익명통신의 개요 및 연구동향

박민호 | 서승우
서울대학교

요 약

본 고에서는 80년대 초부터 시작된 익명통신의 개요와 연구 동향에 대해서 소개한다. 그리고 최근에 이슈가 되고 있는 데이터 연결 계층에서의 익명성 보장 기법에 대해서 살펴본다.

I. 익명 통신이란?

익명통신(anonymous communication)이라 함은 말 그대로 익명성을 보장하면서 통신하는 것을 의미한다. 컴퓨터 네트워크에서 말하는 익명성은 엄밀히 말해 크게 두 가지로 정의 해 볼 수 있다. 먼저 수신/발신자 익명성 (source/destination anonymity) 이다. 이는 어떤 노드(node)를 관찰하고 있는 공격자(attacker)가 그 노드가 메시지를 주고 있는지 혹은 받고 있는지를 알지 못 하거나, 또는 공격자가 주고받는 메시지를 보고 누가 발신자이고 누가 수신자인지를 모르는 것을 의미한다. 두 번째로, 관계 익명성(relationship anonymity)이다. 어떤 노드들을 관찰하고 있는 공격자는 그 노드들 중에서 누가 보내고 누가 받는지를 알 수 있지만, 즉 발신자와 수신자는 알 수 있지만, 누가 누구에게 보내는지는 알 수 없음을 의미한다. 그러나 수신/발신자 익명성이 보장이 되면 당연히 관계 익명성 또한 보장이 되기 때문에, 많은 경우에 있어서 익명통신은 수신/발신자 익명 통신을 의미한다.

II. 익명 통신의 필요성

대부분의 네트워크에서는 안전한 통신을 위해서 보안대책을 마련 한다. 데이터의 암호화/복호화를 통해서 메시지의 기밀성 (confidentiality)을 확보하고, 메시지 인증 코드(message authentication code : MAC)을 사용하여 무결성(integrity) 검사와 발신자 인증(origin identification)을 하게 된다.

그러나 악의적인 공격자로부터 주고받는 메시지의 내용을 감추고, 그들이 임의로 메시지를 수정하는 것을 방지하는 것만으로는 안전하다고 말할 수 없다. 특히 모든 메시지 전송이 브로드캐스팅으로 이루어지기 때문에 누구나 쉽게 도청이 가능하여, 보안상 더 취약 할 수 밖에 없는 무선네트워크의 경우에는 더욱 위험하다. 왜냐하면, 메시지의 통신 패턴이나 주고받는 당사자가 누구냐 라는 정보 또한 악의적인 목적의 공격자에게는 중요한 정보가 될 수 있기 때문이다.

무선 센서 네트워크를 예로 들면, 어떤 이벤트(event)가 발생하였을 때에 어떤 노드(node)가 데이터를 전송했다고 하면 그 데이터가 무엇인지는 몰라도 분명 그 노드가 발생한 이벤트와 연관이 있을 것이라고 추정할 수 있다. 또 WLAN의 경우, STA(station)이 BS(Base Station)와 통신하는 패턴이 공격자에게 어떠한 식으로든지 정보를 줄 수 있고, 메시지의 헤더(header)내에 명시된 STA과 BS의 주소필드 자체가 STA의 위치를 노출 시킬 수도 있다.

이와 같이 메시지의 내용이 암호화 되어 읽을 수 없더라도 통신 패턴 혹은 매우 많은 메시지를 도청하여 저장, 분석함

으로써 필요한 정보를 유추하여 악의적으로 사용하는 공격 형태를 트래픽 분석 공격 (traffic analysis attack)이라고 하는데, 익명통신은 이와 같은 트래픽 분석 공격으로부터 안전하게 통신하기 위한 가장 좋은 방법이다.

