소스 라우팅 기반의 이동 Ad-hoc 네트워크에서 안전한 데이터 전송 방법

준회원 노 효 선*, 종신회원 정 수 환**°

Secure Data Forwarding based on Source Routing in Mobile Ad Hoc Networks

Hyosun Roh* *Associate Member*, Souhwan Jung**° *Lifelong Member*

요 약

본 논문은 MANET 환경에서 소스 라우팅 기반의 안전한 데이터 전송 방법에 대해서 제안한다. 본 논문에서 제안하는 방법은 제 3의 신뢰할 수 있는 키 분배 서버로부터 두 개의 해쉬키 체인을 사용하여 생성된 키를 키 서버와 데이터 전달에 참여하는 노드 간에 미리 설정된 비밀키를 사용하여 안전하게 전달하고, 각 노드 간에 데이터 전송시 키 서버로부터 수신한 해쉬키를 사용하여 MAC 코드를 생성함으로써 각 중간 노드마다 데이터를 인증하는 방식이다. 제안된 방법은 인증서 기반의 PKI를 사용하는 방법보다 간단하며, 비밀키 방식의 경우 임의의 ad-hoc 노드 페어들 간에 비밀키를 미리 설정해야하는 부담을 감소시켰다.

Key Words : MANET MAC, Source routing, Hash-key chain, Hash

ABSTRACT

This paper proposes a secure data forwarding scheme on source routing-based ad-hoc networks. The scheme uses two hash-key chains generated from a trusted third party to generate Message Authentication Codes for data integrity. The selected MAC keys are delivered to the ad-hoc node using a pre-shared secret between the trusted third party and a node. The proposed scheme does not require the PKI, or the provisioning of the pre-shared secrets among the ad-hoc nodes.

Ⅰ. 서 론

MANET (Mobile Ad hoc Network)[1] 환경은 기존 무선 네트워크 환경에서의 AP (Access Point)나 BS (Base Station)와 같은 기반구조 없이 이동 단말들로만 구성된 임시적이며 자율적인 네트워크이다. 이런 Ad hoc 네트워크는 무선 매체를 사용하기 때문에 유선 네트워크 보다 더 많은 보안상의 위협이 존재한다. 특히 Ad hoc 네트워크는 멀티 홉 방식으로 데이터가 전달되기 때문에 악의적인 중간 노드에 의해 데이터의 무결성 및 기밀성 등의 문제가 발생한다. 위와 같은 문제를 해결하기 위해 기존의 AODV[2] (Ad hoc On-demand Distance Vector Routing)나 DSR[3] (The Dynamic Source Routing Protocol)을 이용하여 경로를 설정하는 과정에서 미리 중간 노드들을 인증하는 방법들이 제안되었다. 데이터가 전달되기 전에 미리

※ 본 연구는 숭실대학교 교내연구비 지원 및 21세기 프론티어 연구개발사업의 일환으로 추진되고 있는 정보통신부의 유비쿼터스컴퓨팅 및 네트워크원천기반기술개발사업의 지원에 의한 것임

* 숭실대학교 정보통신전자공학부 통신망보안 연구실 (peterhyo@cns.ssu.ac.kr, souhwanj@ssu.ac.kr)
** 숭실대학교 정보통신전자공학부 부교수 (souhwanj@ssu.ac.kr)(° : 교신저자)

