# 애드 혹 네트워크를 위한 거리기반 인증된 키교환 기법+

조우원*, 김범한*, 이동훈*
*고려대학교 정보보호대학원

# Authenticated Key Agreement for Ephemeral Ad Hoc Network Using Distance Bounding

Woo Won Cho*, Bum Han Kim*, Dong Hoon Lee*
*Center for Information Security Technology, Korea University

## 요 약

무선 이동 Ad hoc 네트워크는 고정된 인프라의 도움 없이 이동 노드들의 협력에 의해 자율적으로 구성되는 독립적이고 융통성 있는 네트워크이다. 최근 상업적인 분야에서도 Ad hoc 네트워크의 응용에 대한 관심이 급증하면서 Ad hoc 네트워크의 보안 문제도 해결되어야 할 기술적 요구사항으로 대두되고 있다. 특히, 이러한 요구사항을 만족시키기 위해 Ad hoc 네트워크상에서 공개키 기반구조(PKI)를 도입하는 것은 고정된 인프라를 사용하지 않는 애드혹 네트워크 특성상 매우 제한적인 기법이다. 또한 password를 기반으로 하는 인증된 키교환을 하기위해서는 모든 사용자가 사전에 password를 공유를 해야 하는 불편함이 있다. 본 논문에서는 인증을 위한 제 3의 신뢰기관이나, 사전 비밀 공유가 필요 없는 인증된 키교환 프로토콜을 제안한다.

## I. 서론

무선 이동 Ad-hoc 네트워크는 고정된 인프라의 도움 없이 이동 노드만으로 구성되는 자율적이고 독립적으로 구성되는 네트워크이다[1, 2, 3]. 이러한 Ad-hoc 네트워크는 기반구조가 존재하지 않거나 기반구조의 구축이 어려운 환경에 적합한 네트워크로 인식되어 왔으나, 최근 유비쿼터스(Ubiquitous) 컴퓨팅 기술이 부각되면서 Ad-hoc 네트워크가 구성의 융통성을 제공하고 일시적이며 필요에 의한 임시 네트워크 구성이 용이하다는 특성으로 인해 최근 다양한 분야에서의 응용이 논의되고 있다[4]. 최근에는 상업적인 분야에서 Ad-hoc 네트워크에 대한 관심이 급증하면서 Ad-hoc 네트워크에서의 보안문제가 큰 이슈가 되고 있지만, Ad-hoc 네트워크상의 특징 때문에 공개키 기반구조에 의존할 수가 없고, 특정 서버에 의존할 수가 없으므로 보안 기능들 역시 노드들의 협력에 의해 분산된 형태로 운영될 수 있어야 한다.

이러한 Ad-hoc 네트워크 중에서 단거리(10m이내) 네트워크를 고려하여, 제안된 거리기반의 인증된 키교환 기법은 기존의 공개키 기반구조(PKI)의 암호시스템에서의 인증서 관리보다 제한성이 적다는 장점과 기존의 ID기반 암호기법을 사용하기 위해 해당 노드의 ID에 대한 키가 미리 발급되는 경우, 기능상이나 의미상의 차이는 있겠지만 기존의 PKI에서와 유사하게 발급된 키의 상태를 관리할 수 있는 보안 관리구조가 필요하지 않는 장점이 있다.