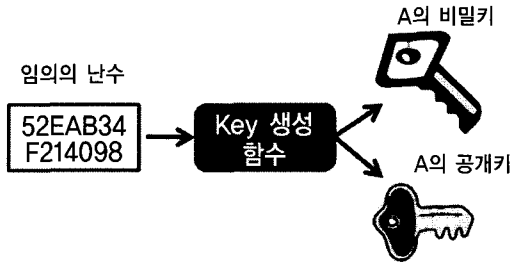
III. 익명 통신 관련 연구들

1. 암호/복호화 기술의 개요

메시지를 주고받을 때에 익명성을 보장하기 위한 방법으로 가장 먼저 연구가 되어 온 형태는 메시지 내의 발신인과 수신인에 대한 정보를 정해진 수신인외에는 확인 할 수 없도록 암호화해서 보내는 것이다. 이것은 안전한 통신을 위해서 발신인이 메시지의 내용을 특정인 외에는 읽을 수 없도록, 즉 메시지의 기밀성을 보장하기 위하여 그 메시지를 암호화하여 보내고, 오직 수신인만이 암호화된 메시지를 복호화 하여 읽을 수 있게 하는 것과 같은 방법이다. 메시지의 내용을 암호화 하느냐, 아니면 주소를 암호화 하느냐의 차이만 있을 뿐이다. 따라서 본 절에서는 익명통신의 관련 연구 설명하기에 앞서, 암호/복호화 기술에 대한 기본 개념에 대해서 소개한다.

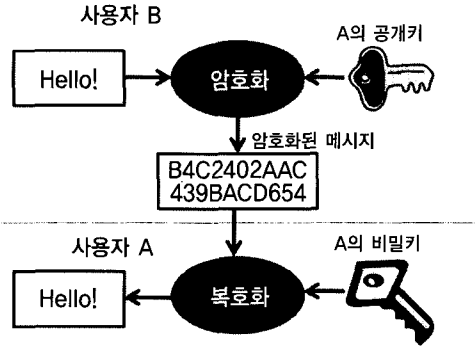
암호화(encryption)라함은 일반적으로 키(key)라고 불리는 특정한 지식이 없이는 정보를 읽을 수 없도록 만드는 일련의 과정을 의미한다. 반대로 복호화(decryption)는 해당 키를 가지고 암호화된 정보를 다시 읽을 수 있도록 바꾸는 과정을 말한다. 암호/복호화 기법은 키의 종류에 따라 대칭키(symmetric key) 기법과 비대칭키(asymmetric key) 기법으로 나눌 수 있다. 대칭키 기법은 암호화를 할 때의 키와 복호화를 할 때의 키가 동일하다. 즉 발신자와 수신자가 같은 키를 가지고 있어야 정보 교환이 가능하다. 반면에 비대칭키 기법은 암호화 할 때의 키와 복호화 할 때의 키가 서로 다르다. 일반적으로 비대칭키 기법은 공개키 암호화기법으로 알려져 있으며, 한 사용자는 공개키(public key)와 개인키(private)를 가지고 있다.

(그림 1)은 사용자 A의 두 개의 키 쌍(key pair)의 생성 예를 나타낸 것이다. 임의의 매우 큰 난수로부터 두 개의 키 값이 생성된다. 일반적으로 키 값은 매우 큰 숫자 값이다. 공개



(그림 1) 공개키 및 개인키 생성 예

키는 말 그대로 외부에 공개되어 있는 키로서 누구나 A의 공개키가 무엇인지를 알 수 있다. 반면 개인키는 A만이 가지고 있는 키로 외부에 노출되지 않고 안전하게 보관된다. 개인키로 암호화된 정보는 공개키로만 복호화 될 수 있으며, 반대로 공개키로 암호화 된 정보는 개인키로만 복호화 될 수 있다. 이러한 특징을 이용하여 두 개의 키는 메시지의 기밀성 제공을 위해서 사용될 수도 있으며, 전자서명에도 이용된다. 아래 (그림 2)는 A와 B와의 통신에서 기밀성을 유지하기 위하여 사용되는 예를 나타낸 것이다.

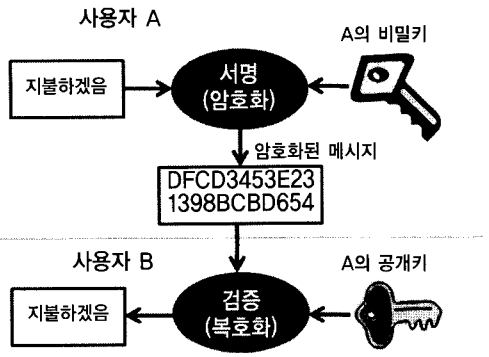


(그림 2) 공개키 기법을 이용한 메시지 기밀성 보장 예

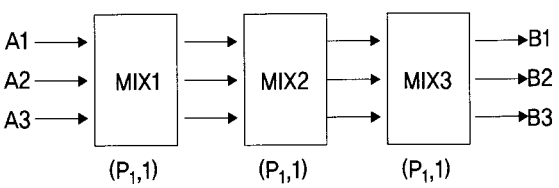
B는 A에게 메시지를 보내기 위해서 메시지를 A의 공개키를 이용하여 암호화하여 보낸다. 이렇게 암호화된 메시지는 A의 개인키로만 복호화가 될 수 있기 때문에 다른 누구도 읽을 수가 없어 기밀성이 보장이 된다.

