情報保護學會論文誌
第17卷 第5號, 2007. 10

그룹서명에 기반한 익명성을 제공하는 애드 혹 라우팅 프로토콜*

백 정 하,† 김 범 한 , 이 동 훈‡
고려대학교

Anonymous Ad Hoc Routing Protocol based on Group Signature

Jung Ha Paik,† Bum Han Kim , Dong Hoon Lee‡
Korea University

요 약

최근 프라이버시 보호에 대한 관심 및 요구가 증가함에 따라 다양한 응용환경에서 익명성을 제공하려는 연구가 진행되고 있다. 익명성을 제공하는 애드 혹 라우팅은 네트워크에 참여하는 노드에게 프라이버시를 보장해 줄 뿐 아니라 네트워크의 정보 수집을 제한하는 장점을 가진다. 현재까지 다수의 익명라우팅 기법들이 제안되었지만 대부분의 기법들은 인증을 고려하지 않고 있어서 패킷 변조뿐만 아니라 서비스 거부 공격에 매우 취약할 수 있다. 본 논문에서는 MANET 및 VANET 등과 같은 모바일 애드 혹 네트워크 환경에서 익명성과 인증을 동시에 제공하는 라우팅 프로토콜을 제안한다. 제안하는 기법은 애드 혹 네트워크에서 제공해야 할 익명성을 모두 지원하고 그룹서명 기법에 기반하여 경로 탐색 과정동안 노드와 메시지에 대한 인증을 제공한다. 그리고 경로 탐색 과정과 세션키 공유 절차가 통합되어 안전한 데이터 전송 과정을 지원한다.

ABSTRACT

According to augmentation about interesting and demanding of privacy over the rest few years, researches that provide anonymity have been conducted in a number of applications. The ad hoc routing with providing anonymity protects privacy of nodes and also restricts collecting network information to malicious one. Until recently, quite a number of anonymous routing protocols have been proposed, many of them, however, do not make allowance for authentication. Thus, they should be able to have vulnerabilities which are not only modifying packet data illegally but also DoS(denial of service) attack. In this paper, we propose routing protocol with providing both anonymity and authentication in the mobile ad hoc network such as MANET, VANET, and more. This scheme supports all of the anonymity properties which should be provided in Ad Hoc network. In addition, based on the group signature, authentication is also provided for nodes and packets during route discovery phase. Finally, route discovery includes key-agreement between source and destination in order to transfer data securely.

Keywords : *Privacy, authentication, manet, ad hoc network, ad hod routing protocol, denial of service*

접수일: 2007년 6월 20일; 채택일: 2007년 8월 21일
* 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음 (IITA-2007-(C1090-0701-0025))
† 주저자, jungha.paik@gmail.com
‡ 교신저자, donghlee@korea.ac.kr

Ⅰ. 서 론

애드 혹 네트워크는 별도의 네트워크 기반구조 없이 노드 스스로 네트워크를 형성 및 유지하는 무선 네트워

크를 말한다. 애드 혹 네트워크에서는 기지국 없이 노드 간 통신이 가능해야 하기 때문에 노드 스스로 통신 경로를 탐색 및 유지하는 라우팅 프로토콜의 설계가 중요한 이슈이다. 국제인터넷표준화기구(IETF) 산하 워킹 그룹인 MANET(Mobile Ad Hoc Network)을 중심으로 효율적인 라우팅 기법들이 많이 제안되고 있으며, 안전한 라우팅 기법에 관한 연구도 성숙기에 들어선 상태이다. 최근에는 프라이버시가 새로운 보안 이슈로 부각되고 VANET(Vehicular Ad Hoc Network)과 같은 애드 혹 환경에서 위치 프라이버시의 보호가 중점이슈가 됨에 따라 익명성을 제공하는 라우팅 기법들에 대한 연구가 활발히 진행되고 있다.

애드 혹 라우팅에서의 익명성이란 네트워크에 참여하는 개체들의 프라이버시를 보장해야하는 성질을 의미한다. 또한 일반 라우팅 프로토콜과 비교하여 익명 라우팅 프로토콜에서는 공격자에게 정보의 수집을 제한하여 신뢰성 있는 네트워크 환경을 제공한다. 익명성을 제공하는 라우팅 프로토콜이 기본적으로 제공해야 하는 익명성의 성질은 다음과 같다.

- **개체 익명성(Entity Anonymity)** : 라우팅 과정과 데이터 전송 과정에서 패킷의 근원지와 목적지의 신원(identity)은 공격자와 중간 노드들이 식별 할 수 없어야 한다.
- **경로 익명성(Route Anonymity)** : 패킷의 근원지와 목적지, 그리고 패킷전송 경로 내에 있는 중간 노드들은 전달되는 패킷의 경로를 구성하는 노드를 파악할 수 없어야 한다.
- **위치/위상 익명성(Location/Topology Anonymity)** : 공격자와 네트워크 구성 노드는 라우팅 경로 탐색 과정 중에 얻을 수 있는 어떤 정보로도 인접노드나 목적지 노드의 위치, 경로의 홉(hop) 수 등을 알아낼 수 없어야 한다. 또한 네트워크 전체를 구성하는 노드의 구조나 개수 등을 알 수 없어야 한다.

기존에 제안된 익명 라우팅 기법들은 개체 익명성, 경로 익명성, 위치/위상 익명성을 만족하는 것을 목적으로 설계되었으나 익명성을 제공하는 대신에 대부분 인증을 고려하지 않고 있다. 인증과 익명성은 상호 대립되는 개념으로 개체 및 메시지 인증을 위해서 서명기법을 적용할 경우 서명검증을 위한 서명자의 공개키와 같은 신원정보가 필요하나 이를 통해서 익명성이 깨지기 때문에 익명성과 인증을 동시에 제공하는 것은 어려운 문제이다. 하지만, 무선 환경이라는 요소와 맞물려 인증이 제공되지 않는 라우팅 프로토콜은 네트워크에 심각한 보안 위협을 초래한다. 특히 익명성만을 제공하는 네트워크는 패킷의 변조뿐만 아니라 서비스 거부 공격에도 쉽게 노출된다.

본 논문에서는 서명자의 익명성을 보장하는 그룹서명의 성질을 이용한 애드 혹 라우팅 기법을 제안한다. 제안하는 기법은 경로 요청/응답 과정동안 익명성과 인증을 동시에 제공하는 것은 물론 경로 탐색과정이 완료된 후에는 근원지와 목적지의 공유 세션키를 생성하여 전송 데이터에 기밀성을 제공한다. 논문의 구성은 다음과 같다. 2장에서는 관련연구를 제시하고, 3장에서는 익명성을 제공하는 라우팅 프로토콜을 제안하며, 4장에서는 제안된 프로토콜의 익명성 및 안전성을 분석하고, 5장에서는 결론을 맺는다.