## II. 관련 연구

기존에 J. Hubaux 등에 의해 제안된 프로토콜은 고정된 인프라와 사전의 어떠한 정보도

+ 본 연구는 2006년도 두뇌한국 21사업으로 수행되었음

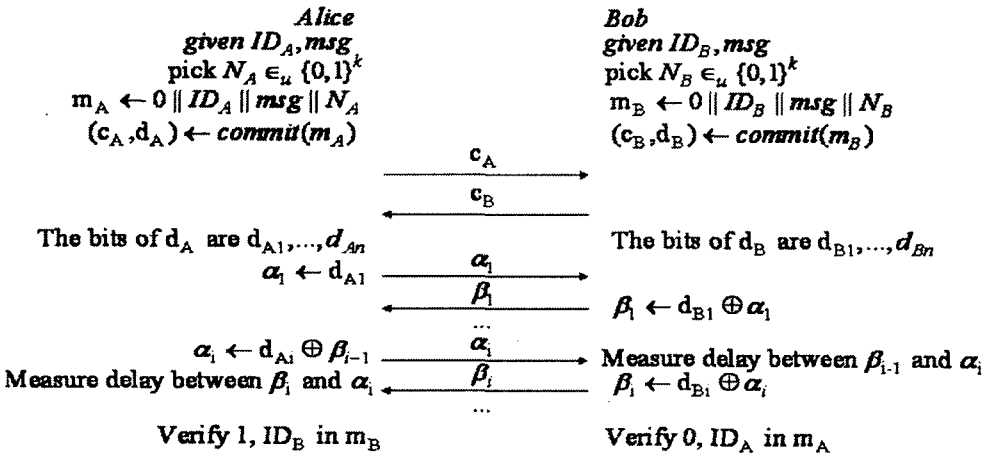


그림 1 거리기반 메시지 교환 방법

없이 단대단으로 키를 설립하는 방법이다.[5] 이 프로토콜은 거리기반[6]의 특징을 사용한다. 거리기반이란, commitment를 이용하여 어떠한 사용자라도 사용자간의 거리를 늘릴 수는 있지만 줄일 수는 없다는 특징이다. 이 프로토콜은 단대단 환경에서 각 사용자는 거리기반의 특징을 이용하여 통신하려고 하는 상대방과의 사이에 아무도 없으면 올바른 공개된 파라미터 값을 악의적인 사용자의 변조 없이 안전하게 교환할 수 있다고 확신을 할 수 있는 프로토콜이다. 하지만 이 프로토콜은 단대단 환경에서만 적용된다는 한계점이 있다. 하지만, 본 논문에서는 Ad-hoc네트워크의 환경에서도 인증된 키교환을 할 수 있는 프로토콜을 제안하였다.

## III. 제안 프로토콜

본 논문에서는 제안하는 프로토콜은 기존 논문에서 제안된 Ad-hoc환경에서의 키교환 프로토콜에의 복잡한 공개키 기반구조(PKI) 혹은 보안관리 구조가 필요한 ID기반 암호기법을 사용하지 않고 거리기반으로 Ad-hoc에 있는 노드들을 인증하여 키교환을 하는 프로토콜이다.

이 프로토콜에서는 모든 메시지 교환을 제안된 거리기반 메시지 교환 방법을 이용하여 수행한다.

이 프로토콜은 다음과 같은 가정 하에 설계되었다.

- 사용자는 라디오 송수신기가 장착된 장치를 가지고 있다.
- 각 장치는 사람에게 친숙한 인터페이스를 제공한다.
- 공격자는 라디오 통신 채널을 악의적으로 조작할 수 있다.
  - 임의의 메시지를 전송할 수 있다.
  - 어떤 사용자와도 통신을 시작할 수 있다.
- 통신하는 노드들은 서로 신뢰하며 그들의 장치들은 정직하다.

1. 제안된 거리기반 메시지 교환 방법 (그림 1)

Step 1. 사용자 A는 주어진 $ID_A$와 메시지와 선택한 $N_A \in_u 0,1^k$를 이용하여 $m_A \leftarrow 0 \| ID_A \| Msg \| N_A$를 생성한다. $m_A$를 commitment 함수에 넣어서 $C_A, D_A$를 생성 후, $C_A$를 B에게 보내고, $C_B$를 받는다.

Step 2. $D_A$를 첫 번째 비트를 B에게 보내고 받은 $D_B$의 비트와 $D_A$의 두 번째 비트를 XOR하여 B에게 보내고 B에게서 bit가 온 시간을 측정한다.

Step 3. 위의 Step 2단계를 $D_A$를 전부 보낼 때 까지 반복 후, $C_B$와 $D_B$를 이용하여 $M_B$를 계산하고 검증한다.