논문번호 : KICS2007-06-279, 접수일자 : 2006년 6월 18일, 최종논문접수일자 : 2006년 11월 19일

안전한 경로를 설정하기 위해 제안된 방법들은 크게 비 대칭키 기반을 이용한 방법과 대칭키 기반을 이용한 방법으로 분류할 수 있다. 비 대칭키를 이용한 방법으로는 ARAN[4] (Authentication Routing for Ad hoc Networks)이 있고, 대칭키를 이용한 방법으로는 Ariadne[5], SRDP[6] (Securing Route Discovery in DSR) 등이 있다. 그리고 비 대칭키와 대칭키를 함께 적용한 SAODV[7] (Secure Ad hoc On-demand Distance Vector Routing)가 있다. 제안된 방법들은 경로설정을 위해 전송되는 RREQ (Route Request)와 RREP (Route Reply) 메시지가 변경되지 않도록 보호하고, 경로설정 과정에 포함되는 중간 노드를 인증하기 위해 개발되었다. 그러나 안전하게 경로가 설정되었다 하더라도 데이터가 전달되는 과정에서 악의적인 공격자가 설정된 경로에 끼어들 수 있으며, 전달되는 데이터를 도청하여 공격할 수 있다. 따라서 경로가 설정된 이후에 데이터를 안전하게 전달하기 위한 방법이 필요하고, 설정된 경로가 데이터가 전달되는 과정에서 임의로 변경되지 않도록 해야 한다. 공개키 기반의 경우 이동 노드에서 사용하기에는 오버헤더가 크고, 대칭키 기반의 경우에는 이동 노드의 키 분배 문제가 있다. 따라서 노드의 부담을 주지 않으며 간단하게 적용 가능한 방법이 필요하다.

이를 위해 본 논문에서 제안하는 방법은 키 분배 서버 T에서 미리 생성해 둔 두 개의 해쉬키 체인 (Double Hash-key Chain, DHC)의 임의의 위치에서 설정된 경로에 포함된 노드의 수만큼 해쉬키 체인[8]을 선택하여 사용한다. 선택된 해쉬키 체인은 각 노드와 키 분배 노드 T가 공유하고 있는 비밀 키로 암호화하여 분배한다. 따라서 악의적인 공격자에게 해쉬키 체인 쌍이 공개되지 않는다. 또한 해쉬키 체인을 이용하여 생성한 MAC을 데이터와 함께 전달하기 때문에 데이터를 변경할 수 없으며, 해쉬키 체인의 특성 때문에 설정된 경로를 수정하여 임의의 노드로 데이터를 전달하는 공격을 막을 수 있다.

본 논문은 다음과 같이 구성된다. 우선 제 Ⅱ장에서 관련된 기술들에 대해서 설명하고, 제 Ⅲ장에서 제안하는 방법의 키 분배 방법과 안전한 데이터 전달 방법에 대해서 설명한다. 제 Ⅳ장에서는 제안된 방법에 대한 안전성 분석과 효율성 비교를 하고, 끝으로 제 Ⅴ장에서 결론을 서술한다.

Ⅱ. 관련기술

이 장에서는 MANET 환경에서 안전한 경로 설정을 위한 라우팅 프로토콜들과 설정된 경로를 통해 데이터를 전달하는 과정에서 비정상적인 동작을 하는 노드를 분별할 수 있는 기술에 대해서 설명한다.

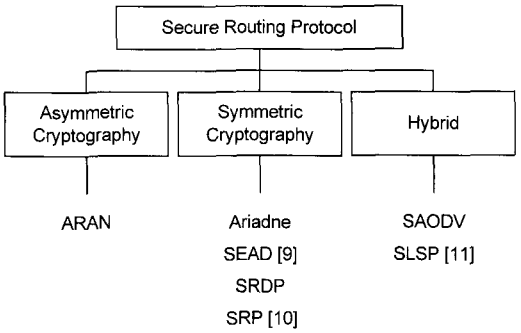


그림 1. 라우팅 프로토콜 분류

MANET 환경에서 안전한 라우팅 프로토콜은 그림 1에서처럼 비 대칭키 기반과 대칭키 기반으로 크게 나눌 수 있으며, 이 둘을 혼합하여 적용한 방법이 있다. 비 대칭키 기반을 이용하는 ARAN은 PKI (Public Key Infrastructure) 기반의 인증서를 사용한다. 신뢰할 수 있는 인증서 서버로부터 인증서를 전달받은 후 RREQ와 RREP 메시지를 자신의 개인키로 서명한다. 서명된 메시지는 인증서와 함께 이웃 노드로 전달되고 인증서를 통해 중간 노드들을 인증하며 경로를 설정한다. 이 방법의 경우 노드는 두 번의 인증서 확인과 두 번의 공개키 계산을 해야 하는 부담이 있다.