또, 공개키 기법은 전자서명에도 이용이 된다.

(그림 3)의 예는 A가 B에게 빌린 돈에 대한 지불을 약속하기 위해서 전자서명을 하는 경우를 예로 든 것이다. A는 지



(그림 3) 공기키 기법을 이용한 전자서명 예



R : 임의의 난수
$E_0(b)$: b를 a의 공개키로 암호화
(P_i,i) : mix서버 i의 공개키와 비밀키 쌍

$A1 \rightarrow MIX1 : E_{p1}(R_1, Adr_2, E_{p2}(R_2, Adr_3, E_{p3}(R_3, Adr_{B1}, E_{B1}(Msg))))$
$MLX1 \rightarrow MLX2 : E_{p2}(R_2, Adr_3, E_{p3}(R_3, Adr_{B1}, E_{B1}(Msg)))$
$MLX2 \rightarrow MLX3 : E_{p3},(R_3, Adr_{B1}, E_{B1}(Msg))$
$MLX3 \rightarrow B1 : E_{B1}(Msg))$

(그림 4) Mix-net의 기본 개념

불에 대한 약속 메시지를 자신의 개인키로 서명한다. 이렇게 생성된 전자 서명은 오직 A의 공개키로만 복호화가 가능하다. 다시 말해, A의 공개키로 복호화된 지불 약속 메시지는 오직 A가 서명했다는 것이 확실하기 때문에 전자서명으로 사용이 가능하다. 비대칭키 기법은 안전하다고 알려져 있으며 활용도 측면에서도 대칭키 기법보다 우수하다. 그러나 비대칭키 기법은 계산량이 매우 크다는 단점이 있다.

지금까지 익명통신을 위해서 사용되는 암호/복호화 기법에 대해서 살펴보았다. 물론 익명성 보장을 위해서 암호/복호화 기법만이 사용되는 것은 아니다. 본 장의 나머지 부분에서는 암호/복호화를 이용하는 익명통신 기법과 이외의 다른 기법들에 대해서 소개한다.

2. Chaum의 Mix-net

익명통신에 대한 연구는 D. Chaum에 의해서 제안된 Mix-net[1]으로부터 시작되었다. Chaum이 제안한 Mix-net은 송신자가 메시지를 전송하기 위해서 구성된 모든 Mix들의 공개 키들이 필요하고, 송신자의 계산량 또한 크게 되는 단점이 존재 한다. (그림 4)는 Mix-net의 기본 개념을 나타낸 그림이다. Mix-net에서는 각 메시지는 수신자 ID, mix 서버들의 ID, 데이터로 구성이 되며, 중간의 mix 서버들에 의해서 믹싱된다. 각 mix서버들은 최초 발신인에 의해 보내진 메시지를 복호화 하여 이를 다시 믹싱 하여 다음 mix서버에게 전달한다. 이해를 돕기 위하여, (그림 4)와 같이 3개의 mix서버가 있는 상황에서 익명 통신의 예를 들어 설명한다.

[A1→MIX1] 발신자 A1은 3개의 난수 R1, R2, R3를 생성하여, (그림 4)와 같이 암호문을 만들어 MIX1에게 전달한다. 이 암호문은 오직 MIX1만이 열어 볼 수 있도록 MIX1의 공개키로 암호화 된다.

[MIX1→MIX2] MIX1은 수신한 암호문을 복호화 하여, 다음에 보내야 할 MIX서버의 주소, 즉 MIX2의 주소인 Adr2 의 주소를 얻게 되고 그 주소로 나머지 암호화 된 부분을 전달한다.

[MIX2→MIX3] 이 과정도 앞서 MIX1→MIX2의 과정과 같은 동작을 반복 수행한다.

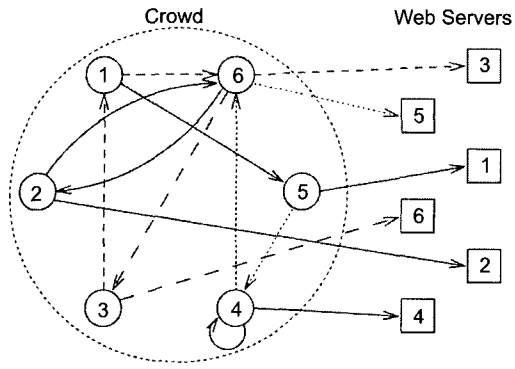
[MIX3→B1] 마지막으로, MIX3은 B1의 공개키로 암호화 된 $E_{B1}(Msg)$를 수신자인 B1에게 전달하고, B1은 자신의 개인키로 복호화 하여 메시지를 얻는다.

