공하기 위한 다양한 무선 네트워크 기술이 존재한다. 또한 사용자의 상황에 가장 적합한 네트워크 서비스를 제공하기 위해 다양한 상황인식 정보가 수집되고, 유비쿼터스 네트워크에 존재하는 다양한 네트워크 장비에서 서비스 제공을 위해 사용된다. 특히 이질적인 무선 네트워크 환경이 공존하는 유비쿼터스 네트워크 환경의 경우 각각의 무선 네트워크마다 통신을 위해 사용되는 라우팅 프로토콜이 다

* 정회원, ** 평생회원-교신저자,
숭실대학교 정보통신전자공학부
(School of electronic Engineering, Soongsil University)

※ 이 논문은 숭실대학교 교내 연구비 지원에 의해 수행되었음

접수일자: 2008년12월13일, 수정완료일: 2009년2월17일

를 수 있으며, 무선 애드 혹 네트워크[1~2]의 경우 단말 간에 최적의 통신을 제공하기 위해 pro-active, re-active 등의 라우팅 프로토콜들이 사용자의 환경에 따라 각기 다르게 사용될 수 있다. 때문에 사용자 단말의 경우 다양한 무선 네트워크 환경으로 이동할 경우 네트워크 상황에 따라 통신할 수 있도록 네트워크 설정을 바꾸어주어야 한다. 또한 다양한 무선 네트워크 환경에서 사용하는 라우팅 프로토콜이 사전에 이동 단말에 설치되어 있지 않을 경우 지속적인 통신을 할 수 없는 상황을 만날 수 있다. 때문에 유비쿼터스 네트워크 환경에서는 사용자의 상황인식 정보를 활용하여 사용자에게 최적의 서비스를 제공할 수 있도록 지원하는 기술이 관심을 받고 있다. 이와 같이 기술로서 최근 연구되고 있는 커뮤니티 네트워크[3]가 있다.

커뮤니티 네트워크는 유비쿼터스 네트워크 환경에서 사용자의 상황인식 정보를 활용하여 사용자에게 최적의 네트워크 서비스를 제공해주기 위해 연구되고 있는 기술로써 존 마스터를 중심으로 구성되는 존 기반의 커뮤니티 네트워크이다. 커뮤니티 네트워크에서는 스마트 패킷 프로토콜[4]을 통해 사용자 이동 단말의 상황인식 정보 및 다양한 네트워크 장비들의 상태 정보들이 상호 인터페이스를 통해 제공된다. 제공되는 상황인식 정보는 사용자가 필요로 하는 서비스를 제공하기 위해 사용된다. 사용자가 특정 커뮤니티로 이동하였을 경우 그 커뮤니티에서 제공되는 서비스를 사용할 수 있도록 서비스 실행 모듈을 자동 전송 및 실행하거나 사전에 사용자 단말에 설치되어 있지 않은 라우팅 프로토콜이 사용되는 커뮤니티 환경의 경우 필요한 라우팅 실행 모듈을 자동 전송 및 실행을 지원한다. 또한 각 사용자가 요구하는 QoS를 만족하는 네트워크 서비스를 제공하기 위해서도 상황인식 정보들이 상호 인터페이스를 통해 제공된다. 그러나 이러한 커뮤니티 네트워크 기반의 유비쿼터스 네트워크 환경에서 아직까지 분명한 보안 구조 및 인증 기술이 구성되지 않았다. 특히 다양한 서비스 커뮤니티가 존재하고 커뮤니티 멤버 간 협업 및 통신을 가능하게 하는 커뮤니티 네트워크의 경우 커뮤니티 멤버 인증 및 안전한 통신을 위한 세션키 교환은 매우 중요한 이슈이다. 커뮤니티 네트워크 환경에서 제공되는 다양한 상황인식 정보는 악의적인 공격자에 의해 위조, 변경되어 악의적인 공격을 위해 사용될 수 있으며, 공격자들이 전송하는 악의적인 목적의 실행 모듈들은 커뮤니티 네트워크에 존재하는 정상적인 사용자들의 네트워크 사용을 제한하거나, 전체 네트워크를 혼란스럽게 만들 수 있다[5]. 따라서 이러한 공격으로부터 커뮤니티 네트워크에서 주고받는 상황인식 정보를 안전하게 보호하고 커뮤니티 멤버를 인증할 수 있는 보안 기술이 필요하다. 본 논문에서는 위와 같은 문제를 해결하기 위해 커뮤니티 네트워크 기반의 유비쿼터스 네트워크 환경에서의 커뮤니티 멤버인증 및 커뮤니티 멤버의 ID를 이용한 세션키 교환 기법을 제안하였다. 제안하는 기법은 커뮤니티 멤버의 ID로 사용할 수 있는 IP 주소, 이 메일 주소, 전화 번호 등을 이용하여 각 커뮤니티 멤버들을 위한 개인 비밀키를 생성하고, 생성된 개인 비밀키를 사용하여 커뮤니티 내에 존재하는 이웃 노드의 인증 및 개인 비밀키를 가진 커뮤니티 멤버들 간에 상대 노드의 ID를 이용하여 세션키를 교환할 수 있도록 제안하였다.