대칭키 기반의 Ariadne는 노드 인증과 안전한 경로 설정을 위해 TESLA (Timed Efficient Stream Loss-tolerant Authentication) 브로드 캐스트 인증 프로토콜[12]을 사용한다. TESLA 키를 이용하여 MAC (Message Authentication Code)을 계산한 후 경로 설정 메시지와 함께 전달한다. 이후 일정 시간 후 TESLA 키를 공개하여 MAC을 검증함으로서 노드를 인증한다. 또한 SRDP는 미리 모든 노드가 공유하는 Diffie-Hellman 값을 이용하여 노드를 인증한다. RREQ에 포함되어 전달되는 공개 값과 RREP를 통해 전달되는 서명 값을 소스에서 비교하여 각 노드를 인증한다.

비 대칭키 방법과 대칭키 방법을 혼합하여 사용하는 SAODV의 경우 전자서명과 해쉬 체인을 사용하여 노드를 인증한다. AODV에서 빈번하게 변하는 홉 카운트를 해쉬하여 다음 노드에서 메시지의 무결성을 검증하게 하였고, 전자 서명을 통해 각 노드를 인증한다.

위에서 설명한 방법들 이외에 데이터가 전달되는 과정에서 비정상적인 행동을 하는 노드들을 분별하여 데이터가 전달되는 경로에서 제외하는 방법들이 있다. 소스 라우팅 프로토콜 기반에서 적용할 수 있는 Watchdog[13]의 경우 데이터가 전달될 때 링크 계층에서 무차별모드 (Promiscuous Mode)로 동작하는 노드를 감시하는 방법이다. Watchdog을 이용하여 비정상적인 노드를 검출 한 후 노드의 평판도를 수정하여 주변 노드에게 알림으로서 평판도[14]가 낮은 노드를 데이터가 전달되는 경로에서 제외시키는 방법을 함께 사용한다.

Ⅲ. 해쉬키 체인을 이용한 안전한 데이터 전달

이 장에서는 소스라우팅에 의해 미리 설정된 경로가 공격자에 의해 변경되는 것을 예방하고, 설정된 경로를 통해 전달되는 데이터를 안전하게 보호하는 방법에 대해서 설명한다. 그리고 제안하는 방법을 적용하기 위해 Zone 기반의 MANET 환경[15]에서 존재하는 존 마스터와 같은 키 분배 서버 T가 존재하며 각 노드와 키 분배 서버 T간에 비밀 키를 공유하고 있다고 가정한다. 또한 소스 라우팅에 의해 경로가 설정되었다고 가정한다.

3.1 해쉬키 체인 생성 및 분배

키 분배 서버 T는 자신의 비밀 키 값인 MK_T와 임의의 수를 이용하여 미리 해쉬키 체인 K_{Di}와 K_{Sj}를 생성하여 보관한다. 식 (1)(2)와 같이 생성된 해쉬키 체인 K_{Di}는 데이터를 안전하게 전달하기 위해 사용하고, K_{Sj}는 ACK를 안전하게 전달하기 위해 사용한다.

