Journal of Korea Multimedia Society Vol. 11, No. 8, August 2008(pp. 1121-1128)

Ad-Hoc환경에서 효율적인 라우팅 및 인증 기술에 관한 연구

강서일†, 이임영††

요 약

Ad-Hoc네트워크는 무선 통신의 디바이스들로 구성된다. 따라서 네트워크의 구성은 동적이며, 통신 경로의 변경이 필수적으로 요구된다. 이로 인해 안전한 라우팅 경로와 인증기술에 대한 연구가 필수적이다. 본 논문은 Ad-Hoc 환경에서 안전한 라우팅과 인증 방안에 대하여 제안하며, Ad-Hoc 네트워크와 무선랜을 연결하여 사용자가 이기종 네트워크 서비스를 제공받을 수 있는 방안을 제시한다. Ad-Hoc네트워크의 라우팅 방식의 경우 기존 연구에서는 구성 디바이스가 탈퇴하면 다시 라우팅이 필요하지만 본 연구에서는 홉 수를 이용한 우회 경로를 제공한다. Ad-Hoc네트워크에서 안전한 사용자 인증 및 라우팅 경로의 설정으로 유비쿼터스 서비스를 제공한다.

A Study on Efficient Routing and Authentication Scheme in Ad-Hoc Environment

Seo-Il kang†, Im-Yeong Lee††

ABSTRACT

Ad-Hoc network is consisted with the device of wireless communication. Therefore, the organization of network is dynamic and the changing communication channel is essential. According this, the study of secure routing route and certification technique has to be needed. In we research, we suggest not only the secure routing scheme in Ad-Hoc circumstance but also the method that user can be serviced the type of network which is connected Ad-Hoc network and wireless lam. In case of the routing form of Ad-Hoc Network, although in preexist study, when the device of organization withdraws, routing is needed, in we research, we suggest the detour route that is used hop frequency. We can offer the service of ubiquitous that the certification of secure user and the creation of routing route in Ad-Hoc network.

Key words: Authentication(인증), Ad-Hoc network(ad-hoc 네트워크), Routing(라우팅)

1. 서 론

Ad-Hoc네트워크는 디바이스의 이동성으로 인해 네트워크 구성이 동적이다. 그러므로 참여 디바이스들은 무선 통신 네트워크를 구성하는 라우팅 방안은 매우 중요하다. 또한 라우팅 경로의 안전성이 확보되어야 통신 및 서비스도 안전하게 제공 될 수 있다. 기존의 연구는 라우팅 경로를 안전하게 확보할 수

※ 교신저자(Corresponding Author) : 이임영, 주소 : 충남 아산시 신창면 읍내리 646(336-745), 전화 : 041) 542-8819, FAX : 041)530-1548, E-mail : imylee@sch.ac.kr
접수일 : 2008년 3월 15일, 완료일 : 2008년 6월 18일
† 준회원, 순천향대학교 컴퓨터공학부 (E-mail : kop98@sch.ac.kr)
†† 종신회원, 순천향대학교 컴퓨터공학부 교수
※ "본 연구는 지식경제부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음" (IITA-2008-(C1090-0801-0025))

있는 방안에 대하여 연구가 진행되어 왔다[1-3]. 경로 역할을 수행하던 디바이스가 이동하는 경우 다시 라우팅을 시작하여야 한다는 취약점을 가지고 있다. 그러므로 본 연구에서는 홉 수에 따른 경로를 저장하여 참여 디바이스가 이동하더라도 우회 경로를 제시하고, 사용자가 외부 서비스를 이용하는 경우 Ad-Hoc네트워크와 무선 랜을 연결하여 인증 및 안전한 통신로를 제공하는 방안에 대하여 논의한다. 본 논문의 2장에서는 보안 요구 사항을 기술하고 3장에서는 기존 라우팅 방식을 알아본다. 4장은 제안 방식을 설명하고 5장에서는 보안 요구사항으로 제안 방식을 분석한다. 마지막 6장에서는 본 연구의 결론 및 향후 방향에 대하여 기술한다.

2. 보안 요구 사항

사용자는 그림 1과 같이 Ad-Hoc네트워크 구성을 이룬 디바이스를 이용해 무선 랜 환경에 접근한다. 이와 같이 서로 다른 네트워크를 이용하는 서버스의 경우 다음과 같은 보안 요구 사항이 필요하게 된다[4,5].

