논문 12-37C-12-07

한국통신학회논문지 '12-12 Vol.37C No.12
http://dx.doi.org/10.7840/kics.2012.37C.12.1256

클러스터 기반 애드혹 네트워크 환경에서의 보안 라우팅 프로토콜

민 성 근◆, 박 요 한*, 박 영 호**, 문 상 재°

Secure Routing Protocol in Cluster-Based Ad Hoc Networks

Sung-geun Min◆, Yo-han Park*, Young-ho Park**, Sang-jae Moon°

요 약

이동 애드혹 네트워크는 고정된 기반 망의 도움 없이 이동 단말만으로 구성된 자율적이고 독립적인 네트워크이다. 최근 애드혹 네트워크의 보안성과 효율성을 높이는 방법으로 클러스터 기반 애드혹 네트워크가 대두되고 있다. 또한 이에 적합한 라우팅 프로토콜 역시 활발히 연구되고 있다. 하지만 클러스터 기반 ad-hoc 네트워크에서 보안을 고려한 라우팅 프로토콜에 대한 연구는 미흡한 실정이다. 본 논문에서는 클러스터 기반 애드혹 네트워크에서 공격에 안전한 보안 라우팅 프로토콜을 제안한다. 제안하는 보안 라우팅 프로토콜은 Diffie-Hellman 키 교환, HMAC, 디지털 서명 등을 사용하여 라우팅 메시지에 대한 무결성을 보장하여 안전한 경로 설정을 수행하였다.

Key Words : Ad hoc Network, Cluster Based, Secure Routing Protocol, Diffie-Hellman, HMAC, Digital Signature, Certification, 애드혹 네트워크, 클러스터 기반, 보안 라우팅 프로토콜, 디피-헬만, 해쉬맥, 디지털 서명, 증명서

ABSTRACT

Mobile ad hoc networks (MANETs) are infrastructure-less, autonomous, and stand-alone wireless networks with dynamic topologies. Recently, cluster-based ad hoc networks which enhance the security and efficiency of ad hoc networks are being actively researched. And routing protocols for cluster-based ad hoc networks are also studied. However, there are few studies about secure routing protocols in cluster-based ad hoc networks. In this paper, we propose secure routing protocol for cluster-based ad hoc networks. We use Diffie-Hellman key agreement, HMAC, and digital signature to support integrity of routing messages, and finally can perform secure routing.

Ⅰ. 서 론

애드혹 네트워크는 고정된 인프라가 없는 환경에서 노드들 스스로 네트워크를 구성하고 유지하는 무선 통신 네트워크다[1]. 초기에는 군사 목적으로 연구가 시작되었고 최근에는 재난 구조, 무선 회의 등과 같은 분야까지 연구가 확대되고 있다. 최근에는 애드혹 네트워크의 보안성과 효율성을 향상시키기 위해 클러스터 구조를 접목한 클러스터 기반 애드혹 네트워크에 대한 연구가 대두되어 활발히 연

※ 본 연구는 2012년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임. (2012R1A1A4A01002603)
※ 본 연구는 2012학년도 경북대학교 학술연구비에 의하여 연구되었음.
◆ 주저자 : 경북대학교 전자전기컴퓨터학부, goldberg7507@gmail.com, 준회원
° 교신저자 : 경북대학교 전자공학부, sjmoon@ee.knu.ac.kr, 종신회원
* 경북대학교 전자공학과, hanny12@ee.knu.ac.kr
** 경북대학교 산업전자공학과, parkyh@knu.ac.kr
논문번호 : KICS2012-08-406, 접수일자 : 2012년 8월 31일, 최종논문접수일자 : 2012년 11월 22일

구 중에 있다.

애드혹 네트워크에서 라우팅 프로토콜은 메시지를 전송하기 위한 경로를 설정하는 방법으로 기본적이면서도 중요한 연구 분야이다. 라우팅 프로토콜은 크게 테이블 기반 방식, 요구 기반 방식, 그리고 두 가지 방식의 장점을 혼합한 하이브리드 방식으로 나누어진다[2,3]. 테이블 기반 방식은 주기적인 통신을 통해 각 노드들이 최신 라우팅 정보를 가지기 때문에 통신이 필요할 때 라우팅 테이블의 정보를 이용하여 바로 경로를 설정하여 메시지를 전송할 수 있다[4]. 요구 기반 방식은 통신이 필요할 때만 경로 설정을 위한 통신을 수행하기 때문에 테이블 기반 방식에 비해 오버헤드가 적다[5,6]. 이 두 가지 방식을 혼합한 하이브리드 방식은 짧은 거리는 테이블 기반 방식을 사용하고, 먼 거리는 요구 기반 방식을 사용한다[7]. 클러스터 기반 애드혹 네트워크에서도 하이브리드 방식을 사용한 라우팅 프로토콜에 대한 연구가 수행 되었다[8].