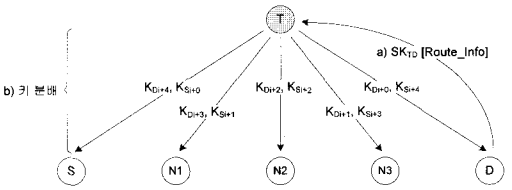


그림 2. 키 분배

$$K_{Di} : K_{D0}, K_{D1}, K_{D2}, K_{D3}, K_{D4}, \ldots, K_{Dn} \quad (1)$$

$$K_{Sj} : K_{S0}, K_{S1}, K_{S2}, K_{S3}, K_{s4}, \ldots, K_{Sn} \quad (2)$$

소스 라우팅 기반의 Ad hoc 네트워크 환경에서 목적지 노드는 RREQ 메시지를 통해 소스에서 설정한 경로를 알게 된다. 이때 그림 2에서처럼 목적지 노드는 자신이 알게 된 경로 정보를 키 분배 서버 T와 미리 공유하고 있는 비밀 키로 암호화 하여 키 분배 노드 T로 전달한다.

키 분배 노드 T가 $SK_{TD}[Route]$를 수신하면 그림 3의 (a)에서처럼 경로에 포함된 노드의 수만큼 해쉬키 선택 창을 조절한 후 미리 생성해둔 해쉬키 체인의 임의의 위치에서 해쉬키 체인을 선택한다. K_{Di}와 K_{Sj} 해쉬키 체인에서 노드의 수만큼 선택된 해쉬키 체인은 그림 3의 (b)에서처럼 각 노드의 비

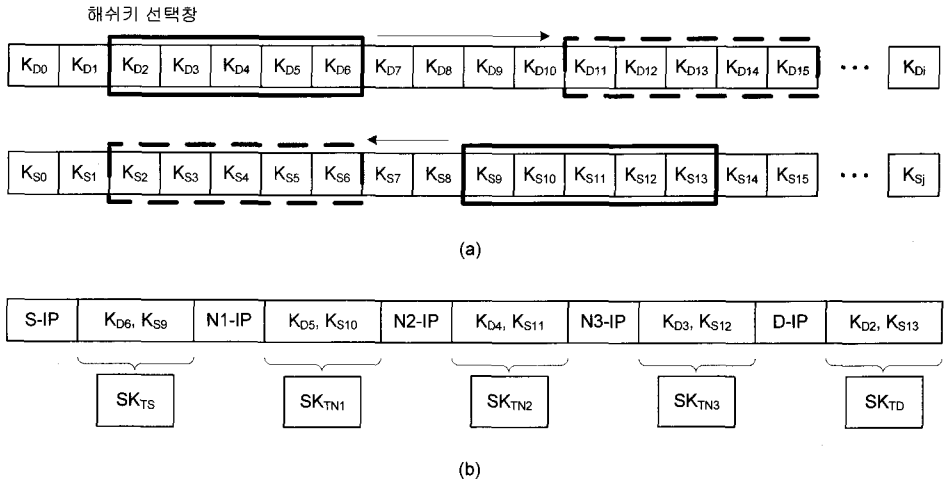


그림 3. 해쉬키 체인 쌍 선택 방법

표 1. T 노드로부터 전달받은 해쉬키 체인 쌍

Data 보호키	K_{Di}	K_{D6}	K_{D5}	K_{D4}	K_{D3}	K_{D2}
ACK 보호키	K_{Si}	K_{S9}	K_{S10}	K_{S11}	K_{S12}	K_{S13}
공유 비밀키	SK	SK_{TS}	SK_{TN1}	SK_{TN2}	SK_{TN3}	SK_{TD}
노드		소스	N1	N2	N3	목적지

밀 키로 암호화한 후 각 노드가 자신이 전달 받아야 하는 해쉬키 체인 쌍을 식별할 수 있도록 각 노드의 IP를 붙여 전달된다. 다음의 표 1은 각 노드에서 분배받은 해쉬키 체인 쌍이다.