본 논문은 다음과 같이 구성되어 있다. Ⅱ장에서는 관련 기술들을 설명하고, Ⅲ장에서 본 논문에서 제안하고 있는 커뮤니티 네트워크 환경에서의 커뮤니티 멤버 인증 및 세션키 교환 기법에 대해서 설명한다. Ⅳ장에서는 제안하는 기법에 대한 비교 분석하고, 마지막 Ⅴ장에서 결론을 맺는다.

## Ⅱ. 관련 기술

다음은 본 논문에서 기본적으로 가정하고 있는 커뮤니티 네트워크 환경과 기존 ID를 이용한 키 생성 알고리즘에 대해서 설명한다.

### 1. 커뮤니티 네트워크

커뮤니티 네트워크란 이동 노드 및 다양한 유비쿼터스 노드들이 사용자, 서비스 혹은 응용의 요구사항을 만족시키기 위해 구성되는 네트워크로 정의할 수 있다. 하나의 커뮤니티 네트워크는 하나 또는 여러 개의 존들이 연결되어 구성할 수 있으며, 각 존은 존 마스터 노드를 중심으로 구성된다. 그림 1은 커뮤니티 네트워크 구조도를 보여준다. 하나의 존을 하나의 커뮤니티로 구성하고 있는 커뮤니티 네트워크로 존 마스터 노드를 기반으로 구성된다. 존 마스터 노드는 여러 개의 무선 인터페이스와 안정적인 전력, 높은 컴퓨팅 파워를 가지고 있으며 커뮤니티 멤버 노드들 간의 통신을 돕는 네트워크 장비이다. 기본적으로 커뮤니티 네트워크에 존재하는 모든 노드들은 애드 혹 라우팅 프로토콜을 통해 통

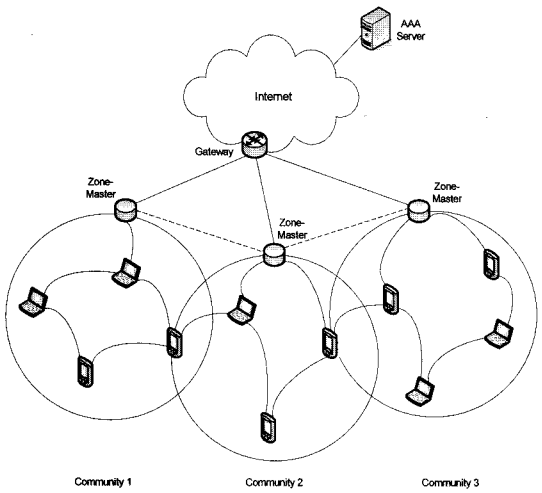


그림 1. 커뮤니티 네트워크 구조
Fig. 1. Community Network Architecture.

신을 수행한다. 존 내부에 존재하는 노드들 간의 통신은 re-active 라우팅 프로토콜을 사용하고 다른 커뮤니티 또는 다른 존에 존재하는 노드와는 pro-active 라우팅 프로토콜을 사용하여 통신한다. 또한 존 마스터 노드에는 현재의 커뮤니티에서 사용되고 있는 라우팅 프로토콜 실행 모듈, 서비스 실행 모듈 등이 보관되어 있으며, 이러한 실행 모듈은 커뮤니티 멤버들의 상황인식 정보를 기반으로 스마트 패킷 프로토콜을 통해 자동 전달 및 실행된다.

### 2. 비대화형 키 분배 방법

대표적인 비대화형 키 분배 기법은 1991년 Eurocrypt에서 Maurer와 Yacobi가 제안한 비대화형 키 분배 방법이다[6]. Maurer와 Yacob가 제안한 방법은 키 분배서버에 사전 등록된 사용자의 ID와 키 분배 서버만이 알고 있는 비밀 값을 이용한 이산대수를 통해 사용자 ID에 대응하는 비밀키를 생성하여 분배하는 방법이다. Maurer-Yacob의 비대화형 키 분배 방법의 핵심은 다음과 같다.

- 선택된 큰 합성수 m을 소인수분해하는 것은 계산상 불가능하다.
- 충분히 큰 소수 p에 대한 이산대수 계산은 가능하다.