- 디바이스의 인증 : Ad-Hoc 네트워크에 참여하는 디바이스는 임의 디바이스로 인증을 받지 못한 상태이며, 무선 랜의 서비스를 이용한다면 무선 랜의 인증 서버의 인증을 받아야 한다.
- 전송 데이터의 기밀성 : Ad-Hoc네트워크의 구성에서 통신 디바이스는 경로를 이루는 디바이스들을 통하여 데이터를 전송하게 된다. 만약 통신의 경로를 이루는 디바이스들 중에서 악의적인 목적을 가진다면 데이터의 수집 및 수정이 가능하다. 그러므로 데이터의 기밀성이 필요하다.

Ad-Hoc 네트워크에서 안전한 라우팅 과정을 위해서는 다음과 같은 사항을 고려하여야 한다.

① 안전한 통신을 위한 키 설립
② 새로운 디바이스가 가입하는 경우
③ 기존 디바이스가 탈퇴하는 경우

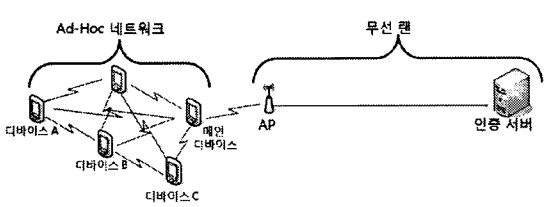

그림 1. Ad-Hoc 네트워크 및 무선 랜 서비스 환경

④ 불법적인 디바이스가 접근하는 경우

위의 사항들은 Ad-Hoc 네트워크에서의 통신 및 라우팅을 설정하는데 있어 필요한 고려 사항이며, 본 연구에서 라우팅 및 키 설립 방안에 대해 논의 한다. 또한 통신 경로의 디바이스가 탈퇴하는 경우 우회할 수 있는 방안이 필요하게 된다. 본 제안 방식에서는 네트워크 구성에 참여한 디바이스가 탈퇴한 경우에 대한 우회 경로를 제공한다. 따라서 본 연구에서는 라우팅 및 키 설립 방안에 대하여 중심적으로 논의하기로 한다.

3. 기존 연구 동향

Ad-Hoc에서 라우팅에 대한 연구는 디바이스의 연산 능력을 고려하여 인증서를 이용하는 공개키 및 해쉬 함수를 이용한다[2,6]. 경로 설정의 메시지들은 브로드캐스팅 됨으로 라우팅 경로를 새로 검색할 때마다 오버헤드가 증가 하며, 경로를 유지하던 디바이스가 탈퇴를 하는 경우 초기 브로드캐스팅의 라우팅 과정을 다시 해야 한다. 무선 랜의 경우 인증 서버에서 사용자의 아이디와 패스워드를 검증하여 인증을 제공하고 있다.

3.1 Ad-Hoc 위치 기반 라우팅 프로토콜

Ad-Hoc에서 디바이스가 이동하는 위치 정보를 근처의 디바이스에 알려 다른 디바이스가 통신 대상의 디바이스 위치를 알 수 있도록 하는 방안이다[7]. 디바이스의 암호화 방식은 공개키를 이용할 수 있다는 가정 하에 공개키의 서명과 GPS의 위치 정보를 제공하게 된다. 공개키 서명을 이용함으로 인해서 각각의 에러 메시지와 위치 정보에 대한 안전성을 제공할 수 있다. 찾는 디바이스의 정보를 알고 있는 다른 디바이스가 대신 알려주는 경우 제공하는 데이터에 전자 서명을 제공하게 된다.

3.2 Ariadne 프로토콜

Ariadne방식은 디바이스의 아이디와 해쉬 정보를 기반으로 라우팅 경로를 설정하는 방식으로 라우팅 경로 설정에 참여한 디바이스 정보를 해쉬하여 데이터를 생성한다[8]. 그러므로 경로가 설정된 이후 참여 디바이스가 탈퇴하는 경우 새로운 라우팅 경로

표 1. 기존 방식 분석

기존 연구	암호 방식	특 징
3.1 Ad-Hoc 위치 기반 라우팅 프로토콜	인증서	GPS를 이용한 위치 정보 제공, 디바이스 이동
3.2 Ariadne 프로토콜	해쉬	해쉬를 이용한 경로 무결성
3.3 ARAN 프로토콜	인증서	서명을 이용한 경로 메시지 제공
3.4 SAODV 프로토콜	인증서	서명 및 해쉬 체인을 이용한 경로 제공

설정을 해야 한다. 따라서 해쉬 정보를 전송하여 라우팅을 설정하게 되며, 해쉬에 사용되는 키는 각각의 참여 디바이스가 제공하게 된다. 라우팅 경로 설정 정보는 브로드캐스팅되므로 새로 경로 설정 시 마다 각각의 디바이스 통신량이 증가된다.