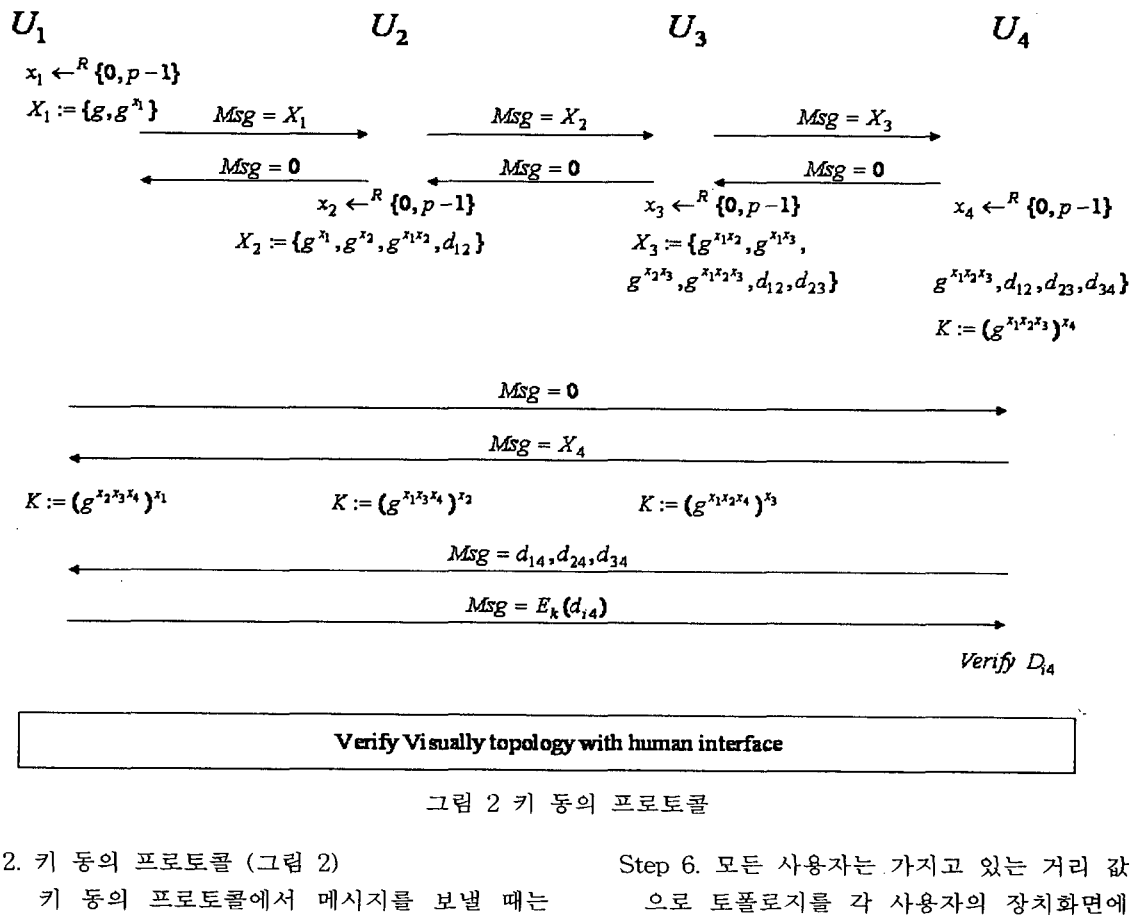


그림 2 키 동의 프로토콜

2. 키 동의 프로토콜 (그림 2)

키 동의 프로토콜에서 메시지를 보낼 때는 항상 제안된 거리기반 메시지 교환방법을 쓴다.

Step 1. 처음 사용자는 자신의 비밀값 $x_1$를 이용하여 $X_1 := g, g^{x_1}$를 생성하여 다음 사용자에게 보낸다.

Step 2. 다음 사용자는 받은 메시지에다가 자신의 비밀값 $x_i$를 지수승한 값과 통신을 하면서 알아낸 거리값($d_{ij}$)을 추가하여 다음 사용자에게 보낸다.

Step 3. 마지막 사용자가 메시지를 받을 때까지 Step 2를 반복한다.