3.2 안전한 데이터 전송 방법

소스는 해쉬키 쌍을 전달받은 후 그림 4와 같이 K_{D6}를 이용하여 MAC을 계산한 후 데이터에 붙여 N1 노드로 전달한다. 이후 중간의 노드들은 식 3에서처럼 MAC을 생성한 후 데이터와 함께 목적지로 전달한다. 그림 4는 생성된 MAC과 데이터가 전달되는 과정을 설명한다.

$$MAC_S = h(Data, K_{D6}) \quad (3)$$

$$MAC_{N1} = h(MAC_S, Data, K_{D5})$$

$$MAC_{N2} = h(MAC_{N1}, Data, K_{D4})$$

$$MAC_{N3} = h(MAC_{N2}, Data, K_{D3})$$

목적지 노드는 자신의 해쉬키 K_{D2}로 이전 노드의 해쉬키를 생성하여 전달받은 MAC_{N3}을 검증한다. 이렇게 하여 데이터의 무결성이 검증되면 목적지 노드는 ACK를 생성한 후 해쉬키 K_{S13}을 이용하여 MAC_D을 계산한 후 소스 쪽으로 전송한다. 전송되는 ACK는 데이터와 동일한 방법으로 MAC 체인 값과 함께 소스로 전달되고 목적지에서 MAC 값을 검증했던 방법으로 ACK를 검증한다. 소스가 ACK를 수신함으로서 데이터가 정상적으로 전달되었음을 알게 된다.

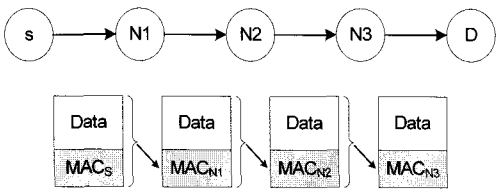


그림 4. 데이터 전달 과정

Ⅳ. 안전성 분석 및 효율성 비교

이 장에서는 본 논문에서 제안하는 두 개의 해시키 체인을 이용한 안전한 데이터 전송 방법에 대한 안전성 분석 및 효율성을 비교를 하였다.

4.1 안전성 분석

MANET 환경에서는 데이터 전달을 위한 경로 설정이 멀티 홉으로 구성되기 때문에 소스 라우팅에 의해 설정된 경로가 임의로 변경되거나 또는 전달되는 데이터가 수정되지 않도록 예방하는 것은 중요하다. 제안하는 방법에서 경로 변경이나 데이터 수정을 통한 공격(Modification Attack)[16]이 가능하려면 다음의 조건을 만족해야 한다. 첫째 소스 라우팅에 의해 설정된 경로에 끼어든 악의적인 공격자는 자신이 위조하여 생성한 MAC과 데이터가 정상적인 경로를 통해 전달되었다고 목적지 노드가 신뢰할 수 있도록 만들어야 한다. 둘째 공격자는 전달되는 데이터를 수정하기 위해서 이전 노드들이 사용한 해쉬키 체인 값을 알아야 한다. 이 두 가지 조건을 만족하지 못하면 설정된 경로의 변경이나 전달되는 데이터를 수정하는 공격은 실패한다. 본 논문에서 제안하는 방법의 경우 각 노드로 분배되는 해시키 체인 쌍은 각 노드의 비밀 키로 암호화되어 전달되므로 해시키 체인 쌍에 대한 비밀성이 보장된다. 또한 전달되는 MAC 값의 경우 수신한 노드가 자신의 해시키 체인을 이용하여 검증이 가능하기 때문에 MAC을 수정하였을 경우 쉽게 공격이 감지된다. 따라서 공격자가 정상적인 해시키 체인 쌍을 알지 못할 경우 경로를 변경하거나 데이터를 수정하는 공격은 불가능 하다.

변경을 통한 공격 이외에도 ad-hoc 네트워크 환경에서 가장 치명적인 서비스 거부 공격이 있다. 즉 소스와 목적지 노드 중간에 존재하는 노드들이 이동 단말의 자원을 절약하기 위해 고의적으로 데이터 패킷 전달을 거부하는 공격이다. 이런 공격의 경우 악의적인 공격자가 아닌 정상적으로 인증된 노드의 이기적인 행동으로 야기되는 공격이기 때문에 발견하기가 쉽지 않다. 때문에 이런 공격은 비정상적인 행동을 하는 노드를 검사하는 방법과 연계하여 처리해야 한다. 본 논문에서 제안하는 방법에서는 인증된 노드의 비정상적인 행동은 고려하지 않았다.