3.3 ARAN 프로토콜

ARAN(Authentication Routing for Ad-Hoc Networks)프로토콜은 Ad-Hoc네트워크 구성의 디바이스가 공개키 기반의 인증서를 이용할 수 있다는 가정 하에 라우팅 경로에 대하여 전자 서명을 하여 제공하게 된다[9]. 초기 서명에 대하여 목적 디바이스가 검증하고 경로상의 참여 디바이스가 전자 서명을 제공함으로써 안전한 경로를 통해서 제공되었다는 것을 확인할 수 있게 된다.

3.4 SAODV 프로토콜

SAODV(Secure Ad-Hoc On-demand Distance Vector)프로토콜은 해쉬를 이용한 경로 프로토콜에서 해쉬 체인을 이용하는 방식으로 변경하여 경로에 참여한 디바이스를 통과할 때 마다 해쉬 체인의 값을 제공하여 해쉬 체인의 값과 홉수를 이용하여 검증하게 된다[10]. 디바이스는 공개키 방식으로 인증서를 이용할 수 있으며, 전자 서명을 제공하여 검증 한다.

각각의 프로토콜을 보면 디바이스의 연산 능력을 어느 정도로 가정하는가에 따라 암호화 방식에 공개키 및 해쉬를 이용한다. 표 1은 각각의 프로토콜을 정리해 보여준다.

4. 제안 방식

제안 방식은 안전한 라우팅을 위한 방식과 무선랜 사용에서의 인증 서버를 통한 인증 방식으로 나누어 기술한다. 라우팅을 위해 사용되는 메시지의 내용은 다음과 같다.

- Request 번호, 출발 디바이스 아이디, 도착 디바이스 아이디, 중간 경유 디바이스 아이디, 경로에 해쉬값(H()), 홉 수(hop_No)로 표현한다.

4.1 안전한 라우팅 방식

안전한 라우팅 방식은 그림 2와 같은 Ad-Hoc 네트워크 환경에서 디바이스 (S)가 디바이스 (D)와 통신을 하기위해 경로를 설정하려고 한다. 경로는 디바이스 (A)부터 디바이스 (K)까지 여러 경로가 존재한다.

4.1.1 초기 경로 설정

step 1. 디바이스(S)는 라우팅을 위해 경로 설정 메시지를 브로드 캐스팅하여 도착 디바이스(D)까지의 경로를 찾게 된다. 즉 디바이스(S)는 디바이스 (A), (B), (C)에게 브로드캐스팅으로 Request_No가 1이며 S_{ID}로부터 출발하여 D_{ID}에 도착하여야 하고 현재 1홉 떨어져 있다는 경로 메시지를 전송한다.

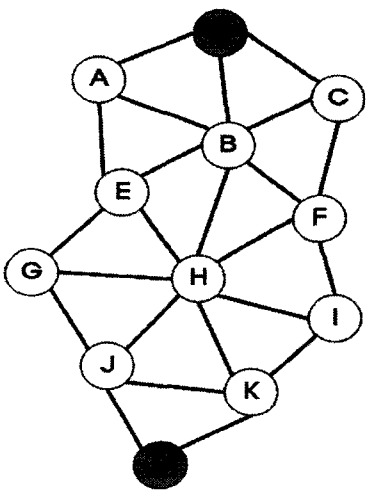

그림 2. 제안된 Ad-Hoc 환경

S→ A, B, C : 1,S_{ID},D_{ID},1

step 2. 디바이스 (A), (B), (C)는 경로에 참여 디바이스임을 알리기 위해 디바이스 아이디를 삽입하고, 해쉬 값을 포함 시킨다. 그로인해 참여 디바이스를 알 수 있다. 예로 디바이스 (A)는 디바이스 (E)와 디바이스 (B)에 전송하고, 디바이스 (B)는 디바이스 (A), (C), (E), (H), (F)에 전송한다. 그리고 디바이스 (C)는 디바이스 (B)와 (F)에 브로드캐스팅 한다. 디바이스 (A)와 (B)가 브로드캐스팅 메시지는 다음과 같다.