위와 같은 내용을 기반으로 하는 Maurer-Yacobi 기법은 크게 초기 사용자 등록 과정과 키 분배 과정 등의 두 단계로 나눌 수 있다. 시스템이 시작되면 키 분배 서버는 네 개의 소수 $p_i$와 자신의 비밀 값 등을 선택한다. 이후 $ID_i$를 사용하는 사용자가 자신의 $ID_i$를 키 분배 서버에 등록을 원할 경우 오프라인 또는 온라인으로 안전하게 전달된 사용자 식별정보와 $ID_i$를 다음 식 1과 같은 방법으로 사용자를 등록하며 $ID_i$에 대응하는 비밀키 $S_i$를 생성한다.

$$S_i = \log_g(ID_i^2) \bmod \phi(m) \tag{1}$$

위와 같은 첫 단계가 끝나면 키 분배 서버는 사용자에게 안전한 방법을 통해 생성된 비밀키 Si를 분배한다. 이후 이렇게 비밀 키 Si를 분배 받은 사용자들은 키 분배 서버에 등록된 또 다른 사용자들과 키 분배 서버에 등록한 ID를 이용하여 안전하게 키를 분배한다. ID를 이용한 키 공유는 다음 식 2와 같은 방법으로 키를 생성하고 공유한다.

$$K_{ij} \equiv (ID_j)^{2S_i} \equiv (ID_i)^{2S_j} \equiv K_{ji} \tag{2}$$

## III. 제안기법

다음은 앞의 그림 1과 같은 커뮤니티 네트워크 기반 유비쿼터스 네트워크 환경에서 제안하는 커뮤니티 멤버 인증 및 세션키 교환 기법을 자세하게 설명한다. 다음의 표 1은 본 논문에서 제안하는 기법에서 사용되는 주요 용어들을 정리하였다.

표 1. 용어 정리
Table 1. Definition.

| 표 기 | 정 의 |
|---|---|
| $TEK$ | 커뮤니티 멤버 노드와 uT-게이트웨이 간에 공유하는 키 |
| $PSK_{Ci}$ | AAA 서버로부터 초기 인증을 끝낸 커뮤니티 멤버의 개인 비밀키 |
| $ID_{Ci}$ | 커뮤니티 멤버의 식별자 |
| $ID_{Zi}$ | 존 마스터의 식별자 |
| $d$ | uT-게이트웨이의 비밀 값 |
| $n$ | uT-게이트웨이의 공개 값 |
| $R_i$ | 임의의 수 |
| $E_{TK}$ | TEK로 암호화 |
| $E_{PK}$ | PSK로 암호화 |
| $h\{\ \}$ | 일방향 해쉬함수 |
| $Beacon$ | 비콘 메시지 |
| $t_p$ | 타임 스탬프 값 |

### 1. 세션키 분배 기법

#### 가. 설계 원리 및 제안 기법 개요

본 논문에서 제안하는 커뮤니티 네트워크 기반의 유비쿼터스 네트워크 환경에서의 커뮤니티 멤버 간 인증 및 세션키 교환 기법을 적용하기 위해서 다음과 같은 가정을 하였다. 첫째, 사용자의 이동 단말은 초기 인증을 위해 EAP-TLS[7]를 수행하고, 인증된 사용자의 경우 자신이 속한 커뮤니티를 관리하는 게이트웨이로부터 ID 기반의 비밀키를 분배받는다. 둘째, 사용자 ID 기반의 커뮤니티 멤버 간 세션키 공유를 위해 Maurer-Yacobi가 제안한 키 생성 방법에 기반한 키 생성 알고리즘을 사용한다. 마지막으로 게이트웨이와 존 마스터 간, 그리고 존 마스터들 간에는 TLS 또는 IPSec[8]이 적용된 안전한 채널을 가정한다. 다음 그림 2는 사용자의 이동 단말이 초기 인증 후 게이트웨이로부터 개인 비밀키인 PSK(Private Secret Key)를 분배받는 과정을 보여준다.

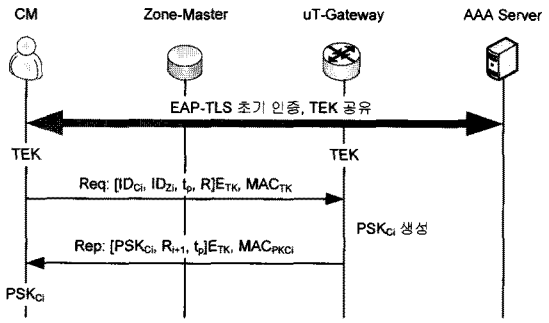


그림 2. 초기 인증 및 PSK 생성 과정
Fig. 2. Initial Authentication and Private Security Key Generation Procedure.

사용자 CM(Community Member node)의 이동 단말이 처음 부팅을 시작하면 EAP-TLS를 통해 AAA 서버로부터 초기 인증을 받은 후, 성공적인 초기 인증 과정에서 생성된 TEK(Traffic Encapsulation Key)를 uT-G(uT-Gateway)와 공유하게 된다. 성공적으로 초기 인증을 받은 후 $CM_i$는 uT-G에게 등록된 자신의 $ID_{Ci}$에 대응하는 비밀키 $PSK_{Ci}$를 요청한다. 다음 식 3은 $CM_i$가 uT-G에게 $PSK_{Ci}$를 요청하는 메시지를 보여준다.

$$Req = [ID_{Ci}, ID_{Zi}, t_p, R]E_{TK}, MAC_{TK} \quad (3)$$

위와 같은 $PSK_{Ci}$ 요청 메시지를 수신한 uT-G는 다음의 식 4와 같이 $PSK_{Ci}$를 생성한 다음 식 5와 같은 응답 메시지를 통해 생성한 $PSK_{Ci}$를 $CM_i$에게 전송한다.

$$PSK_{Ci} = d(\log_g(ID_{Ci})^2) \bmod \phi(n) \quad (4)$$

$$Rep = [PSK_{Ci}, R_{i+1}, t_p]E_{TK}, MAC_{PKCi} \quad (5)$$

위에서와 생성된 $PSK_{Ci}$는 uT-G와 공유하고 있는 TEK로 암호화하여 안전하게 $CM_i$에게 전달된다.