최근에는 보안성을 강조한 라우팅 프로토콜들이 연구되고 있다[9,10]. 이것은 애드혹 네트워크가 고정된 인프라 시설이 없고 무선 통신이라는 특성 때문에 도청이나 메시지 수정 등과 같은 공격에 쉽게 노출될 수 있고 라우팅 프로토콜에 있어서도 다양한 공격이 제안되었기 때문이다[11-15]. Ariadne[16], ARAN(authenticated routing for ad hoc networks)[17], Endaira[18,19], SAODV(secure AODV)[20] 등이 대표적인 보안 라우팅 프로토콜로 알려져 있다. 클러스터 기반 애드혹 네트워크에서도 threshold cryptography를 사용한 보안 라우팅 프로토콜에 대한 연구가 수행되었다[21]. 하지만 클러스터 기반 애드혹 네트워크에서 보안을 고려한 라우팅 프로토콜에 대한 연구는 현재 미흡한 실정이다.

본 논문에서는 클러스터 기반 애드혹 네트워크를 위한 보안 라우팅 프로토콜을 제안한다. 제안하는 방법은 기존에 제안된 보안 라우팅 프로토콜인 ARAN과 Endaira 방식의 장점을 조합한 것으로 다양한 공격에 안전하다. 또한 메시지의 무결성을 보장하기 위한 방법으로 디지털 서명의 사용을 최소화하고, 대신 HMAC을 사용하여 효율성을 높였다. 따라서 클러스터 구조가 효율적인 규모가 큰 애드혹 네트워크 환경에서 안전하고 효과적으로 라우팅을 할 수 있다.

Ⅱ. 관련연구

2.1. 기존의 보안 라우팅 프로토콜

2.1.1. Ariadne 프로토콜[16]

Ariadne 프로토콜은 요구 기반 방식으로 통신이 필요할 때 마다 라우팅 프로토콜이 수행된다. 출발 노드와 목적지 노드는 비밀키를 사전에 분배하고 모든 노드는 TESLA (timed efficient stream loss tolerant authentication) 일 방향 키 체인을 가진다. 또한, 서로 다른 노드의 TESLA 일 방향 키 체인의 인증키를 안다고 가정한다. 출발 노드가 전송한 RREQ (route request) 메시지를 목적지 노드는 TESLA, MAC, 해쉬, 디지털 서명을 사용하여 인증한다. 이 방식은 대칭키 방식을 사용하므로 빠르게 경로를 설정할 수 있다. 하지만 중간 노드들이 인증을 수행하지 않고 메시지를 전달만 하기 때문에 중간에 경로 설정 메시지가 바뀔 경우 경로 설정이 안 되는 단점이 있다.

2.1.2. ARAN 프로토콜[17]

ARAN 프로토콜 역시 요구 기반 방식으로 모든 노드들은 네트워크에 참여하기 전에 증명서를 발급받는다. RREQ와 RREP (route reply) 메시지의 무결성을 위해 증명서와 디지털 서명을 이용한다. 공개키 방식을 사용하기 때문에 Ariadne에 비해 경로 설정 시간이 다소 오래 걸린다.

2.1.3. Endaira 프로토콜[18,19]

Endaira 프로토콜 또한 요구 기반 방식이지만 ARAN 프로토콜과는 다르게 RREP 메시지만 증명서와 디지털 서명을 이용하여 무결성을 제공한다. RREQ 메시지를 전송할 때는 메시지의 오버헤드를 줄이기 위해서 평문 그대로 전송한다. 하지만 메시지 자체만을 전송하므로 중간 경로에서 메시지의 수정이 가능하다는 단점이 있다.

2.1.4. SAODV 프로토콜[20]

SAODV 프로토콜은 요구 기반 방식으로 메시지의 무결성 제공을 위해 디지털 서명을 사용하고, 각 홉의 노드들을 인증하기 위하여 해쉬 체인을 사용한다. 각 노드는 RREQ 및 RREP 메시지를 주위 노드에게 전송할 때 마다 시퀀스 번호를 1씩 증가시킨 후 전달하게 된다. 하지만 홉-카운트 수정이 가능하기 때문에 공격에 취약하다.