디바이스 (A)의 메시지 :

2,S_{ID},D_{ID},A_{ID},H(S_{ID},A_{ID}),2

디바이스 (B)의 메시지 :

2,S_{ID},D_{ID},B_{ID},H(S_{ID},B_{ID}),2

step 3. 디바이스 (A)의 경로 메시지를 받은 디바이스 (B)와 (E)는 동일한 경로 메시지를 전송하였는지 확인한다. 디바이스 (B)의 경우 request번호가 2번인 경로 메시지를 동일하게 전송하였으므로 디바이스 (A)와 (B) 사이의 경로를 삭제한다. 그러므로 최종에는 디바이스 (A)에서 디바이스 (E)로만 경로가 설정된다. 디바이스 (B)의 경우 디바이스 (A), (C)가 동일한 request번호의 메시지를 전송하므로 디바이스 (E), (H)와 (F)로 설정된다.

이와 같이 step 2 와 step 3를 반복적으로 실행하면 표 2와 같은 결과를 획득하게 된다. 표 2는 S_{ID}와 D_{ID}의 경로 중 홉 수가 4에 속하는 경로 두 개((ㄱ), (ㄴ)), 홉 수가 5에 속하는 두 개((ㄷ), (ㄹ))로 총 4개의 경로를 설정할 수 있게 된다. 이때 홉 수가 같은 두 개의 경로가 발견되면 왼쪽 우선순위를 두어 구별한다. 예로 표 2에서 4홉의 두 개의 경로((ㄱ), (ㄴ))를 보면 디바이스 (S)부터 디바이스 (H)까지 동일하고 디바이스 (J), (K)로 구별된다. 그림 3을 보면 디바이스 (J)가 왼쪽에 있으므로 무선 통신 경로는 4홉의 (ㄱ)이 된다.

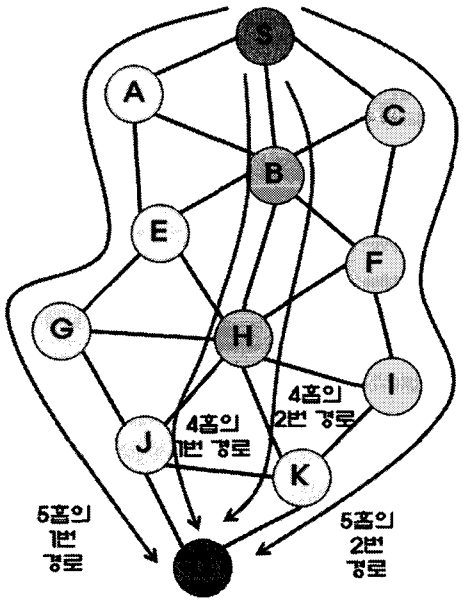

그림 3. 안전한 라우팅의 경로 설정

4.1.2 우회 경로 선택

표 2에서 디바이스 (S)와 (D)는 4홉의 (ㄱ)의 경로로 통신을 하고 있던 중 디바이스 (H)가 탈퇴하는 경우 디바이스 (H)가 포함된 경로를 이용하지 못한다. 그러므로 디바이스 (S)는 5홉의 경로 중 왼쪽우선 순위로 인해 (ㄷ)의 경로를 선택하여 통신한다.

4.1.3 키 설립

안전한 통신을 위한 키 설립 방안으로 경로 설정에 따른 서로 다른 키를 생성하여야 한다. 디바이스 (S)와 디바이스 (D)는 공유한 키 K를 가지고 있고 각각의 설정 경로에 따라 해쉬 값을 가지고 있다. 표 3에서 각각의 설정 경로에 따른 4개의 암호키 설립 내용을 표시한다.

표 2. 경로 설정 내용

출발	도착	홉수	라우팅 경로
S_{ID}	D_{ID}	4	(ㄱ) S → B → H → J → D
			(ㄴ) S → B → H → K → D
		5	(ㄷ) S → A → E→ G → J→ D
			(ㄹ) S → C → F→ I → K→ D

표 3. 경로에 따른 암호키

출발	도착	홉수	암호 키
S_{ID}	D_{ID}	4	(ㄱ) $K' = H(K\|\|S_{ID}\|\|D_{ID}\|\|B_{ID}\|\|H_{ID}\|\|J_{ID})$
			(ㄴ) $K'' = H(K\|\|S_{ID}\|\|D_{ID}\|\|B_{ID}\|\|H_{ID}\|\|K_{ID})$
		5	(ㄷ) $K''' = H(K\|\|S_{ID}\|\|D_{ID}\|\|A_{ID}\|\|E_{ID}\|\|G_{ID}\|\|J_{ID})$
			(ㄹ) $K'''' = H(K\|\|S_{ID}\|\|D_{ID}\|\|C_{ID}\|\|F_{ID}\|\|I_{ID}\|\|K_{ID})$

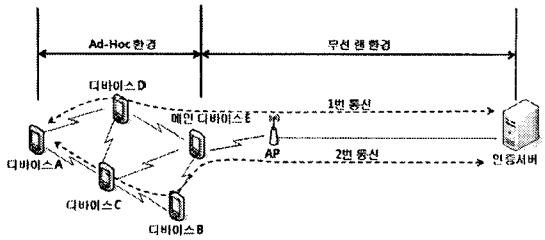

그림 4. 디바이스 A와 인증 서버의 환경

4.2 인증 서버를 이용한 인증 방식

Ad-Hoc 네트워크의 사용자 디바이스는 무선 랜의 서비스를 이용하기 위해 그림 4에서 인증 서버의 인증을 받아야 하며, 다음과 같은 과정을 가정한다.