Ⅱ. 관련 연구

2.1. 기존에 제안된 익명 라우팅 기법들

Kong 등이 제안한 ANODR[9]은 *Onion Routing*[7][8][11] 방식의 라우팅 기법으로서 목적지의 trapdoor정보를 패킷에 포함시키고, 패킷을 전달하는 각 노드들은 전달되는 과정마다 패킷을 자신의 비밀키로 암호화 하고 경로 응답 패킷이 돌아오면 패킷을 복호화 하여 전달한다. 대부분의 익명성을 제공하는 라우팅 프로토콜들은 ANODR과 같이 목적지의 신원정보를 목적지만이 식별할 수 있게 패킷에 첨부하여 요청 패킷을 전달한다. Cheng 등은 공개키 시스템에 기반한 라우팅 프로토콜인 ASRP[6]를 제안하였다. 중간 노드들은 전달받은 라우팅 요청 패킷에 자신의 *pseudonym*을 랜덤하게 생성하여 패킷에 추가하여 전달하고, 라우팅 응답 패킷에서 *pseudonym*으로서 자신이 경로에 있었음을 확인한다. Sy 등은 ODAR[15]에서 *Bloom Filter*[2]를 사용한 익명 라우팅 기법을 소개하였다. *Bloom Filter*는 일련의 원소들을 포함하는 집합으로서 원소의 추출은 불가능 하지만 원소가 집합에 포함하는지에 대한 여부를 확인 할 수 있는 자료구조이다.

앞서 소개한 라우팅 기법들은 물론이고 대부분의 라우팅 프로토콜들은 인증을 제공하지 않고 있다. 이는 공격자가 라우팅 과정 중간에 끼어들어 악의적인 행위가

가능함을 암시한다. 특히 이들은 서비스 거부(DoS) 공격에 매우 취약하여 외부에 존재하는 공격자가 라우팅 경로 요청을 무작위로 시도하거나, 기존에 있던 라우팅 패킷을 캡쳐하여 재전송 하는 공격에 대한 해결책이 존재하지 않는다. 보다 자세히 설명하면, ANODR의 경우 공격자가 임의의 목적지의 공개키를 알고 있으면 목적지에 대한 경로 요청 패킷을 작성하여 무작위로 전송하는 것이 가능하다. 만약 공격자가 어떤 목적지의 공개키를 알 수 없다 하여도 경로 요청 패킷의 형태와 일치하는 의미 없는 패킷을 작성하여 무작위로 전송할 수 있고, 그렇게 포워딩 되는 패킷은 목적지를 찾지 못하고 모든 노드를 순회한 후 소멸할 것이다. 전자의 경우는 임의의 목적지에 대한 서비스 거부 공격이 발생 되는 것이고, 후자는 네트워크 전체에 대한 과도한 트래픽 발생이 공격의 결과가 될 것이다. 이는 ANODR과 같이 목적지의 공개키 정보에 기반 하여 경로를 탐색하는 익명 라우팅 기법들[6][9][17]에 모두 동일하게 적용된다. 그리고 공격자가 패킷을 임의로 생성하는 것이 가능하지 않은 라우팅 기법들[5][6][9][13][15][17]의 경우는 기존에 발생된 정당한 패킷들을 공격자가 저장한 후 무작위로 재전송하는 방법으로 서비스 거부 공격이 가능하다. 따라서 서비스 거부 공격을 원천적으로 봉쇄하기 위해서는 공격자가 임의로 패킷생성을 할 수 없게 방지해야 하는 것뿐만 아니라, 재전송되는 패킷이 네트워크에 포워딩 되지 않도록 사전에 차단해야 한다.

2.2. Group Signature 소개

그룹 서명은 그룹 멤버가 각자 신뢰된 키 발급 기관으로부터 서명용 개인키를 발급받아 서명을 생성할 수 있고, 검증자는 그룹의 공개키로 서명을 검증하여 서명자에게 신원을 노출하지 않고 그룹의 구성원임을 검증하는 서명 기법이다. 그룹서명에 사용되는 키는 그룹멤버의 서명용 개인키, 서명 검증용 그룹 공개키, 키 발급 기관이 가지는 마스터 비밀키와 같이 세 부분으로 구성된다. 그룹 서명이 일반적으로 제공하는 성질은 다음과 같다[1].

- **anonymity** : 그룹의 서명자는 검증시 신원이 노출되지 않아야 한다.
- **exculpability** : 그룹 멤버가 다른 그룹 멤버의 서명을 생성할 수 없어야 한다.
- **traceability** : 그룹 마스터 비밀키에 의해(신뢰된 키 발급기관에 의해) 서명의 신원추적이 가능해야 한다.
- **framing** : 그룹 멤버들의 결탁에 의해 임의의 멤버의 서명을 생성할 수 없어야 한다.
- **unlinkability** : 각기 다른 메시지와 서명 쌍이 주어져도 같은 서명자인지 아닌지 판단할 수 없어야 한다.

본 논문은 그룹서명에 기반한 라우팅 프로토콜을 제안한다. 위의 성질을 만족하는 그룹서명 기법을 이용함으로써 라우팅 프로토콜에 익명성을 보장하면서 동시에 인증을 제공할 수 있다. 본 절에서는 Boneh 등[4]이 제안한 SDH(Strong Diffie-Hellman) 문제[3]의 어려움에 기반 한 그룹서명 기법을 소개한다.

Short Group Signature : $\mathbb{G}_1$과$\mathbb{G}_2$가 위수를 소수 p로 갖는 순환군이라 하자. g_1, g_2는 각각 $\mathbb{G}_1, \mathbb{G}_2$의 생성자이다. x, γ는 각기 $\mathbb{Z}_p^*$에서 임의로 선택된 원소라고 할 때, 주어진 $(g_1, g_2, g_2^{\gamma}, g_2^{\gamma^2}, \ldots, g_2^{\gamma^q})$로부터 $(g_1^{(1/\gamma+x)}, x)$를 계산하는 문제를 *q-SDH(q-Strong Diffie-Hellman)* 문제라고 한다. SDH문제에 기반한 Boneh 등의 그룹 서명 기법은 [표 1]과 같다.