#### 나. 제안 기법

- 커뮤니티 멤버 간 인증 및 세션키 공유

다음 그림 3은 동일한 커뮤니티에 속한 커뮤니티 멤버 CM들 간에 상대방의 ID 정보를 이용하여 상호 인증 및 세션키를 교환하는 과정을 보여준다. 존 마스터로 구성된 커뮤니티에 속한 커뮤니티 멤버들은 주기적으로 비콘 메시지를 브로드 캐스트 한다. 이 비콘 메시지에는 자신이 속한 커뮤니티의 존 마스터 ID와 자신의 ID가 포함되어 있어 비콘 메시지를 수신하는 커뮤니티 멤버들은 이웃 커뮤니티 멤버들의 ID 정보를 알게 된다. 따라서 동일한 커뮤니티에 존재하는 커뮤니티 멤버 노드들은 비콘 메시지를 받은 후 이웃 노드들과 세션키 공유를 위한 메시지 교환 없이 세션키를 공유할 수 있게 된다. 다음 식 6에서처럼 비콘 메시지를 수신한 커뮤니티 멤버 노드 $CM_1$은 상대 노드 $CM_2$의 ID를 이용하여 세션키 $SK_{12}$를 생성한다.

$$SK_{12} = (ID_{C2}^2)^{Ri * PSK_{Ci}} \bmod N \quad (6)$$

이후 자신이 원하는 커뮤니티 멤버들과의 인증 과정을 통해 상호 인증을 수행한 후 안전한 통신을 수행한다.

커뮤니티 멤버간의 상호 인증은 앞의 그림에서처럼 인증을 요청하는 $CM_1$이 자신의 $ID_{C1}$, 통신하고자 하는

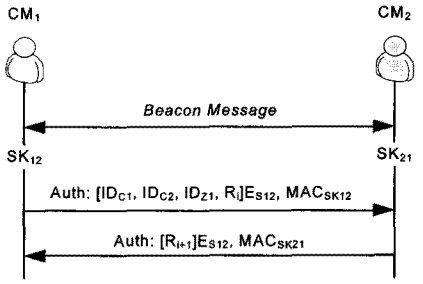


그림 3. 세션키 공유 및 멤버 인증 과정
Fig. 3. Session Key Exchange and Member Authentication Procedure.

커뮤니티 멤버의 $ID_{C2}$, 그리고 자신이 속한 커뮤니티의 존 마스터 $ID_{Z1}$과 임의의 수 $R_i$를 상호 공유하는 세션키 $SK_{12}$로 암호화한 메시지와 세션키를 이용하여 생성한 $MAC_{SK12}$를 보냄으로 인증과정을 수행한다. 함께 보내는 $MAC_{SK12}$는 다음의 수식 7과 같이 생성한다.

$$MAC_{SK12} = h[ID_{C1}, ID_{C2}, ID_{Z1}, R_i, SK_{12}] \quad (7)$$

커뮤니티 멤버 $CM_2$는 인증 요청 메시지를 수신한 다음 $MAC_{SK12}$를 검증한 후 인증 응답 메시지에 수신한 임의의 수를 1 증가한 후 세션키로 암호화하여 전달한다. 이때 함께 전달하는 $MAC_{SK21}$은 다음의 수식 8과 같이 생성한다.

$$MAC_{SK21} = h[MAC_{SK12}, R_{i+1}] \quad (8)$$

위와 같은 과정을 통해 상호 인증과정이 성공하며 서로의 ID 정보를 통해 생성한 세션키를 이용하여 안전한 데이터를 전송할 수 있다. 다음의 그림은 커뮤니티 멤버가 현재의 커뮤니티에서 다른 커뮤니티로 이동할 경우, 다른 커뮤니티에 존재하는 커뮤니티 멤버들과 세션키 교환 및 인증하는 과정을 보여준다.

• 커뮤니티 멤버 간 안전한 멀티 홉 보안 통신

다음 그림 4는 커뮤니티 기반 유비쿼터스 네트워크 환경에서 커뮤니티 멤버들 간의 멀티 홉 통신 과정을 보여준다.