① 사용자 디바이스는 Ad-Hoc 네트워크 환경으로 이루어 져 있으며, 메인 디바이스를 통해서 무선 랜 망을 이용한다.

② 사용자 디바이스는 인증 서버에 등록한 아이디, 패스워드 그리고 대칭키를 소유하고 있다.

4.2.1 안전한 Ad-Hoc의 경로 설정

그림 4는 Ad-Hoc 네트워크와 무선 랜 환경을 연동하는 것을 보여주고 있다. Ad-Hoc 네트워크에 참여하는 디바이스의 개수는 5개(A, B, C, D, E)이며, 무선 랜 환경과 연결하는 역할은 디바이스 E가 수행하고 메인 디바이스라 표시한다. 1번과 2번의 통신 경로를 보면 디바이스 (A)로부터 출발하여 디바이스 (D)와 (C), (B) 그리고 (E)를 통해서 AP에 접근하게 된다. 통신되는 데이터에 기밀성이 제공되지 않는 다면 경유 디바이스 (D), (C), (B), (E)에 노출된다. 제안 방식은 이와 같은 문제를 해결할 수 있는 방안을 제시한다. 안전한 Ad-Hoc의 경로설정은 4.1의 안전한 경로 설정 방식을 이용하며, 표 4는 경로 및 경로에 따른 암호화 키를 나타낸다.

4.2.2 시스템 계수

인증 서버를 통한 안전한 서비스 제공에서 사용되는 시스템 계수는 다음과 같다.

- BID : 익명 아이디
- KA : 인증 서버와 디바이스 (A) 간의 암호화 키
- R* : * 번째 랜덤 수
- ID : 인증 서버에 등록한 사용자 식별자
- pw : 인증 서버에 등록한 사용자 패스워드
- K : 경로에 따른 암호화 키
- Time_stamps : 시간 데이터
- K_{AE} : 디바이스 (A),(E)간의 공유키

4.2.3 디바이스 인증 프로토콜

디바이스 (A)가 메인 디바이스 (E)를 통해 인증 서버에 접근하여 인증을 받는 방식은 아래 단계와 같다.

step 1. 디바이스 (A)는 랜덤 수를 두 개(R1, R2)생성하여 사용자의 아이디를 대신할 BID($=h(A_{ID}||R1)$)를 생성한다. 그리고 인증 서버까지 안전하게 전송하기 위해서 암호화 키($KA=h(pw||R1)$)를 생성하여 데이터를 암호화($E_{KA}[h(pw||R2)||R2]$)한다. 그리고 경로에 따른 암호화 키 K(예:$K=h(A_{ID}||E_{ID}||D_{ID}||K_{AE})$)로 전체 데이터를 암호하여 디바이스 (E)에 전송한다. 전체 암호화 된 데이터는 아래와 같다.

$$E_K[BID||E_{KA}[h(pw||R2)||R2]||R1]$$

step 2. step 1의 암호화된 데이터를 디바이스 (A)와 공유한 키 K로 복호화한 메인 디바이스(E)ssm 디바이스 (A)의 BID와 R1을 획득한다. 그리고 AP에 디바이스 (A)로부터 전송받은 암호 데이터 $(BID, E_{KA}[h(pw||R2)||R2], R1)$를 전송한다. 이때 메인 디바이스 (E)는 익명 아이디(BID)를 통해서 이후 데이터를 전송할 디바이스를 분류한다.

step 3. 인증 서버는 디바이스 (E)로부터 수신한 데이터 R1을 이용하여 전체 참여 디바이스들의 BID($=h(*_{ID}||R1), *=A,B,...$)를 생성하여 수신한 BID와 일치하는 값을 조사하여 디바이스 (A)로부터 온