2.2. 클러스터 기반 애드혹 네트워크

애드혹 네트워크의 규모가 커질 경우 라우팅을

위한 경로 설정 데이터들이 증가하게 되어 네트워크의 효율이 떨어지게 되고 경로 중간에 공격으로 인한 문제에 대해서도 노드들이 능동적으로 대처하기 쉽지 않다. 이런 한계점을 보완하기 위해서 클러스터 구조를 접목한 애드혹 네트워크가 대두되었다. 클러스터 기반 애드혹 네트워크는 물리적 접근성에 따라 노드들을 몇 개의 클러스터로 그룹화 하여 관리하는 방식으로 각 각의 클러스터는 하나의 클러스터 헤더와 다수의 노드들로 구성된다.

클러스터 기반 애드혹 네트워크는 상대적으로 능력이 뛰어난 클러스터 헤더가 전체적인 경로 설정에 관여하고 일반 노드들은 시작과 마지막 부분에만 관여하기 때문에 네트워크의 통신량이 줄어들게 된다. 또한 공격에 대한 방어나 경로 수정도 클러스터 위주로 할 수 있기 때문에 효과적으로 대처할 수 있다[22]. 결과적으로 기존의 애드혹 네트워크 보다 라우팅을 위한 메시지들의 관리가 쉽고, 메시지의 주고받는 양과 횟수를 줄일 수 있다. 그림 1은 클러스터 기반 애드혹 네트워크의 구조를 나타낸 것이다.

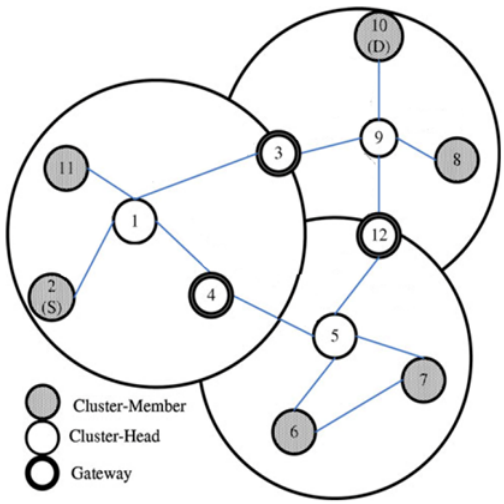


그림 1. 클러스터 기반 애드혹 네트워크의 구조
Fig. 1. Cluster-based ad hoc networks structure

Ⅲ. 제안하는 기법

논문에서는 클러스터 기반 애드혹 네트워크에서 안전한 보안 라우팅 프로토콜을 제안한다. 각 노드들은 신뢰할 수 있는 기관으로부터 증명서를 발급받았다고 가정한다. 발급 받은 증명서에는 해당 노드의 아이디, 해당 노드의 공개키, 증명서의 만료시간이 포함되어 있다. 표 1은 제안하는 라우팅 프로토콜에서 사용되는 기호들이다.

표 1. 사용하는 기호들
Table 1. Notations

Notation	Description
$Node_{id}$	node's identity
CH_{id}	cluster head's identity
$H_k[\ldots]$	hashed message authentication code
ti	time interval
<....>	digital signature
p	a large prime number
g	a generator of order p-1
x_{id}	node's private key
X_{id}	node's public key ($X_{id} = g^{x_{id}} \bmod p$)
y_{id}	cluster head's private key
Y_{id}	cluster head's public key ($Y_{id} = g^{y_{id}} \bmod p$)
RREQ	route request
RREP	route reply
k	session key

제안하는 기법은 요구 기반 방식으로 디지털 서명과 HMAC을 사용하여 라우팅 메시지의 무결성을 보장한다. 또한 매 홉마다 각 노드들의 인증을 수행하여 여러 공격에 대한 안전성을 보장한다. 다음 그림 2는 HMAC을 사용할 때 필요한 세션 키를 생성하는 과정이다.

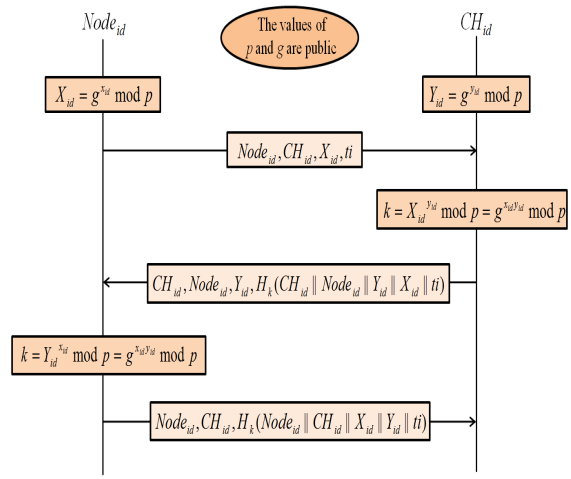
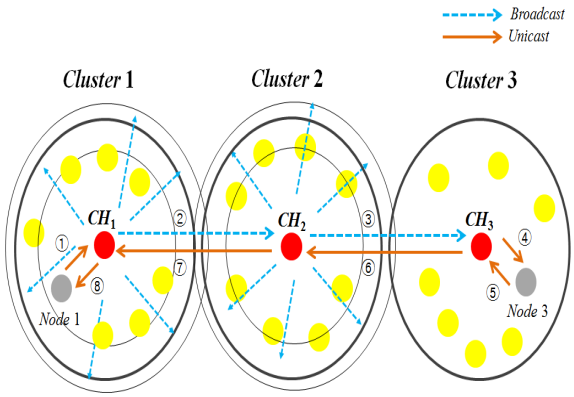