그림에서처럼 커뮤니티에 참여한 커뮤니티 멤버 노드가 초기 인증 과정을 끝낸 후 uT-G로부터 개인 비밀키 PSK를 분배 받은 후 이웃 커뮤니티 멤버 노드들과 특별한 세션키 교환 과정 없이 안전한 데이터 통신을

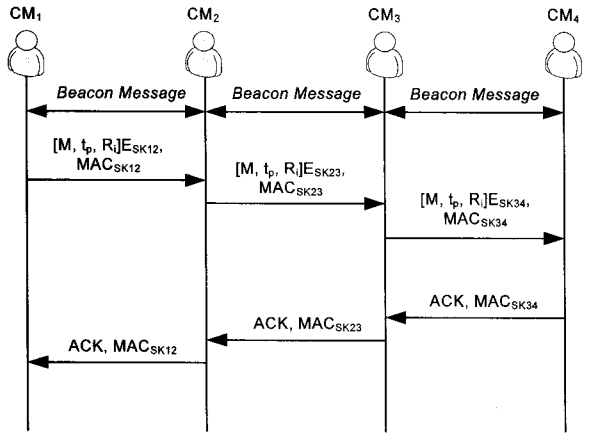


그림 4. 커뮤니티 멤버 간 보안 통신
Fig. 4. Secure Communication between the Community Members.

수행할 수 있다. $CM_1$이 $CM_4$와 통신을 원할 경우 $CM_1$은 $CM_2$와 공유하는 세션키 $SK_{12}$로 다음 식 9와 같이 전송할 데이터 메시지를 암호화하고 MAC 값을 포함하여 전송한다.

$$MAC_{SK12} = h[M, t_p, R_i, SK_{12}]$$
$$Message = [M, t_p, R_i]E_{SK12}, MAC_{SK12} \quad (9)$$

암호화된 메시지를 수신한 $CM_2$는 세션키 $SK_{12}$로 메시지를 복화화 할 수 있으며 MAC 값을 검증하여 정상적인 $CM_1$이 보낸 메시지임을 확인한다. 이후 다시 이전 $CM_1$이 생성하여 보낸 MAC 값을 포함하여 식 9에서와 동일한 방법으로 메시지를 암호화하고 MAC을 생성하여 다음 커뮤니티 멤버 노드에게 전달한다. $CM_2$가 전송하는 메시지에 포함되는 MAC 값과 암호화된 메시지는 식 10에서와 같다.

$$MAC_{SK23} = h[MAC_{SK12}, M, t_p, R_i, SK_{23}]$$
$$Message = [M, t_p, R_i, MAC_{SK12}]E_{SK23}, MAC_{SK23} \quad (10)$$

위와 같은 방법으로 $CM_1$에서 $CM_4$까지 암호화된 메시지가 전달된다. 최종적으로 $CM_4$가 메시지를 수신하면 자신의 세션키로 메시지를 복호화 할 수 있으며, MAC 값을 검증할 수 있다. 이후 $CM_4$는 정상적인 메시지 수신을 알리는 ACK 메시지를 $CM_1$에게 전송하고, 메시지의 무결성을 제공하기 위해 MAC 값을 추가하여 전송한다. 이렇게 함으로써 기존 방법에 비해 세션키를 교환하는데 필요한 메시지 수를 줄일 수 있다. 또한 메시지를 전달하기 처음 설정한 경로가 변경되어 재설정될 경우에도 추가적인 세션키 교환 과정 없이 암호화된 메시지를 새로운 경로에 포함된 커뮤니티 멤버들에게 전송할 수 있으므로 기존 기법에 비해 통신 오버헤드를 줄일 수 있다. 그리고 전달되는 메시지에는 바로 이전 커뮤니티 멤버 노드가 생성한 MAC 값을 포함하여 생성한 MAC 값이 포함되어 전달되기 때문에 중간에 있는 노드가 임의로 메시지를 변경할 수 없다. 때문에 전달되는 데이터에 대한 메시지 무결성이 보장된다.

## IV. 분석 및 비교

### 1. 제안 프로토콜의 안전성 분석

• MITM 공격

본 논문에서 제안하는 기법은 기본적으로 존 마스터와 uT-게이트웨이 간에 IPSec 또는 TLS와 같은 보안

프로토콜을 사용하여 안전한 채널이 형성되어 있음을 가정하였다. 따라서 uT-게이트웨이와 존 마스터 간의 주고받는 메시지와 존 마스터 간에 주고받는 메시지에 대한 MITM(Man In The Meddle) 공격에 안전하다. 또한 커뮤니티 멤버와 uT-게이트웨이, 커뮤니티 멤버와 존 마스터 간에는 성공적인 초기 인증 과정을 수행하고 나면 상호 간에 안전한 세션키인 TEK가 공유되고, 주고받는 메시지는 모두 TEK로 암호화하여 전달되므로 MIMT 공격에 안전하다. 커뮤니티 멤버와 존 마스터 또는 uT-게이트웨이 사이에서 공격자가 MIMT 공격을 성공하려면 이들 간에 공유하는 키를 알아야 하지만 이 키들은 초기 인증 과정을 통해 안전하게 분배되기 때문에 공개되지 않는다. 그리고 공격자가 커뮤니티 멤버들 간에 세션키를 공유하는 과정 또는 상호 인증하는 과정에서 MIMT 공격을 시도할 수 있다. 그러나 커뮤니티 멤버들 간에 공유하는 세션키는 메시지 교환 없이 비콘 메시지에 포함된 상호간의 ID를 통해 생성하기 때문에 MIMT 공격이 성립하지 않는다. 악의적인 공격자가 ID를 위조하거나 정상적인 커뮤니티 멤버의 ID를 도용할 경우에도 uT-게이트웨이로부터 분배받은 PSK를 모르기 때문에 정상적인 세션키를 생성 및 위조할 수 없으므로 MIMT 공격은 성립하지 않는다.