표 4. Ad-Hoc에서의 경로 설정

출발	도착	홉	경로	암호화 키
디바이스 A	메인 디바이스E	2	A→D→E	$K'=h(A_{ID}\|\|E_{ID}\|\|D_{ID}\|\|K_{AE})$
			A→C→E	$K''=h(A_{ID}\|\|E_{ID}\|\|C_{ID}\|\|K_{AE})$
		3	A→C→B→E	$K'''=h(A_{ID}\|\|E_{ID}\|\|C_{ID}\|\|B_{ID}\|\|K_{AE})$

것임을 확인한다.

step 4. 인증서는 A의 패스워드 pw를 가지고 복호화키($KA = h(pw||R1)$)을 생성하고, R2를 획득한다. 디바이스 (A)와의 통신에 사용될 KA2($= h(R2||R3)$)를 생성하여 디바이스 (E)에 암호화된 데이터 ($BID, E_{KA2}[\text{success}, \text{Server}_{ID}], R3$)를 전송한다. 이후 디바이스 (A)의 서비스나 통신에 있어 암호키 KA2를 이용한다.

step 5. 디바이스 (E)는 BID를 통해 디바이스 (A)에 암호 데이터($E_{KA2}[\text{success}, \text{Server}_{ID}], R3$)를 전송하고, 디바이스 (A)는 이후 인증 서버에 데이터와 타임스탬프를 암호화($E_{KA2}[data, Time\_stamps]$)하여 전송한다. 그림 5는 디바이스 (A)의 프로토콜의 전체 데이터의 생성 및 검증을 나타낸다.

5. 제안 방식 분석

제안 방식의 분석으로 디바이스 인증과 데이터의 기밀성에 대하여 논의한다.

• 디바이스 인증 방식 : 디바이스 (A)의 인증은 사용자의 아이디와 패스워드를 확인하고 각각의 키를 개별적으로 생성하여 메인 디바이스 (E)가 검증한다. BID는 메인 디바이스가 데이터를 전송할 디바이스를 구분할 수 있지만 사용자 실제 ID는 모르게 된다. 그러므로 통신 완료 이후 메인 디바이스 (E)는 부정한 아이디를 사용하려고해도 사용자 ID를 알 수 없으므로 BID를 만들 수 없다.

• 데이터의 기밀성 방안 : 데이터의 기밀성을 제공하기 위하여 암호화키 설립을 하는데 있어 인증서버와 공유한 정보를 이용하며, 메인 디바이스 E의 키는 사전의 공유를 통하여 디바이스 경로에 따라 서로 다른 대칭키 암호를 제공하게 된다.

제안 방식은 두 가지의 장점을 가지고 있다. 우선 첫 번째로 경로의 설정에 있어 중간 경유 디바이스가 사라지거나 기능을 제공하지 못하는 경우 이미 다른 홉의 경로를 알고 있기 때문에 우회 경로를 통해 서비스가 지속적으로 이용된다. 그림 3에서 최종적으