Chaum의 Mix-net 제안 이후에, 발신자부터 중간 노드들을 거쳐 수신자까지 가는 경로에 있는 노드들의 공개키를 사용하여 익명성을 보장하는 방식인 Mix-net 기반의 많은 익명통신 관련 연구들이 이루어 졌다. 그러나 Mix-net은 몇 가지 문제점들이 존재한다.

첫째, 발신자부터 수신자까지의 메시지 전송 경로가 손상되기 쉽고 경로관리가 어렵다. 경로 중간의 한 노드라도 손상이 된다면 전체 경로를 재설정해야 하기 때문에 유지비용이 많이 발생한다. 또한 비대칭키 기법에 기반 하기 때문에 계산량이 매우 많아서 모든 메시지에 대해서 적용하기가 힘들다. 이러한 단점들 때문에 다른 방법의 익명성 보장도 제안이 되었다.

3. Crowd

Crowd는 WWW(World Wide Web)에서의 발신자 익명성

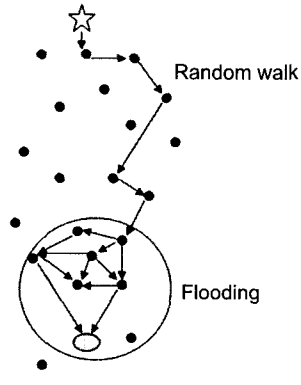


(그림 5) Crowd의 예

을 제공하기 위해 미국의 AT&T 연구원들이 제안하였다. 이 시스템은 웹서버에 접속하고자하는 사용자의 익명성을 보장한다. (그림 6)은 Crowd의 예를 나타낸 그림이다. 사용자들은 그림과 같이 Crowd를 형성한다. Crowd의 각 구성원들은 전달받은 메시지를 웹서버에 보낼 수도 있고, 다시 다른 구성원에게 전달 할 수 도 있는데 이에 대한 결정은 모두 랜덤하게 이루어진다. 이때 메시지를 전달한 구성원은 전달받은 구성원에게 이 메시지가 자신이 보낸 것인지, 아니면 그냥 전달만 하는 것인지를 알려주지 않는다. 이런 방법으로 웹서버의 접속에서의 익명성을 보장한다.

4. Phantom routing

Mix-net과 Crowd가 유선 네트워크에서의 익명성 보장 기법이었다면, Phantom routing은 무선 네트워크에서의 익명통신 기법이다.



(그림 6) Phantom routing의 개념도

최근 유비쿼터스 시대의 도래에 대한 기대감과 무선 통신이 급속도로 발전으로 무선 네트워크가 점점 비중이 높아져 가고 있다. 따라서, 예전에 유선 네트워크에서 발생했던 문제들이 무선 네트워크에서도 똑같이 문제가 된다. 더욱이 무선 네트워크는 모든 메시지 전송이 브로드캐스팅 되기 때문에, 즉 메시지가 공기 중으로 전파되기 때문에, 수신자 이외의 다른 노드도 메시지를 쉽게 엿들을 수 있어 보안상 취약성이 더 크다. 이런 문제 때문에 센서 네트워크에서의 발신자 익명성 보장을 위해서 phantom routing이 제안되었다.

phantom routing은 2 단계로 나뉜다. 1단계에서 메시지는 일정 홉(hop)동안 무작위 경로를 통해서 전달된다. 2단계로 일정 홉 이후부터는 정해진 규칙, 즉 무조건 전달(flooding) 혹은 단일경로 (single-path)로 전달된다. 그러나 경로가 길어지기 때문에 많은 시간지연이 발생할 수 있는 단점이 있다.

IV. 무선 네트워크에서 데이터 연결 계층 (data link layer) 익명통신

지금까지 대부분의 익명통신은 발신자와 수신자간의 다중 홉 (multi-hop)상황을 고려해왔다. 즉, 대부분의 연구에서 익명성을 위해서 필요했던 작업은 메시지 내의 라우팅 정보를 감춤으로서 악의적인 공격자가 발신자와 수신자 간의 연결을 알아내지 못 하게 하는 것에 목적이 있었다. 그러나 최근에 급속도로 보급되고 있는 WLAN이나 와이브로 (Wibro) 혹은 셀룰러 기반의 이동통신과 같이 무선 단일 홉 (single-hop)상황에서도 익명성 보장에 대한 필요성이 생겨나기 시작했다.