Ⅲ. 제안하는 라우팅 프로토콜

제안하는 프로토콜은 경로 탐색 과정에서 익명성을 제공하고 동시에 그룹서명을 이용하여 개체 인증을 제공한다. 라우팅에 적용되는 그룹서명 기법은 Boneh 등이 제안한 기법을 사용하지만 반드시 이 기법을 사용해야 하는 것은 아니다. 노드가 서명을 검증할 때 서명자의 익명성이 지켜지는 성질을 만족하고 안전성이 증명된 그룹서명이면 어떤 것이든지 제안하는 프로토콜에 적용이 가능하다. 또한 제안하는 프로토콜은 경로 탐색 과정을 모두 마치면, 근원지와 목적지와의 *Diffie-Hellman* 키 교환[16]을 수행되어 데이터 전송 과정에 포함되는 데이터의 기밀성을 보장한다. 제안하는 프로토콜은 다음과 같은 가정을 전제로 한다.

- 노드가 네트워크에 참여시 *TA*에 의해 동기화된 시간 정보는 매우 작은 오차범위에서 유지 가능하다.
- 라우팅 절차와 서명에 필요한 연산은 각 노드들이 효율적으로 계산 가능하다.
- 경로 요청을 하려는 근원지 노드는 목적지 노드의 공개키를 알고 있다.

〔표 1〕 Boneh의 Short Group Signature

(1) **키 설정 절차** : $KeyGen(n)$

- $u^{\xi_1}=v^{\xi_2}=h$의 관계를 만족시키는 $u,v,h\in\mathbb{G}_1$, $\xi_1,\xi_2\in\mathbb{Z}_p^*$, 를 선정하고, $\gamma\in^R\mathbb{Z}_p^*$, $w=g_2^{\gamma}$를 계산한다.
- n명의 멤버에 대해 $sk[i]=(A_i,x_i), 1\le i\le n$를 발급한다. $x_i\leftarrow^R\mathbb{Z}_p^*$에 대해 $A_i\leftarrow g_1^{(\gamma+x_i)^{-1}}$이다.
- $gpk=(g_1,g_2,h,u,v,w)$와 $gsk=(\xi_1,\xi_2)$를 각각 그룹 공개키와 비밀키로 정한다.

(2) **서명 절차** : $\sigma\leftarrow sign(gpk,gsk[i],M)$

- $\alpha,\beta\leftarrow^R\mathbb{Z}_p^*$를 선택 후, $T_1\leftarrow u^{\alpha}$, $T_2\leftarrow v^{\beta}$, $T_3\leftarrow Ah^{\alpha+\beta}$를 계산하고, $r_{\alpha},r_{\beta},r_x,r_{\delta_1},r_{\delta_2}\leftarrow^R\mathbb{Z}_p^*$를 선택 후, $R_1\leftarrow u^{r_{\alpha}}$, $R_2\leftarrow v^{r_{\beta}}$, $R_3\leftarrow e(T_3,g_2)^{r_x}\cdot e(h,w)^{-r_{\alpha}-r_{\beta}}\cdot e(h,g_2)^{-\delta_1-\delta_2}$, $R_4\leftarrow T_1^{r_x}\cdot u^{-r_{\delta_1}}$, $R_5\leftarrow T_2^{r_x}\cdot v^{-r_{\delta_2}}$ 를 계산한다.
- $c\leftarrow H(M,T_1,T_2,T_3,R_1,R_2,R_3,R_4,R_5)$와 $s_{\alpha}\leftarrow r_{\alpha}+c\alpha$, $s_{\beta}\leftarrow r_{\beta}+c\beta$, $s_x\leftarrow r_x+cx$, $s_{\delta_1}\leftarrow r_{\delta_1}+c\delta_1$, $s_{\delta_2}\leftarrow r_{\delta_2}+c\delta_2$를 계산한다.

(3) **검증 절차** : $True$ or $False\leftarrow verify(gpk,M,\sigma)$

- $\widetilde{R_1}\leftarrow u^{s_{\alpha}}\cdot T_1^{-c}$, $\widetilde{R_2}\leftarrow v^{s_{\beta}}\cdot T_2^{-c}$, $\widetilde{R_3}\leftarrow e(T_3,g_2)^{s_x}\cdot e(h,w)^{-s_{\alpha}-s_{\beta}}\cdot e(h,g_2)^{-s_{\delta_1}-s_{\delta_2}}\cdot(e(T_3,w)/e(g_1,g_2))^{c}$, $\widetilde{R_4}\leftarrow T_1^{s_x}\cdot u^{-s_{\delta_1}}$, $\widetilde{R_5}\leftarrow T_2^{s_x}\cdot v^{-s_{\delta_2}}$를 계산한다.
- $c=H(M,T_1,T_2,T_3,\widetilde{R_1},\widetilde{R_2},\widetilde{R_3},\widetilde{R_4},\widetilde{R_5})$이 성립하면 서명 검증을 통과한다.

3.1. 용 어

제안하는 라우팅 프로토콜에서 사용되는 용어는 〔표 2〕와 같다.

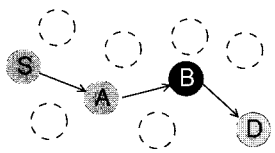
〔표 2〕 용어 정리

P_N	노드 N의 임시 식별자(pseudonym)
sk_N	노드 N의 그룹 서명에 사용되는 개인키
gpk	그룹서명 검증에 사용되는 공개 파라미터
$sign_{sk_N}$	그룹 서명 알고리즘
$verify_{gpk}$	그룹 서명 검증 알고리즘
σ_N	노드 N이 서명한 그룹 서명값
$E_k()/D_k()$	대칭키 암/복호화 알고리즘
$\{\}_N$	노드 N의 공개키의 의한 암호화
$H_k()$	비밀키 k가 적용된 해시함수
$H()$	해시함수
T_N	노드 N이 생성하는 타임 스탬프
k_N	노드 N이 생성하는 임시키
r_N	노드 N이 생성하는 난수

3.2. 네트워크 설정

라우팅 프로토콜에 그룹 서명을 지원하기 위해 신뢰된 키 발급기관인 TA가 그룹 키 생성 및 관리를 담당한다. 네트워크에 노드가 참여할 때 TA는 노드 N에게 서명용 비밀키 sk_N을 발급한다. sk_N은 그룹 서명 $\sigma_N\leftarrow sign_{sk_N}(m)$를 생성하는데 사용된다. 그리고 TA는 노드에게 시간 정보와 타임스탬프의 임계치(threshold)를 설정한다. TA로부터 입력된 시간정보를 이용해 노드는 타임스탬프 T_N을 생성한다. 임계치는 타임스탬프의 허용 한계치로서 네트워크 참여 노드의 데이터 전송속도와 통신반경에 근거하여 설정된다.