표 2. 효율성 비교 분석

항목	DHC	ARAN	Ariadne
키 분배	▸ 키 분배 서버	▸ 인증서 분배 서버	▸ 키 분배 서버
키 관리	▸ 비밀키 : 1개 ▸ 해쉬키 체인 : 1쌍	▸ 공개키 : 3개 ▸ 비밀키 : 1개	▸ 비밀키 : n(n+1)/2개, n:노드 수 ▸ 세션키 : 1개
오버헤드	▸ Data + MAC	▸ Data + 소스 인증서 + 중간 노드 인증서	▸ Data + 노드 리스트 + MAC(노드 수만큼)
데이터 전송 시 노드 연산	▸ 해쉬함수 계산 : 2번	▸ 인증서 확인 : 2번 ▸ 공개키 계산 : 2번	▸ 해쉬함수 계산 : 2번
효율성	▸ 연산 부담이 적음 ▸ 키 관리 부담 없음 ▸ 적용이 쉽고 간단 ▸ 키 분배 서버에 대한 의존도 큼 ▸ 소스 라우팅 기반에서 적용	▸ 부인방지 제공 ▸ 이동 노드의 연산 부담이 큼 ▸ 키 분배 불필요 ▸ 소스라우팅 방식과 on-demand 라우팅 방식에 적용가능	▸ 부인방지 제공 ▸ 모든 노드 간 시간 동기화 필요 ▸ 노드는 n(n+1)/2개의 키를 보관하고 있어야 함 ▸ 노드수가 증가하면 오버헤드 증가 ▸ 소스라우팅 기반에서 적용

4.2 효율성 분석

MANET 환경에서 안전한 경로 설정과 데이터를 전달하기 위해 다양한 방법들이 제안되었다. 제안된 방법들 중 앞서 설명했던 ARAN과 Ariadne 그리고 본 논문에서 제안하는 DHC에 대해 효율성 측면에서 비교하였고 표 2로 정리하였다. 제안된 DHC의 경우 다른 방법에 비해 비교적 노드의 연산부담이 적은 해쉬함수를 사용하여 데이터를 안전하게 전달할 수 있게 하였다. 그러나 키 분배 서버에서 미리 계산된 해시키 체인을 분배받아서 사용하기 때문에 다른 방법에 비해 키 분배 서버에 대한 의존도가 큰 단점이 있다.

V. 결 론

본 논문에서는 MANET 환경에서 소스 라우팅 기반의 안전한 데이터 전송 방법에 대해서 제안하였다. 제안된 방법은 키 분배 서버 T로부터 분배된 해쉬키 체인 쌍을 이용하여 데이터를 전달하기 때문에 이동 단말에서의 연산 부담이 공개키 기반 방식보다 훨씬 적다. 또한 사용되는 비밀 키는 키 분배 서버와 이동 노드 간에만 공유하고 데이터나 ACK를 전달할 때는 분배받은 해쉬키 쌍을 사용하기 때문에 대칭키에서 문제가 되는 키 분배 문제를 해결할 수 있다.

본 논문은 안전성 분석을 통해 데이터를 전달하는 과정에서 임의의 공격자로부터 설정된 경로를 변경하기위한 공격이나 전달되는 데이터를 수정하는 공격에 안전하다는 것을 보였고, 효율성 분석을 통해 공개키나 대칭키 방식에 비해 효율적임을 확인하였다. 따라서 제안하는 방법은 제한된 자원을 가진 ad-hoc 환경에서 통신하는 이동 노드들 간의 안전한 데이터 전송을 지원하는데 활용할 수 있다.