Step 4. 마지막 사용자가 값을 받으면 마지막 사용자는 모든 사용자에게 키를 제외한 자신의 비밀 값을 지수승 한 값들과 거리 값들을 모든 사용자에게 보내준다.

Step 5. 마지막 사용자는 Step 4.에서 알아낸 거리 값들을 모든 사용자에게 보내주고 각 사용자에게 받은 값으로 키를 검증한다.

Step 6. 모든 사용자는 가지고 있는 거리 값으로 토폴로지를 각 사용자의 장치화면에 표시를 하고 검증을 한다.

3. 토폴로지 검증

토폴로지 검증단계에서 각 사용자들은 자신이 가지고 있는 거리의 값으로 토폴로지를 장치에 표시를 할 수 있다. 그림 3은 사용자들이 가지고 있는 거리로 토폴로지를 화면에 표시한

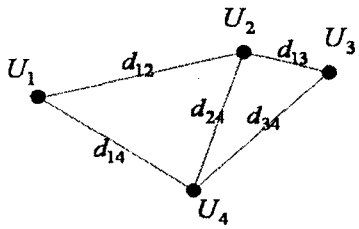


그림 3 거리로 그린 토폴로지

예이다. 사용자마다 토폴로지의 방향은 다르지

만은 결과적으로 토폴로지의 모양은 같게 된다. 이러한 토폴로지의 모양을 보면서 사용자들은 자신의 주변에 공격자가 없다는 것을 확인 할 수 있다.

4. 제안 프로토콜의 안전성 분석

제안된 프로토콜은 거리기반 메시지 교환방법에 의해 공격자가 메시지를 변조할 수 없으며, 토폴로지 검증방법에 의해서 정당하지 않은 사용자가 MITM(man-in-the-middle) 공격을 하는 것을 막을 수 있다. 이렇게 모든 사용자가 인증이 되면 이 프로토콜의 안정성은 Bresson 논문[7]에서와 같은 방법으로 증명 할 수 있다.

## IV. 결론

본 논문에서는 Hubaux에 의해서 제안된 키교환 프로토콜에의 복잡한 공개키 기반구조(PKI)와 보안관리 구조가 필요한 ID기반 암호기법을 사용안하고 거리기반으로 상대 노드를 인증하는 프로토콜의 peer-to-peer환경에서 고정된 인프라의 도움 없이 이동 노드들의 협력에 의해 자율적으로 구성되는 독립적이고 융통성 있는 무선 이동 Ad hoc 네트워크로 확장을 시켰다. 이 제안된 프로토콜은 현재 상업적으로 큰 인기가 있는 모바일 또는 게임기 등과 같은 단거리 Ad-hoc에서 사용할 수 있다.

## [참고문헌]

[1] 권혜연, 신재욱, 이병복, 최지혁, 남상우, 임선배, "이동 ad hoc 네트워크 기술 동향", 전자통신동향분석서, 제18권, 제2호, 2003년 4월

[2] Mohammad Ilyas, "The Handbook of ad hoc Wirelss Networks", CRC Press, 2003.

[3] C. E. Perkins, Ad hoc Networking, AddisonWesley, 2001.

[4] 권혜연, 신재욱, 이병복, 최지혁, 남상우, 임선배, "이동 ad hoc 네트워크 기술 동향", 전자통신동향분석서, 제18권, 제2호, 2003년 4월.

[5] Mario Cagalj, Srdjan Capkun와 Jean-Pierre Hubaux, "Key Agreement in peer-to-peer Wireless Networks", IEEE, Vol. 94, NO. 2, February 2006.

[6] S. Brands and D. Chaum, "Distance-bounding protocols", EUROCRYPT. Heidelberg, Germany, Springer-Verlag, 1993, vol. 765, *Lecture Notes in Computer Science*, pp. 344-359

[7] Emmanuel Bresson, Olivier Chevassut, David Pointcheval, jean-jacques Quisquater, "Provably Authenticated Group Diffe-Hellman Key Exchange", ACM CCS '01, November 2001.