네트워크의 모든 노드는 $gpk:\{g_1,g_2,h,u,v,w\}$를 공개 파라미터로 갖으며, 각 노드는 라우팅 절차를 위해 〔그림 1〕과 같이 라우팅 테이블을 유지한다. 라우팅 테이블의 정보는 $(tag,P_I,k_I,status)$와 같이 유지된다. tag는 경로 요청/응답 패킷의 식별 번호로서 라우팅 테이블 참조를 위해 사용된다. P_I는 노드 I가 해당 경로 요청/응답 과정에서 사용하는 임시 식별자로서 이전 노드의 임시 식별자가 P_{I-1}라고 할 때, 해당 경로 요청세션에 대한 임시 키 k_I를 설정하여 $P_I=H_{k_I}(P_{I-1})$와 같이 계산한다.



tag -num	pseudo -nym	temp -key	status
tag	$P_B\leftarrow H_{k_B}(P_A)$	k_B	RQ
...	...	...	...

〔그림 1〕 라우팅 요청 과정 중의 노드 B의 라우팅 테이블

마지막으로 $status$는 현재 경로 요청에 관한 네 가지 상태를 나타내며 다음과 같다. RQ(requesting)는 경로

요청 중인 상태를 나타내며 매우 짧은 시간동안 테이블의 정보를 유지하고, *EST*(established)는 경로 요청이 완료된 상태로서 경로 에러 발생 전이나 매우 긴 시간 동안 정보를 유지한다. *SRC*(source)는 근원지 노드가 경로요청을 시도할 때 자신의 상태를 나타나는 것이고, *DST*(destination)은 경로 요청 패킷을 전달 받은 목적지가 사용하는 상태정보이다.

3.3. 경로 요청 단계

경로 요청을 하려는 근원지 노드 S에서 목적지 노드 D로의 경로요청(RREQ) 패킷의 구조는 다음과 같다.

$$< tag, \{tag \| g_2^{r_S}\}_D, P_N, T_N, \sigma_N >^{RREQ}$$

$\{tag \| g_2^{r_S}\}_D$는 RREQ 패킷을 전달받는 노드가 자신이 목적지임을 식별하기 위한 *trapdoor* 정보가 된다. 즉, 목적지가 $\{tag \| g_2^{r_S}\}_D$를 복호화 하였을 때 함께 첨부된 tag와 일치하는 것을 확인하여 경로요청의 목적지가 자신임을 확인할 수 있다. T_N은 *RREQ* 패킷 작성 시점의 시간정보, σ_N는 패킷을 전송하는 노드 N이 패킷 전체를 대해 $sign_{sk_N}$으로 그룹 서명을 생성한 값이다. $g_2^{r_S}$는 경로 요청/응답 과정이 완료된 후 근원지와 목적지 사이에 키 교환에 사용된다.

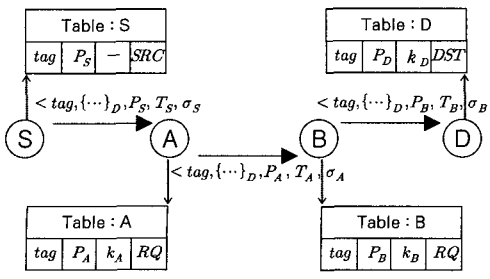
- **근원지 노드** : 근원지 노드 S는 목적지 노드 D로의 경로를 요청하기 위해 자신이 임의로 생성한 $r_S \in^{random} \mathbb{Z}_p^*$를 이용하여 $g_2^{r_S}$를 생성한다. S는 경로에 대한 $tag \in^{random} \mathbb{Z}_p^*$를 임의로 설정하고 tag와 $g_2^{r_S}$를 목적지의 공개키로 암호화 한다. 그리고 현재 시간정보 T_S를 생성하여 패킷에 저장하고, 마지막으로 자신의 임시 식별자 P_S와 패킷 전체에 대한 서명 σ_S 를 생성하여 RREQ 패킷을 작성한 후 다음과 같이 브로드캐스트 한다. 근원지 노드의 라우팅 테이블에는 $(tag, P_S, Null, SRC)$와 같이 저장된다.

$$S \rightarrow * : < tag, \{tag \| g_2^{r_S}\}_D, P_S, T_S, \sigma_S >^{RREQ}$$

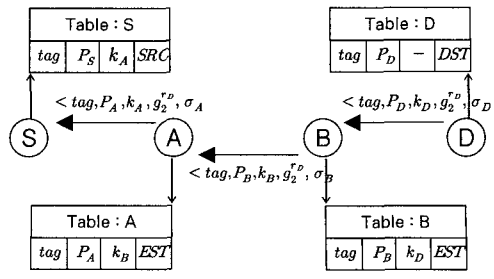
- **중간 노드** : RREQ 패킷을 전송받은 중간 노드 I는 자신의 라우팅 테이블에 일치하는 tag가 있으면 패킷을 버린다. 그렇지 않다면, 서명값 σ_{I-1}과 T_{I-1}를 확인하여 정당한 패킷인지 검사한다. 정당한 패킷이라면 자신의 암호화용 비밀키로 $\{tag \| g_2^{r_S}\}_D$를 복호화 하여 tag를 확인한다. $\{tag \| g_2^{r_S}\}_D$에 사용된 공개키와 연계된 비밀키를 가진 목적지만이 암호화되지 않고 첨부된 tag와 복호화 한 tag가 일치하게 된다. 다음 노드로 패킷을 전달하기 위한 임시식별자 생성을 위해 임시키 k_I를 생성하고 $P_I = H_{k_I}(P_{I-1})$를 계산 한다. 임시식별자 P_I와 타임스탬프 T_I를 첨부하고 전체 패킷에 대한 서명 σ_I 를 생성하여 다음과 같이 브로드캐스트 한다. 중간노드 I는 라우팅 테이블에 (tag, P_I, k_I, RQ)와 같이 저장한다.

$$I \rightarrow * : < tag, \{tag \| g_2^{r_S}\}_D, P_I, T_I, \sigma_I >^{RREQ}$$

- **목적지 노드** : 목적지 노드 D에 RREQ패킷이 도착하면 동일한 방법으로 이전 노드에 대한 서명을 검증하고 패킷의 tag와 T_{D-1}를 확인한다. 그리고 자신의 비밀키로 $\{tag \| g_2^{r_S}\}_D$를 복호화 하여 tag가 일치하는지 확인한다. 목적지 노드가 자신이 목적지임을 확인하면 복호화한 $g_2^{r_S}$ 로부터 자신이 선택한 $r_D \in^{random} \mathbb{Z}_p^*$를 이용하여 $g_2^{r_S r_D}$를 계산한다. $g_2^{r_S r_D}$는 근원지와 목적지가 갖게 되는 공유 비밀값이고, 데이터 전송단계에 사용될 대칭키를 계산해 낼 수 있다. 목적지 D는 자신의 라우팅 테이블에 (tag, P_D, k_D, DST)와 같이 저장 한다.