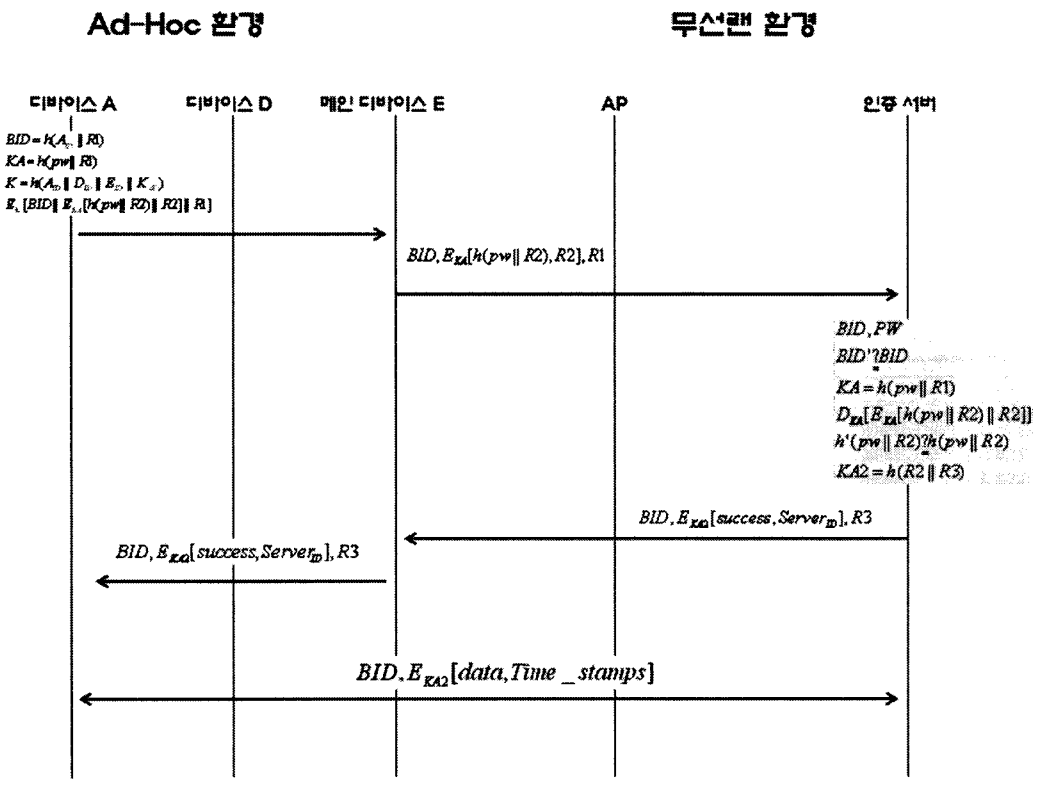

그림 5. 디바이스 A 인증 프로토콜의 전체 흐름도

로 연결되는 디바이스 (J)와 (K)가 빠진다면 다시 경로를 설정하여야 하지만 Ad-Hoc 네트워크의 크기가 크다면 우회 경로는 충분히 생길 수 있다. 단 디바이스의 개수가 증가하면 경로의 설정 테이블이 증가하는 오버헤드는 발생한다.

두 번째로 설정 경로에 따른 대칭키의 설립으로 경로에 따라 메시지 안전성을 제공할 수 있게 된다.

이전의 방식들은 경로가 변경되더라도 동일한 암호키를 사용하므로 제 3자가 동일한 키로 암호화 된 메시지를 많이 수집할 수 있다. 하지만 통신의 객체는 동일하면서도 경로가 변경되면 다른 암호키를 이용하기 때문에 이전의 암호 메시지를 수집하더라도 의미가 없어진다. 또한 디바이스의 연산량을 감안 한다면 공개키 보다 대칭키를 이용하는 방안이 좋을 것으로 사료된다.

그러나 본 방식은 홉 수의 차이가 나는 경로를 모두 저장하므로 테이블의 크기가 문제가 될 수 있다. 그러므로 향후 연구에서는 경로 저장 테이블의 크기를 어느 정도로 결정하는 지가 중요할 것으로 예상된다. 표 5에서 외부 네트워크 연결 방안은 기존 논문의 언급이 없으므로 비교에서 제외한다.

표 6에서의 비교는 총 참여 디바이스가 10개를 가정한다면 초기 경로 설정의 브로드캐스팅되는 메시지의 수는 다음과 같이 동일하다. 그러나 디바이스가 탈퇴 후에는 표 5에서 언급한 것처럼 새로운 설정을 위해 기존 방식은 동일하게 메시지를 브로드캐스팅하지만 제안 방식이 이전에 설정한 경로의 확인을 위한 메시지만 전송하면 됨으로 1회로 가능하다. 하지만 재설정후 경로의 최적화에 대하여 논의하면 기존 방식은 새로운 설정에 대한 경로의 최적화를 제공할 수 있지만 제안 방식의 경로는 홉수 내의 최적화일 뿐 현재 네트워크 상태에서의 최적화라고는 정확히 제시할 수 없다.

6. 향후 연구 및 결론

본 연구는 Ad-Hoc 네트워크에서의 경로를 설정하는 방안과 대칭키를 이용한 암호화 방식 및 무선

표 5. 기존 연구 방식과 제안 방식의 비교

	3.1 Ad-Hoc 위치 기반 라우팅 프로토콜	3.2 Ariadne 프로토콜	3.3 ARAN 프로토콜	3.4 SAODV 프로토콜	제안 방식
암호 방식	인증서	해쉬	인증서	인증서	해쉬, 공유키
디바이스의 탈퇴 경우	새로운 라우팅 필요	새로운 라우팅 필요	새로운 라우팅 필요	새로운 라우팅 필요	기존 홉 수를 변경
경로 우회 기능	제공 못함	제공 못함	제공 못함	제공 못함	제공 가능
암호키 분배	없음 (공개키 이용)	없음 (다른 방안 필요)	없음 (공개키를 이용)	없음 (공개키를 이용)	있음 (공유키와 경로로 결정)
경로 설정의 통신량	전자서명의 데이터	해쉬	전자서명의 데이터	해쉬 +전자서명 데이터	해쉬
외부 네트워크 망과 연결 방안	비교 제외	비교 제외	비교 제외	비교 제외	제시