- 메시지 위조 및 위장 공격

제안하는 기법에서 악의적인 공격자가 정상적인 커뮤니티 멤버처럼 위장하여 uT-게이트웨이에게서 PSK를 분배받거나, 정상적인 커뮤니티 멤버들과 세션키를 공유하여 통신을 하려고 시도할 수 있다. 그러나 본 논문에서 제안하는 기법은 이러한 공격에 안전하다. 먼저 PSK는 커뮤니티 멤버 노드가 초기 인증을 통해 인증 서버로부터 인증을 받은 후, 인증된 커뮤니티 멤버에게만 uT-게이트웨이가 PSK를 분배한다. 이때 분배하는 PSK는 초기 인증 과정에서 인증 서버와 커뮤니티 멤버 노드간에 공유하는 MSK로부터 유도된 TEK로 암호화되어 전달된다. 따라서 공격자가 정상적인 PSK를 분배받기 위해서는 우선 TEK를 위조하거나 정상적인 TEK를 습득해야 한다. 그러나 공격자가 TEK를 습득하는 것은 불가능하기 때문에 PSK를 분배받기 위한 메시지를 위조할 수 없다. 또한 정상적인 커뮤니티 멤버 노드간에 공유하는 세션키의 경우 uT-게이트웨이가 PSK를 생성할 때 등록한 ID를 통해 공유한다. 때문에 악의적인 공격자가 정상적인 커뮤니티 노드의 ID를 도용하여 비콘 메시지를 브로드 캐스팅하여 세션키를 공유하려고 시도할 경우에도 PSK를 알지 못하므로 정상적인 세션키 공유가 불가능하다.

- 재전송 공격

제안하는 기법은 커뮤니티 멤버 노드가 uT-게이트웨이에게 PSK를 요청할 때 전송하는 요청메시지에 타임스템프와 임의의 수를 포함하여 전송하며, 매번 전송할 때마다 그 값을 변경하여 전송한다. 따라서 재전송 공격을 쉽게 차단할 수 있으며, 또한 이러한 값은 암호화되어 공개되지 않기 때문에 재전송 공격에 안전하다. 그리고 커뮤니티 멤버 노드들 간의 상호 인증을 위해 주고받는 메시지의 경우도 매번 임의의 수를 변경하고 암호화하여 전달하기 때문에 재전송 공격에 안전하다.

## 2. 기존 프로토콜과 비교 분석

다음 그림 5는 제안하는 기법과 AAA 인증 서버를 이용한 세션키 공유 기법[9]에 대해 통신 오버헤드와 커뮤니티 멤버 노드들 간의 세션키 공유 과정에서 발생하는 인증 지연시간을 비교분석하기 위한 실험 환경을 보여준다. 비교분석을 위해 본 논문에서 앞서 설명했던 존 마스터 기반의 커뮤니티 네트워크 환경을 구성하였고, 제안하는 기법과 AAA 인증 서버 기반 기법에서의 초기 인증 과정은 동일하게 EAP-TLS를 가정하였으며, 각 네트워크 구성 요소들 간의 지연시간은 다음과 같이 정의하였다.

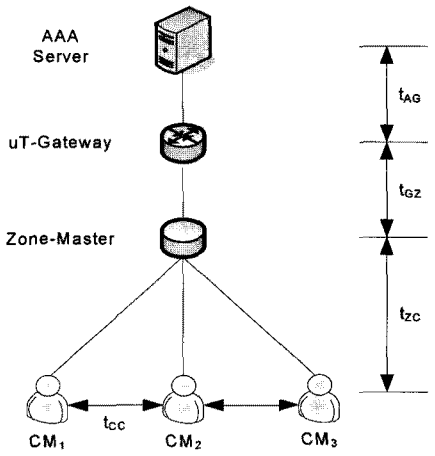


그림 5. 실험 환경
Fig. 5. Test Environment.

- $t_{AG}$: 인증 서버와 uT-G 간 지연시간
- $t_{GZ}$: uT-G와 존 마스터 간 지연시간
- $t_{ZC}$: 존 마스터와 커뮤니티 멤버 노드 간 지연시간

- $t_{CC}$: 커뮤니티 멤버 노드 간 지연시간

또한 본 논문에서는 데이터를 전달하는 과정에서 설정된 경로가 빈번하게 변경될 경우 지연시간을 비교 분석하였다. 이를 위해 애드혹 라우팅 프로토콜인 AODV[10]를 가정하였다.