〔그림 2〕 경로 요청 과정 및 라우팅 테이블 저장 정보



〔그림 3〕 경로 응답 과정 및 라우팅 테이블 저장 정보

3.4. 경로 응답 단계

목적지 D에서 근원지 S로의 경로 응답 패킷(RREP) 구조는 다음과 같다.

$$< tag, P_N, k_N, g_2^{r_D}, \sigma_N >^{RREP}$$

P_N와 k_N는 노드 N 자신의 라우팅 테이블에 저장된 임시식별자와 임시키이고 $g_2^{r_D}$는 근원지가 양단간 공유 비밀을 생성하기 위한 정보이다.

- **목적지 노드** : 목적지 노드 D는 다음과 같은 RREP 패킷을 작성하고 서명을 하여 브로드캐스트하고 테이블의 임시키 k_D를 삭제한다.

$$D \rightarrow * : < tag, P_D, k_D, g_2^{r_D}, \sigma_D >^{RREP}$$

- **중간 노드** : 패킷을 전달받은 중간 노드 I는 서명을 검증하고 자신의 테이블의 같은 값의 tag가 있는지 확인한다. tag가 존재하면 임시식별자를 확인하여 자신이 경로였는지 확인한다. 즉, 전달받은 패킷에 첨부된 임시식별자를 P_{I+1}, 임시키를 k_{I+1}이라 할 때, 자신의 테이블에 저장된 P_I를 이용하여 $P_{I+1} = ?H_{k_{I+1}}(P_I)$를 확인하고, 이를 만족하면 자신을 라우팅 경로로 판단한다. 경로가 되는 중간노드는 패킷의 임시식별자와 임시키를 테이블에 저장된 자신의 P_I와 k_I로 교체하고 그룹서명을 계산하여 브로드캐스트 한다. 그리고 테이블에 임시키 k_I를 전달받은 임시키 k_{I+1}로 교체한다. 중간노드는 패킷 작성을 마친 후 자신의 서명을 생성하여 패킷에 첨부하고 브로드캐스트 한다. 마지막으로 경로 상태를 EST로 교체한다. 따라서 라우팅 테이블은 (tag, P_I, k_{I+1}, EST)와 같이 설정된다.

$$I \rightarrow * : < tag, P_I, k_I, g_2^{r_D}, \sigma_I >^{RREP}$$

- **근원지 노드** : 근원지 노드에 패킷이 도착하면 근원지 S는 서명과 tag을 검사한다. 서명이 정당한고 tag와 연계되는 테이블의 상태정보가 SRC이면 근원지 노드는 목적지 노드로의 경로 요청이 완료되었음을 확인한다. 근원지 노드는 중간노드와 마찬가지로 임시식별자를 확인하고 테이블 정보를 교체한다. 또한 전달받은 $g_2^{r_D}$를 이용하여 $g_2^{r_S r_D}$를 계산하여 목적지와의 공유 비밀값을 도출한다.

3.5. 데이터 전송 절차

경로가 설정된 근원지 S에서 목적지 D로의 데이터 전송(DFWD) 패킷의 구조는 다음과 같다. 데이터 전송 시에는 경로 탐색과정과는 다르게 근원지의 그룹 서명만 사용된다.

$$< P_{N+1}, tag, E_{K_{SD}}(DATA), \sigma_S >^{DFWD}$$

- **공유키 생성** : 근원지 S와 목적지 D는 공유 비밀값 $g_2^{r_S r_D}$를 이용하여 세션키 K_{SD}를 생성한다.

- **근원지 노드** : 근원지는 DFWD 패킷 작성을 위해 테이블을 참조한다. 포워딩 노드의 임시식별자 $P_{S+1} = H_{k_{S+1}}(P_S)$를 계산하여 패킷에 첨부한다. 그리고 데이터를 K_{SD}로 암호화하여 패킷을 작성한다. 그리고 자신의 라우팅 테이블에 tag를 $H(tag)$로 업데이트 한 후 마지막으로 P_{S+1}을 제외한 패킷의 서명을 생성하고 포워딩 한다.

- **중간 노드** : 패킷을 전달받는 중간노드 I는 서명과 T_S를 확인하여 패킷의 정당성을 검사하고, tag가 자신의 라우팅 테이블에 tag리스트에 포함되어 있는지 확인한다. tag가 포함되어 있다면 라우팅 테이블의 tag에 해당하는 임시식별자가 첨부된 임시식별자와 일치하는지 확인 한다. 경로가 되는 노드는 라우팅 테이블의 정보를 이용하여 P_{I+1}을 계산하고 자신의 라우팅 테이블에 tag를 $H(tag)$로 업데이트 한 후 패킷을 포워딩한다.

- **목적지 노드** : 패킷이 목적지에 도착하면 목적지는 서명 및 tag를 확인한 후 자신의 라우팅 테이블에 tag를 $H(tag)$로 업데이트 한다. 그리고 데이터를 K_{AB}로 복호화 하여 데이터를 처리한다.

Ⅳ. 제안하는 프로토콜에 대한 분석

4.1. 익명성 분석

- **개체 익명성** : 제안하는 라우팅 프로토콜은 신원정

보의 사용 없이 근원지에서 목적지로의 경로 요청/응답 과정을 완료한다. 따라서 중간 노드들이나 패킷을 감청하는 공격자는 근원지, 목적지의 신원을 알 수 없다. 응답과정에서 필요한 임시 식별자 P_I는 근원지는 임의로 생성하고 중간 노드와 목적지 노드는 $H_k()$를 이용해 생성하기 때문에 원래의 노드 신원 정보와의 연계는 불가능하다. 목적지 D가 자신이 경로 요청에 목적지라는 것을 판단하기 위해 사용되는 $\{tag \| g_2^{rs}\}_D$에는 g_2^{rs}가 포함되어 있다. g_2^{rs}는 근원지와 목적지 사이의 세션키 생성 목적 이외에도 목적지의 익명성 강화를 위한 의미도 포함한다. 만약 g_2^{rs}와 같은 랜덤한 값이 포함되어 있지 않다면 이전 세션에서 목적지 D의 공개키를 알고 있는 노드가 있다고 가정했을 때, tag를 목적지의 공개키로 암호화 하면 경로 요청 패킷의 목적지에 대한 부분적인 정보가 노출 된다. 하지만 랜덤한 값 g_2^{rs}이 포함되어 tag를 목적지의 공개키로 암호화 하는 방법으로는 목적지를 확인하는 것이 불가능하다.