표 6. 기존 방식과 제안 방식의 메시지 비교

	3.1 Ad-Hoc 위치 기반 라우팅 프로토콜	3.2 Ariadne 프로토콜	3.3 ARAN 프로토콜	3.4 SAODV 프로토콜	제안 방식
브로드캐스팅되는 총 메시지	10	10	10	10	10
디바이스 탈퇴후 브로드캐스팅되는 총 메시지	10	10	10	10	1
재설정 후 통신 경로의 최적화 가능성	최적화	최적화	최적화	최적화	홉 수의 최적화

랜과 연동 방안을 제시하였다. 제안 방식에서 디바이스에 대한 연산 능력을 작게 보았기 때문에 대칭키를 이용한다. 이와 같은 무선 통신 망간의 연동 동향은 향후 유비쿼터스 보안 기술로 지속적으로 연구되어질 것이다. 왜냐하면 어디서나 서비스를 받기 위해서는 선이 없는 무선 통신이 꼭 필요하며, 이러한 환경은 Ad-Hoc 환경이 적용되기 좋은 사례가 되며 외부 서비스를 제공받을 수 있는 방안이 된다. 홈 네트워크의 가전제품들도 Ad-Hoc 형태의 네트워크를 이루어 서비스를 제공하게 될 것이다. 향후 연구에는 기존 인프라와 Ad-Hoc 네트워크의 경계를 나타내고 이를 통합하는 보안에 대한 기술이 연구되어야 될 것으로 사료된다.

본 방식에서의 키 관리의 중요성이 부각되는데 이는 각각의 디바이스가 안전한 통신을 위해 암호 방식을 이용하므로 암호화 키의 안전한 관리 방안이 연구될 것이며, 디바이스에 따른 키 로밍 및 키 설립 과정이 더욱 연구 될 것으로 사료된다.

참 고 문 헌

[1] 박영호, 이경근, 이상곤, 문상재, "무선 Ad Hoc 네트워크에서의 안전한 라우팅 프로토콜에 관한 연구," 정보보호학회 논문지, 제15권 3호, pp. 76-81, 2005. 06.

[2] Seung Yi, Robin Kravets, "MOCA : Mobile Certificate Authority for Wireless Ad Hoc Networks," PKI 03, 2003.

[3] 이원희, 구재형, 이동훈, "Ad-Hoc환경에서의 2-라운드 비대칭 키 공유 기법," 한국정보보호학회 하계정보보호학술대회, Vol.13, No.1, pp. 89-92, 2003.

[4] S. Brands, D. Chaum, "Distance Bounding Protocols," EUROCRYPT, Heidelberg, Germany, Springer-Verlag, Vol.765, Lecture Notes in Computer Science, pp. 344-359, 1993.

[5] 이석래, 송주석, "Ad-hoc 네트워크에서 Hamming Distance를 이용한 인증프로토콜," 정보보호학회 논문지, 제16권 5호, pp. 47-56, 2006. 10.

[6] 조우원, 김범한, 이동훈, "애드 혹 네트워크를 위한 거리기반 인증된 키 교환 기법," 한국정보보호학회 하계정보보호학술대회 논문집, Vol.16, No.1, pp. 661-664, 2006.

[7] 임지환, 김상진, 오희국, "애드혹 위치기반 라우팅을 위한 안전한 위치 서비스," 한국정보보호학회 하계정보보호학술대회 논문집, Vol.16, No.1, pp. 665-669, 2006.

[8] Y.C. Hu, A.Perrig, and D.B.Johnson, "Ariadne: S Secure On-Demand Routing Protocol for Ad Hoc Networks," MOBICOM 2002, ACM Press, pp. 12-23, 2002.

[9] K. sanzgiri et al, "A Secure Routing Protocol for Ad Hoc Networks," ICNP 2002, IEEE Press, pp. 78-87, 2002.

[10] M. G. Zapata and N. Asokan, "Securing Ad Hoc Routing Protocols," WISE 2002, ACM Press, pp. 1-10, 2002.

강 서 일

2003년 2월 순천향대학교 정보기술 공학부 학사
2005년 2월 순천향대학교 전산학과 석사
2005년 3월~현재 순천향대학교 전산학과 박사 과정

관심분야 : 무선 네트워크 보안, 전자 투표, 전자 화폐

이 임 영

1981년 홍익대학교 전자공학과 졸업
1986년 오사카대학 통신공학전공 석사
1989년 오사카대학 통신공학전공 박사
1989년~1994년 한국전자통신연구원 선임연구원
1994년~현재 순천향대학교 컴퓨터 학부 교수

관심분야 : 암호이론, 정보이론, 컴퓨터 보안