기존의 연구와의 차이점은 기존 연구가 네트워크 계층에서 익명성을 보장하는 기법을 제안해왔다면, 단일 홉 네트워크에서는 데이터 연결 계층 (data link layer)에서 익명성 문제를 접근해야 한다는 것이다. 다시 말하면, 네트워크 계층에서의 익명성 보장은 여러 홉을 거쳐서 메시지가 전달될 때, 그 메시지를 최초에 누가 보냈으며 최종적으로 누가 받느냐를 감추는 것이지, 전달되는 중간에 누가 보내고 누가 받는지를 숨기는 것은 크게 중요하지 않다는 말이다. 반

면에 단일 홉 상황에서 데이터 연결 계층의 익명성이라 함은 어떤 메시지를 누가 보냈고 누가 받았는지를 감춰야 하는 것이다. 즉 메시지 전송의 필수요소인 발신인 주소와 수신인 주소를 감춰야 하기 때문에 기존의 연구를 그대로 적용하기가 어렵다. 본 장에서는 기존의 익명통신 기법을 크게 3가지로 분류하고, 단일 홉 통신에서 익명성 보장이 어려운 이유를 설명한다.

1. pair-wise 대칭키 기법

pair-wise 대칭키 기법이란 발신자와 수신자가 똑같은 키를 가지고 주소를 암호/복호화하는 기법을 말한다. 한 노드가 N개의 노드와 통신을 한다면 모든 노드에 대해서 하나씩의 키를 가져야 하므로 총 N개의 키를 보유해야 한다.

A라는 노드가 B라는 노드에게 메시지를 보내는 과정을 생각해보자. A는 보낼 메시지에 발신자와 수신자를 적어서 보내야 하는데, 이때 발신자(A의 주소)와 수신자(B의 주소)를 이리 설정된 pair-wise 대칭키(A와 B가 공유하고 있는 대칭키)를 이용하여 암호화해서 보낸다. 이 암호화된 주소는 A와 B 이외에는 열어볼 수 없기 때문에 익명성을 보장된다고 할 수 있다. 그런데 문제는 전송이후에 수신할 때에 발생한다. 전송된 메시지를 받은 모든 노드는 이 메시지가 누구로부터 왔는지, 누구에게 가야 하는지 모르기 때문에 자신이 가진 모든 pair-wise 키를 이용하여 복호화 해 봐야한다. 예를 들어, 노드 C나 D같이 해당 수신자가 아닌 노드도 메시지의 수신자가 누구인지를 모르기 때문에 자신이 가진 키를 이용하여 복호화를 시도해봐야 한다. 또한 메시지의 수신자인 B도 역시 누구에게서 온 것이라는 것을 모르기 때문에 다른 노드와 마찬가지로 자신이 가진 모든 pair-wise 키를 이용하여 복호화 해봐야 한다. 이러한 복호화 오버헤드(overhead)가 가장 큰 문제가 된다.

2. network-wide 대칭키 기법

network-wide 대칭키 기법이란 발신자와 수신자의 주소를 암호/복호화 하기위해서 네트워크 내의 모든 노드가 하나의 전용키를 사용하는 기법이다.

모든 노드는 1개의 키만 있으면 되고, 암호화된 주소를 가진 메시지도 전용키를 이용하여 단 한 번의 복호화로 쉽게 알 수 있다. 그러나 1개의 단일키를 사용하기 때문에 하나의 노드라도 키를 노출시키게 되면 네트워크 전체가 위험해 질 수 있는 취약성을 가지며, 키를 가진 노드라면 모든 메시지의 발신인과 수신인을 확인 할 수 있기 때문에 완벽한 익명성을 보장한다고 할 수도 없다.

3. 비대칭키 기법

비대칭키 기법은 발신자가 수신자의 공개키를 이용하여 주소를 암호화하여 보내는 기법이다. 이 경우에 수신가 이외에는 주소를 복호화 해 낼 수 없기 때문에 익명성이 보장된다. 그러나, 주소가 암호화된 메시지를 받는 모든 노드는 pair-wise 대칭키 기법에서와 마찬가지로 누가 수신자인지를 모르기 때문에 모든 노드가 복호화를 시도해 봐야하는 문제점을 가진다. 뿐만 아니라, 비대칭키 기법은 많은 계산량을 요구하기 때문에, 상대적으로 하드웨어의 성능이 약한 무선 장치에 적용이 힘들고 암호/복호화 시간도 오래 걸리기 때문에 모든 메시지에 사용하는 것이 불가능하다.