- **경로 익명성** : 제안하는 프로토콜은 경로 요청/응답 패킷에는 경로를 구성하는 중간노드들의 식별자가 난수로 생성되고 노드들은 이웃 노드들이 전달해주는 난수 P_{I-1}의 해시값으로 저장하고 있다. 따라서 외부 공격자는 물론이고 근원지/중간/목적지 노드들 또한 경로 구성에 대해 알 수 없다.

- **위치/위상 익명성** : 경로 요청 패킷이 전달되는 동안 패킷은 일정한 크기를 유지하고 홉 수를 유추할 수 있는 정보가 존재하지 않는다. 또한 네트워크 전체를 구성하는 위상 구조나 노드의 수 등을 유추할 수 있는 정보가 패킷에 포함되지 않는다.

4.2. 안전성 분석

4.2.1. 인 증

제안하는 라우팅 프로토콜은 익명성을 유지하고 그룹 서명을 이용하여 경로 요청/응답 과정에 있는 노드에 대한 정당성과 데이터의 무결성 및 인증을 제공한다. TA로부터 인증 받고 그룹 서명키를 발급받지 못하는 외부 공격자는 패킷에 첨부되는 서명을 생성하지 못하기 때문에 네트워크에 참여하는 것이 불가능하다. 그리고 내부 노드가 경로 요청 및 응답 패킷과 데이터 전송 패킷을 임의로 생성하거나 변조하기 위해서는 그룹 서명을 위조(forgery)해야 한다. 따라서 제안하는 라우팅 프로토콜의 인증에 대한 안전성은 그룹서명의 안전성에 기반한다. 그룹서명은 exculpability 성질에 의해 타 노드의 서명을 생성할 수 없고, traceability 성질에 의해 신뢰기관이 개입으로 서명을 생성한 노드를 추적 할 수 있다. 만약 악의적인 목적을 가진 패킷이 생성되어 네트워크에 피해를 입혔다면, TA가 자신의 그룹 마스터 키를 이용해 악의적인 패킷을 생성한 노드를 추적할 수 있을 것이다.

4.2.2. 서비스 거부 공격

애드 혹 네트워크에서는 패킷이 생성되어 전송되면 네트워크 전체에 확산된다. 따라서 서비스 거부 공격에 의한 패킷을 네트워크에 참여하는 노드들이 판단하지 못하면 네트워크 전체에 과도한 트래픽이 생성되어 네트워크는 제 기능을 하지 못한다. 이 문제를 해결하기 위해 정당한 노드만이 패킷을 생성할 수 있어야 하고, 정당한 노드가 생성한 패킷을 공격자가 재전송 했을 때 그 패킷은 유효하지 않아 패킷이 포워딩되지 않아야 한다.

제안하는 기법은 경로 탐색 과정 중에 생성되는 패킷에는 그룹 서명과 타임스탬프가 포함된다. 또한 데이터 전송 과정 시마다 테이블에 저장되어 있는 tag에 대해 해시를 계산하고 테이블을 갱신한다. 이는 대부분의 익명 라우팅 기법이 가지고 있는 서비스 거부 공격(DoS)에 대한 취약점을 보완한다. 외부 공격자에 의한 서비스 거부 공격이 발생 가능한 시나리오를 다음과 같이 분류할 수 있다.

- **임의로 생성한 RREQ 전송** : 외부 공격자는 그룹 서명을 생성할 수 없으므로 정당한 패킷을 생성할 수 없다. 만약 의미 없는 RREQ를 생성하여 전송하여도 다음 노드에서 서명 검증을 통해 패킷은 버려질 것이다.

- **RREQ패킷 획득 후 재전송** : RREQ패킷을 전달받은 노드는 타임스탬프를 확인하기 때문에 패킷은 네트워크에 포워딩 되지 않을 것이다.

〔표 3〕 익명성 및 안전성 비교

프로토콜	개체 익명성	경로 익명성	위치/위상 익명성	인증/DoS 공격	세션키 일치
ANODR[9]	○	○	×†	×	×
ASRP[6]	○	○	○	×	△‡
ODAR[15]	○	○	○	×	○
제안하는 기법	○	○	○	○	○

† ANODR-BO, ANODR-TBO에 해당됨
‡ ASRP는 양단간 키 일치 과정을 수행하지 않고 근원지가 일방적으로 세션키를 전달

- **임의로 생성한 RREP 전송** : RREQ와 마찬가지로 RREP에는 각 홉의 서명이 추가되기 때문에 RREP 전송에 의한 서비스 거부 공격은 불가능하다.

- **RREP패킷 획득 후 재전송** : RREP에는 타임스탬프가 추가되지는 않지만, 라우팅 테이블에는 경로 상태에 대한 정보가 포함되어 있다. 공격자가 RREP 패킷을 획득 후 재전송하는 시점에는 경로 상태에 정보가 *EST*로 설정되어 경로 설정이 완료된 상태이기 때문에 패킷은 역시 버려질 것이다.

- **임의로 생성한 DFWD 전송** : DFWD에는 근원지의 그룹서명이 포함되어 공격자에 의한 패킷 전송은 불가능하다.

- **DFWD패킷 획득 후 재전송** : DFWD 패킷은 전송 시 마다 경로 안에 있는 노드들의 *tag*가 $H(tag)$로 업데이트 된다. 즉, 재전송 되는 DFWD의 *tag*는 네트워크에서 의미 없는 정보가 되어 버리므로, 서비스 거부 공격에 대해 안전하다.

제안하는 기법은 패킷에 그룹서명과 타임스탬프를 첨부하고 *tag*를 매 전송 시 마다 갱신하여 서비스 거부 공격 패킷의 네트워크 확산을 방지한다. 물론 네트워크 계층이 극복하기 어려운 서비스 거부 공격 문제는 여전히 가지고 있다. 예를 들어 공격자가 경로요청패킷을 임의로 생성하여 무작위로 전송하면 다음 홉에 있는 노드는 서명검증을 통해 무작위로 생성된 패킷임을 판단할 수 있고 네트워크로 포워딩 하지 않지만, 그 자체만으로 다음 홉에 있는 노드의 자원이 고갈 될 수 있다. 하지만 라우팅 환경에서의 서비스 거부 공격 방지의 주안점은 서비스 거부 공격 트래픽의 네트워크 분산을 억제하는 것이고, 위의 언급된 공격의 탐지 및 해결은 하위 계층인 데이터링크 계층에서 다루어야 할 문제이다.