• 커뮤니티 멤버 간의 상호 인증 및 세션키 공유

AAA 인증 서버 기반 환경에서 커뮤니티 멤버 노드는 EAP-TLS를 통한 초기 인증을 수행한다. 이후 CM1이 CM2와 안전한 통신을 위해 상호 인증 및 세션키 교환을 수행한다. 이때 모든 과정이 AAA 서버를 통해 이루어지므로 다음 식 11에서와 같은 인증 지연시간이 발생한다.

$$T_{td-A} = 2(t_{AG} + t_{GZ} + t_{ZC}) + 3t_{CC} \quad (11)$$

위의 수식에서 $T_{td-A}$는 커뮤니티 멤버 노드들 간의 상호 인증 과정에서 발생하는 전체 지연시간을 의미한다. AAA 인증 서버 기반 환경에서 커뮤니티 멤버 노드들 간에 세션키 교환을 위해서는 먼저 상호인증이 필요하다. 그러나 AAA 인증 서버 기반의 경우 커뮤니티 멤버 인증을 위한 상호인증이 AAA 인증 서버를 통해 수행되기 때문에 $CM_2$는 $CM_1$의 인증 요청 메시지의 검증 정보를 AAA 인증 서버에게 보내고, AAA 인증 서버가 $CM_1$의 인증 요청 메시지에 포함된 정보를 기반으로 $CM_1$을 인증한 후 인증 성공 메시지를 $CM_2$에게 보내어 $CM_1$을 인증하게 한다. 이후 상호 간에 세션키 교환을 하게 된다.

제안하는 기법의 경우 초기 인증 과정을 끝낸 커뮤니티 멤버 노드들 간의 상호 인증 및 세션키 교환 과정에서 발생하는 지연시간은 다음의 수식 12와 같다.

$$T_{td-A} = 2t_{CC} \quad (13)$$

제안하는 기법의 경우 세션키 공유를 위한 메시지 교환 없이 이웃 노드의 비콘 메시지를 통해 알고 있는 ID를 이용하여 세션키를 생성한다. 그리고 생성한 세션키로 자신의 ID와 상호 인증을 수행하고자 하는 커뮤니티 멤버의 ID, 그리고 자신이 속한 커뮤니티의 존 마스터 노드의 ID 정보를 생성한 세션키로 암호화하여 전달한다. 이때 이 메시지를 수신한 이웃 노드는 상대 노드의 ID를 이용하여 동일한 세션키를 생성함으로써 인증 메시지를 보낸 노드를 인증하고 세션키를 공유한다. 때문에 두 번의 메시지 교환만이 필요하다. 위에서 설명한 것처럼 제안하는 기법이 초기 인증 이후 커뮤니티 멤버 노드들 간의 상호 인증 및 세션키 교환시 지연시간이 감소하는 것을 확인할 수 있다.

• 존 마스터 간 이동

커뮤니티 네트워크 기반의 유비쿼터스 환경에서 사용자는 다양한 커뮤니티 환경을 자유롭게 이동하며 필요한 서비스를 받을 수 있어야 한다. 때문에 안전한 서비스를 제공받기 위해서 사용자에 대한 재인증 과정이 필요하다. AAA 인증 서버 환경의 경우 커뮤니티가 변경되면 사용자는 새로운 커뮤니티로 이동하기 전이나 이동 후에 AAA 인증 서버에게 인증을 요청하여 재인증을 받은 후 다른 커뮤니티 멤버와의 상호 인증을 수행 한다. 때문에 커뮤니티를 이동할 경우 다음과 같은 지연시간이 발생한다.

$$T_D = (j_{ZM} \times T_t) + T_t + 3t_{CC} \quad (14)$$

위의 식에서 $j_{ZM}$은 존 마스터의 개수로 커뮤니티가 바뀌면 1씩 증가한다. $T_D$는 재인증 과정에서 발생하는 전체 지연시간을 의미하고, $T_t$는 커뮤니티 멤버 노드가 AAA 인증 서버에게 인증을 요청하고 받는 과정에서 발생하는 지연시간으로 $T_{AG}$, $T_{GZ}$, $T_{ZC}$를 더한 값이다. 그러나 본 논문에서 제안하는 기법의 경우 커뮤니티를 이동할 경우에도 존 마스터의 ID를 알게 되면 두 번의 메시지 교환만으로 재인증을 받지 않고도 다른 커뮤니티 멤버들과 세션키를 교환할 수 있다. 다음은 이때 발생하는 지연시간은 다음과 같다.

$$T_D = (t_{ZC} \times j_{ZM}) + 2T_{CC} \quad (15)$$

다음 그림 6은 여러 커뮤니티를 이동하는 커뮤니티 멤버 노드의 재인증 과정과 이웃 노드와의 세션키 교환 과정에서 발생하는 지연시간을 비교하였다. 이를 위해