결국, 데이터 연결 계층에서의 익명성을 보장하기 위해서는 기존의 연구를 적용할 때 발생하는 복호화 오버헤드를 효과적으로 해결 할 수 있거나, network-wide 대칭키에서 발생하는 보안상의 취약점을 해결할 수 있는 새로운 접근이 필요하다.

최근 한 논문[3]에서 이러한 데이터 연결 계층에서의 익명성을 보장 할 수 있는 기법을 제안하였다. 이 연구에서는 pair-wise 대칭키 기법을 사용하며, 복호화 오버헤드는 메시지를 주고받으면서 수신자와 발신자 간에 동기화(synchronization)를 맞춰서 해결한다.

그러나 채널 에러와 같은 문제로 메시지 전송이 실패하여 동기화가 어긋날 경우, 마찬가지로 복호화 오버헤드가 여전히 발생 할 수가 있다.

본 고에서는 익명통신의 개요와 기존의 관련 연구, 그리고 최근에 이슈가 되고 있는 데이터 연결 계층에서의 익명성 보장 기법에 대해서 살펴보았다. 지금까지 익명통신은 여러 보안 대책 중에서 없어도 상관없는, 그러나 있으면 좋은 정

도로 여겨져 왔다. 하지만 사회 전반에 걸쳐 정보통신망을 통한 개인정보의 수집이 쉬워지고 침해 가능성이 높아지기 때문에, 프라이버시 보호를 위한 익명통신은 더 이상 선택이 아닌 필수적인 기술이 되어야 한다.

참 고 문 헌

[1] D. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms," Communications of the ACM, vol. 24, no. 2, pages 84-88, Feb. 1981.

[2] Michael K. Reiter and Aviel D. Rubin, "Crowds: Anonymity for web transactions," ACM Transactions on Information and System Security (TISSEC), vol. 1, no. 1, pp. 66-92, 1998.

[3] Frederik Armknecht, Joao Girao, Alfredo Matos, and Rui L. Aguiar., "Who said that? privacy at link layer," In 26th Annual IEEE Conference on Computer Communications, Anchorage, Alaska, USA, May 2007. INFOCOM 2007. Minisymposium.

[4] R.L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Comm. of the ACM, vol. 21, no. 2, pp. 120-126, Feb. 1978.

[5] Azzedine Boukerche, Khalil El-Khatib, Li Xu and Larry Korba, "SDAR: A Secure Distributed Anonymous Routing Protocol for Wireless and Mobile Ad Hoc Networks," Proceedings of the 29th Annual IEEE International Conference on Local Computer Networks (LCN04)

[6] Wireless medium access control and physical layer specifications for lowrate wireless personal area networks. IEEE Standard, 802.15.4-2003, May 2003. ISBN 0-7381-3677-5.

[7] O. Berthold, H. Federrath, and M. Kohntopp, "Project Anonymity and Unobservability in the Internet," In Computers Freedom and Privacy Conference 2000 (CFP 2000), Workshop on Freedom and Privacy by Design, 2000.

[8] D. Kesdogan, J. Egner, and R. Buschkes, "Stop-and-go MIXes Providing Probabilistic Security in an Open System," Second International Workshop on Information Hiding, Lecture Notes in Computer Science 1525, pages 83.98, 1998.

[9] S. Basagni, K. Herrin, E. Rosti, and D. Bruschi. "Secure Pebblenets," In MobiHoc, pages 156.163, 2001.

약 력

박 민 호

2000년 고려대학교 전자공학(학사)
2002년 고려대학교 전자공학(석사)
2005년 서울대학교 전기공학부 박사과정
관심분야 : 무선 네트워크 센서 네트워크 보안

서 승 우

1987년 서울대학교 전기공학 (학사)
1989년 서울대학교 전기공학 (석사)
1993년 미국 펜실베니아 주립대학 전기공학 (박사)
1990년 ~ 1991년 서울대 기초전력연구소 연구원
1993년 ~ 1994년 미국 펜실베니아 주립대학 전산기공학과 조교수
1994년 ~ 1996년 미국 프린스톤대학 전기공학 poem 연구소
1996년 ~ 현재 서울대학교 전기 · 컴퓨터공학부 정교수
관심분야 : 유/무선 네트워크, 네트워크 보안 알고리즘, 무선망 라우팅 및 다중 접속 기술, 센서네트워크