4.2.3. 중간자 공격(Man-in-the-middle attack)

경로 요청/응답 과정 중에 수행하는 *D-H* 키 교환은 잘 알려져 있듯이 중간자 공격에 취약하다. 외부 공격자의 경우, 서명을 생성 할 수 없기 때문에 패킷에 포함되는 $g_2^{r_S}$ 및 $g_2^{r_D}$를 변조할 수 없음이 자명하다. 만약 악의적인 중간 노드 M이 존재하여 전달되는 데이터의 도청을 시도하려 한다고 가정하자. 노드 M은 경로 요청 과정 중에 $g_2^{r_S}$와 경로 응답 과정중에 $g_2^{r_D}$를 $g_2^{r_M}$으로 바꿔치기 하고 근원지로부터 오는 정보를 $g_2^{r_S r_M}$을 이용하여 복호화 하고, 목적지로 전달될 정보를 $g_2^{r_M r_D}$로 암호화 하여 전달해야 할 것이다. 하지만 제안하는 프로토콜에서는 근원지가 전송하는 값 $g_2^{r_S}$가 목적지의 공개키로 암호화 되어 있어 바꿔치기는 불가능하다. 경로응답 패킷의 $g_2^{r_D}$를 $g_2^{r_M}$으로 바꿔치기 하여도 $g_2^{r_S}$를 모르기 때문에 M은 $g_2^{r_S r_M}$를 계산할 수 없다.

4.3. 기존 기법들과의 익명성 및 안전성 비교

본 절에서는 앞서 소개한 기존에 제안되었던 라우팅 기법들과의 익명성과 안전성을 비교한다. 〔표 3〕은 기존에 제안되었던 익명성을 제공하는 라우팅 기법들과 본 논문에서 제안하는 라우팅 기법들이 비교 한다. 비교된 프로토콜들은 근원지와 목적지의 신원을 노출하지 않아 모두 개체 익명성을 만족한다. 또한 라우팅 경로 탐색 과정동안 생성된 경로에 대한 익명성도 보장되고 있다. 하지만 ANODR의 경우에 ANODR-BO와 ANODR-TBO 라우팅 모드에서 개체 익명성과 경로 익명성을 보장을 위해 대칭키 암호시스템을 사용하고, 라우팅 요청 과정

에서 각 중간 노드는 자신의 nonce 값이나 신원정보를 패킷에 덧붙여서 암호화 한다. 이로 인해 라우팅 경로의 길이가 패킷의 크기에 비례하게 되고 따라서 위치 익명성이 보장되지 않는다. ASRP와 ODAR은 경로 탐색 과정동안 패킷의 길이가 일정하게 유지되므로 위치 익명성을 보장한다. 하지만 위의 기법들은 모두 인증을 고려하지 않아 경로 탐색 과정에 대한 신뢰성이 결여되어 있고, 패킷 변조 등에 대한 공격에 안전하지 않다. 그리고 경로 요청 패킷의 확산되는 특성을 가진 애드 혹 네트워크에서 공격자가 서비스 거부 공격을 시도하면 네트워크에 전체적인 과부하가 발생하게 되어 결국 네트워크는 정상적인 작동을 하지 않게 된다. 제안하는 기법은 기본적인 익명성을 제공하는 것 뿐 만 아니라 그룹 서명에 기반 하여 개체 및 메시지 인증을 제공하고, 네트워크 단에서의 서비스 거부 공격에 대해 안전하다. 마지막으로 ANODR의 경우 경로 탐색과정 완료 후 키 일치에 대한 고려를 하지 않았고, ASRP는 키 일치를 수행하는 것이 아니라 근원지가 일방적인 세션키를 생성하여 목적지에게 전송한다.

4.4 효율성 분석

ID-Based 암호 시스템이나 그룹서명등에 사용되는 bilinear pairing 연산은 기존의 지수승, 대칭키 암호화 등 보다 무거운 연산으로 알려져 있다. 특히 제안하는 기법은 pairing 기반의 Boneh 등이 제안한 그룹 서명을 적용하기 때문에 그룹 서명 기법의 계산 효율성이 프로토콜의 계산 효율성에 큰 영향을 준다. Boneh 등의 기법은 자주 쓰이는 값을 선 계산하는 방법으로 필요한 연산횟수를 최적화 하면 서명 계산 시 8번의 지수승 연산이 소요되고 서명 검증 시 6번의 지수승연산과 1번의 pairing 연산이 필요하다[3]. 암호 및 pairing 라이브러리인 MI-RACL(Multiprecision Integer and Rational Arithmetic C/C++ Library)[10]에 대한 성능 측정 결과[12][14]에 의하면 Pentium-3 1.x GHz 대의 PC에서 1024bits 수준의 tate pairing 연산 1회에 20ms 정도소요 된다. 보다 명확히 하기 위해 MIRACL 라이브러리를 이용해 제안하는 기법에 필요한 암호 연산을 PocketPC-2003 기반의 PDA에서 속도를 측정하였다.

해당 기종의 CPU는 624MHz Intel PXA270 프로세서이고 이 CPU는 정수연산 및 부동소수점 연산이 Pentium-4 3.X GHz CPU보다 20배 이상 느린 속도로 동작한다. pairing 모드는 "The Eta Pairing over $\mathbb{F}_{2^m}$" 으로서 160bits 수준으로 설정하였다. PDA에서 테스트 결과 임의의 지수승 연산에 약 10ms, 임의의 두 포인트에 대한 pairing 연산에 약 25ms, 그리고 SHA1은 약 1~2ms가 소요되었다. 제안하는 기법에서 중간노드는 경로 요청 및 응답 패킷을 포워딩 할 때 서명을 검증하고 또 자신의 서명을 생성한다. 위의 수치에 근거하여 볼 때, 서명 생성 시에 약 80ms가 소요되고, 서명 검증 시에 약 85ms가 소요된다. 이는 제안하는 라우팅 프로토콜에서 중간노드가 패킷을 전달받고 다시 전송하는데 약 0.165 sec 정도의 시간이 소요됨을 의미한다. 물론 센서 네트워크와 같은 매우 제한적인 계산능력을 가진 환경에 적용하는 것은 어렵겠지만, PDA와 같은 모바일 환경에서는 충분히 적용 가능하다고 보여 진다.