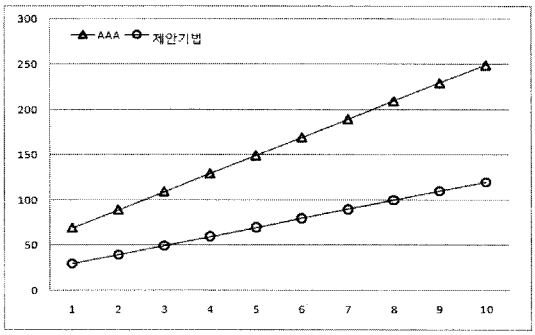


그림 6. 존 마스터간 이동시 지연시간
Fig. 6. Handover latency between the Zone-Masters.

무선 구간의 전송 속도는 10ms로 가정하였고, 가로 축은 존 마스터의 개수, 세로축은 지연시간을 나타낸다.

그림 6에서처럼 본 논문에서 제안하고 있는 기법이 AAA 인증 서버 환경에 비해 지연시간이 감소함을 확인할 수 있다. 이는 제안 기법의 경우 커뮤니티 멤버간 상호 인증 및 세션키 분배과정에서 AAA 인증 서버의 도움 없이 상대 이웃 노드의 ID 정보만을 이용하여 상호 인증 및 세션키를 교환하여 전체 메시지 교환수를 줄였기 때문이다. 이처럼 제안 기법은 커뮤니티 네트워크 기반 유비쿼터스 환경에서 빈번하게 커뮤니티를 이동하는 커뮤니티 멤버노드의 상호 인증 및 세션키 교환 과정에서 통신오버헤드를 줄일 수 있다.

## V. 결 론

본 논문은 커뮤니티 네트워크 기반의 유비쿼터스 환경에서 커뮤니티 멤버 노드의 ID를 이용한 상호 인증 및 세션키 교환 기법을 제안하였다. 커뮤니티 멤버 노드가 다양한 커뮤니티 환경을 자유롭게 이동할 경우 AAA 인증 서버 환경에서는 매번 AAA 인증 서버를 통해 재인증을 받아야 한다. 때문에 전체 인증 지연시간 및 통신 오버헤드가 증가한다. 이러한 문제를 해결하기 위해 본 논문에서는 ID 기반의 커뮤니티 멤버간 상호 인증 및 세션키 교환 기법을 제안하였고, 제안 기법과 AAA 인증 서버 환경과의 비교 분석을 통해 상호 인증 및 세션키 교환 과정에서 발생하는 지연시간과 통신 오버헤드가 감소하는 것을 확인하였다.

## 참 고 문 헌

[1] S. Corson and J. Macker, "Mobile ad-hoc networking (MANET)," IETF RFC 2051, January 1999.
[2] C. Siva Ram Murthy and B. S, Manoj, Ad Hoc Wireless Networks Architectures and Protocols, Prentice Hall PTR, New Jersey, 2004.
[3] K. Namhi, P. Ilkyun, and K. Younghan, "Ubiquitous zone networking technologies for multi-hop based wireless communications," IWSOS 2006, LNCS 4124, September 2006.
[4] C. Jaeduck, R. Hyosun, J. Souhwan, and K. Younghan, "Support of Context-awareness in Ubiquitous Networks using Smart Packet," IPSJ SIG 2005, pp. 275-280, 2005.
[5] P. Argyroudis and D. O'Mahony, "Secure routing for mobile ad hoc networks," Communications surveys & Tutorials, IEEE volume 7, pp. 2-21, 2005.
[6] M. Maurer and Y. Yacobi, "A remark on a Non-interactive public-key distribution system," EUROCRYPT' 92, 1998.
[7] D. Simon, B. Aboba and R. Hurst, "The EAP-TLS Authentication Protocol," IETF RFC 5216, March 2008.
[8] S. Kent and K Seo, "Security Architecture for the Internet Protocol," IETF RFC 4301, December 2005.
[9] T. Kwon, S. Baek, S. Pack, and Y. Choi, "AAA for NEMO", IETF Internet Draft, draft-kwon-aaa-nemo-00, January 2006.
[10] C. Perkins, E. Belding-Royer and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing," IETF RFC 3561, July 2003.

### 저 자 소 개

노 효 선(정회원)
2005년 숭실대학교 정보통신전자공학부 학사
2007년 숭실대학교 정보통신전자공학과 석사
2007년~현재 숭실대학교 전자공학과 박사과정
<주관심분야 : 이동 네트워크 보안, 네트워크 보안>

정 수 환(평생회원)-교신저자
1985년 서울대학교 전자공학과 학사
1987년 서울대학교 전자공학과 석사
1996년 University of Washington 박사
1996년~1997년 Stellar One SW Engineer
1997년~현재 숭실대학교 정보통신전자공학부 부교수
<주관심분야 : 이동인터넷 보안, 네트워크 보안, VoIP 보안, RFID/USN 보안>