참 고 문 헌

[1] S. Corson and J. Macker, "Mobile Ad hoc Networking (MANET)," RFC2501, IETF, January 1999.

[2] C. Perkins, E. B. Royer, and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing," RFC3561, IETF, July 2003.

[3] D. Johnson, D. Maltz, and Y-C. Hu, "The dynamic source routing protocol for mobile ad hoc networks (DSR)," IETF Internet Draft, April 2003.

[4] K. Sanzgiri, D. LaFlamme, B. Dahill, B. Levine, C. Shields, and E. Royer, "Authenticated Routing for Ad Hoc Networks," IEEE Journal on Selected Areas in Communications, vol. 23, no. 3, March 2005.

[5] Y-C. Hu, A. Perrig, and D. B. Johnson,

"Ariadne: A Secure On-demand Routing Protocol for Ad Hoc Networks," 8th Annual Int'l. Conf. Mobile Comp. and Net. MobiCom 2002, September 2002.

[6] J. Kim, and G. Tsudik, "SRDP: securing route discovery in DSR," MobiQuitous 05, July 2005.

[7] M. Guerrero, "Secure Ad hoc On- Demand Distance Vector (SAODV) Routing," IETF Internet Draft, September 2006.

[8] P. Papadimitratos, and Z. J. Haas, "Secure Routing for Mobile Ad hoc Networks," Proc. Communication Networks and Distributed Systems Modeling and Simulation Conf, January 2002.

[9] Y.-C. Hu, D. Johnson, and A. Perrig, "SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks," Proc. Fourth IEEE Workshop on 20-21, June 2002.

[10] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," INFOCOM 2003 IEEE, vol.3, April 2003.

[11] P. Papadimitratos, and Z. J. Haas, "Secure link state routing for mobile ad hoc networks," Proc. Applications and the Internet Workshops, January 2003.

[12] A. Perrig, R. Canetti, D. Song, and J. D. Tygar, "Efficient and Secure Source Authentication for Multicast," In Network and Distributed System Security Symposium, NDSS'01, February 2001.

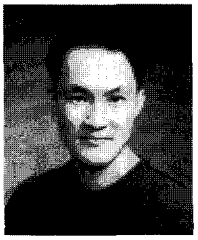
[13] S. Marti et al., "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," ACM Mobile Comp. and Net, MOBICOM, 2000.

[14] S. Buchegger, J.-Y. L. Boudec, "A Robust Reputation System for Mobile Ad-hoc Networks," EPFL IC, Tech. Rep, July 2003.

[15] N. Kang, I. Park, and Y. Kim, "Secure and Scalable Routing Protocol for Mobile Ad-hoc Networks," Proc. MATA 2005, October 2005.

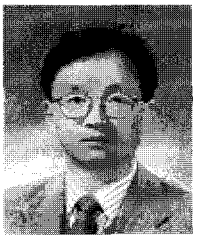
[16] K. Sanzgiri, "A Secure Routing Protocol for Ad Hoc Networks," 10th IEEE Int'l. Conf. Network Protocols (ICNP '02), November 2002.

노 효 선 (Hyosun Roh) 준회원



2005년 2월 숭실대학교 정보 통신 전자공학부(학사)
2007년 2월 숭실대학교 정보 통신 전자공학과 (석사)
2007년~현재 숭실대학교 전 자공학과(박사과정)
<관심분야> 이동 네트워크 보안, 네트워크 보안

정 수 환 (Souhwan Jung) 종신회원



1985년 2월 서울대학교 전자 공학과(학사)
1987년 2월 서울대학교 전자 공학과(석사)
1998년~1991년 한국통신 전임 연구원
1996년 6월 University of Washington (박사)
1996년~1997년 Stellar One SW Engineer
1997년~현재 숭실대학교 정보통신전자공학부 부교수
<관심분야> 이동인터넷 보안, 네트워크 보안, VoIP 보안, RFID/USN 보안