V. 결 론

프라이버시 보호와 공격자에 의한 데이터 수집 제한을 위해 애드 혹 라우팅 프로토콜에 익명성을 보장하는 것은 매우 중요하다. 하지만 익명성만을 제공하는 애드 혹 라우팅 프로토콜은 공격자에 의한 가장공격, 패킷 변조 및 서비스 거부 공격에 매우 취약하다. 특히 애드 혹 네트워크는 패킷이 네트워크에 확산되는 특성을 가지기 때문에 서비스 거부 공격은 매우 치명적이다. 이를 해결하기 위해 라우팅 프로토콜에 익명성 이외에도 인증을 반드시 고려해야 한다. 제안하는 기법은 기본적인 익명성 요소를 모두 충족시키는 것 이외에도 그룹서명 기법을 이용하여 인증을 부여하였다. 각 노드는 네트워크에 참여시 신뢰된 키 발급기관(*TA*)으로부터 개인 서명키와 그룹 공개키를 발급 받아야만 패킷을 전송 및 전달할 수 있다. 그룹서명을 이용한 인증은 네트워크에 참여하고 있는 노드에게 익명성을 보장하는 동시에 정당한 노드만이 패킷을 전송 할 수 있게 한다. 이로 인해 외부 공격자에 의한 패킷 변조를 방지할 뿐 아니라 서비스 거부 공격을 차단하여 신뢰성 있는 네트워크 환경을 제공한다. 또한 제안하는 기법은 경로 설정이 완료 된 후 근원지와 목적지 사이에 공유키를 생성하여 데이터 통신의 기밀성을 보장해 준다. 향후 앞에서 언급했던 것과 같이 데이터 링크 계층과의 연계를 통한 인접 노드의 서비스 거부 공격 탐지 방안을 강구하여 보다 신뢰성 있는 네트워크 제공을 해야 한다. 그리고 그룹 서명 기법이 기본적으로 제공하는 *TA*에 의한 *open*절차를 적

절히 활용한 외부 공격자 이외에도 악의적인 내부 노드 탐지 기법의 고려가 필요하다.

참고문헌

[1] M. Bellare, D. Micciancio, and B. War-inschi, "Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions.", *Proceedings of Eurocrypt 2003,* volume 2656 of LNCS, pages 614-629, Springer-Verlag, May, 2003.

[2] B.H. Bloom, "Space/time trade-offs in hash coding with allowable errors.", *Communications of ACM,* 13(7):422-426, Jul 1970.

[3] D. Boneh and X. Boyen, "Short sig-natures without random oracles.", *Eurocrypt 2004,* pages 56~73. Springer-Verlag, May, 2004.

[4] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures.", *In CRYPTO,* vol.3152 of LNCS, pp. 41~55, 2004.

[5] A. Boukerche, K. El-Khatib, L. Xu, and Larry Korba, "SDAR:A Secure Distributed Anonymous Routing Protocol for Wireless and Mobile Ad Hoc networks", *LCN 2004,* IEEE, 2004.

[6] Yi Cheng and Dharma P. Agrawal, "Distributed Anonymous Secure Routing Protocol in Wireless Mobile Ad Hoc Networks.", *In OPNETWORK 2005,* Aug, 2005.

[7] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The Second-Generation Onion Router.", *Proceedings of the 13th USENIX Security Symposium,* Aug, 2004.

[8] D. Goldschlag, M. Reed, and P. Syver-son, "Onion Routing for anonymous and private internet connections." *Communi-cations of the ACM,* 42(2):39C4, 1999.

[9] J. Kong and X. Hong, "ANODR: Anony-mous On Demand Routing with Untraceable Routes for Mobile Ad-hoc Networks.", *In MOBIHOC,* 2003.

[10] MIRACL-Multiprecision Integer and Rational Arithmetic C Library, Available via anonymous ftp from ftp.compapp.dcu.ie in /pub/crypto

[11] M. Reed, P. Syverson, and D. Goldschlag, "Anonymous Connections and Onion Routing." *IEEE Journal of Selected Areas in Communications,* vol.16, no.4, pp.482-494, May 1998

[12] M. Scott, "Comparison of Methods for Modular Exponentiation on 32-bit Intel 80×86 processors", http://www.shamus.ie, 11. 1996

[13] S. Seys, and B. Preneel, "ARM: Anony-mous Routing Protocol for Mobile Ad hoc Networks", *AINA 2006 Workshops,* IEEE, pp. 133-137, 2006.

[14] Shamus Software, http://www.shamus.ie/

[15] D. Sy, R. Chen and L. Bao, "ODAR: On-Demand Anonymous Routing in Ad Hoc Net-works", *in Proc. of The Third IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASS),* October 2006.

[16] S. Wilson and A. Menezes, "Authen-ticated Diffie-Hellman Key Agreement Protocols.", *Selected Areas in Cryptography,* pp. 339-361, 1998

[17] L. Yang, M. Jakobsson and S. Wetzel. "Discount Anonymous On Demand Routing for Mobile Ad Hoc Networks." *SECURECOMM '06,* 2006.

〈著者紹介〉

백 정 하 (Jung Ha Paik) 학생회원
2006년 2월 : 고려대학교 수학과 졸업
2006년 3월~현재 : 고려대학교 정보경영공학전문대학원 석사과정
<관심분야> 암호 프로토콜, 애드 혹 네트워크, 응용암호, DRM

김 범 한 (Bum Han Kim) 학생회원
2004 년 2월 : 숭실대학교 수학과 졸업
2004 년 3월 : 고려대학교 정보경영공학전문대학원 석사
2006 년 3월~현재 : 고려대학교 정보경영공학전문대학원 박사과정
<관심분야> 암호프로토콜, VANET, USIM 보안, 애드 혹 네트워크, 응용암호

이 동 훈 (Dong Hoon Lee) 종신회원
1983년 8월 : 고려대학교 경제학사
1987년 12월 : Oklahoma University 전산학 석사
1992년 5월 : Oklahoma University 전산학 박사
1993년 3월~1997년 2월: 고려대학교 전산학과 조교수
1997년 3월~2001년 2월: 고려대학교 전산학과 부교수
2001년 2월~현재: 고려대학교 정보경영공학전문대학원 교수
<관심분야> 암호프로토콜, 암호이론, USN이론, 키 교환, 익명성 연구, PET 기술