그림 2. 키 생성 과정
Fig. 2. Key generation process



① $Node_1 \rightarrow CH_1 = [RREQ, Node_1, Node_3, ti]$, $H_{k_1}[RREQ, Node_1, Node_3, ti]$

② $CH_1 \rightarrow * = [RREQ, Node_1, Node_3, ti, (CH_1)]$, $< RREQ, Node_1, Node_3, ti, (CH_1) >_{y_{CH_1}}$, $CERT_{CH_1}$

③ $CH_2 \rightarrow * = [RREQ, Node_1, Node_3, ti, (CH_1, CH_2)]$, $<< RREQ, Node_1, Node_3, ti, (CH_1) >_{y_{CH_1}}$, $(CH_2) >_{y_{CH_2}}, CERT_{CH_1}, CERT_{CH_2}$

④ $CH_3 \rightarrow Node_3 = [RREQ, Node_1, Node_3, ti, (CH_1, CH_2, CH_3)]$, $H_{k_3}[RREQ, Node_1, Node_3, ti, (CH_1, CH_2, CH_3)]$

⑤ $Node_3 \rightarrow CH_3 = [RREP, Node_3, Node_1, ti, (CH_1, CH_2, CH_3)]$, $H_{k_3}[RREP, Node_3, Node_1, ti, (CH_1, CH_2, CH_3)]$

⑥ $CH_3 \rightarrow CH_2 = [RREP, Node_3, Node_1, ti, (CH_1, CH_2, CH_3)]$, $H_{k_{2-3}}[RREP, Node_3, Node_1, ti, (CH_1, CH_2, CH_3)], CERT_{CH_3}$

⑦ $CH_2 \rightarrow CH_1 = [RREP, Node_3, Node_1, ti, (CH_1, CH_2, CH_3)]$, $H_{k_{1-2}}[RREP, Node_3, Node_1, ti, (CH_1, CH_2, CH_3)], CERT_{CH_2}$

⑧ $CH_1 \rightarrow Node_1 = [RREP, Node_3, Node_1, ti, (CH_1, CH_2, CH_3)]$, $H_{k_1}[RREP, Node_3, Node_1, ti, (CH_1, CH_2, CH_3)]$

그림 3. 클러스터 기반 애드혹 네트워크에서의 보안 라우팅 프로토콜
Fig. 3. Secure routing protocol in cluster based ad hoc networks

노드와 클러스터 헤더는 Diffie-Hellman 키 생성 방식을 사용하여 세션 키를 만든다. 먼저 키를 생성하고자 하는 노드는 <자신의 아이디, 클러스터 헤더의 아이디, 노드의 공개키, 시간간격상수> 메시지를 클러스터 헤더에게 전송한다. 클러스터 헤더는 노드의 공개키를 이용하여 세션 키를 생성하고 이 키를 사용하여 만든 HMAC 값과 다른 정보를 전송한다. 이 값을 받은 노드도 세션키를 생성하여 만든 HMAC 값과 다른 정보를 클러스터 헤더에게 전송한다.

그림 3은 제안하는 보안 라우팅 프로토콜에 대한 설명이다. 그림에서 출발 노드는 $Node_1$이고, 목적지 노드는 $Node_3$이다. 먼저 $Node_1$은 $Node_3$과의 경로 설정을 위해 <RREQ, $Node_1$, $Node_3$, ti> 메시지와 HMAC 값을 CH_1에게 보낸다. 이 값을 받은 CH_1은 $Node_1$과의 세션키를 사용하여 해쉬값을 확인하고, 이 값이 일치하면 받은 메시지의 자신의 아이디를 포함하여 서명값과 함께 브로드캐스트 한다. CH_2 역시 서명값을 확인한 다음 CH_1에서 받은 메시지에 자신의 아이디를 추가하여 브로드캐스트 한다. 다른 메시지들은 노드간의 세션 키를 사용하여 HMAC을 하는 반면 ②와 ③의 과정에서 디지털 서명을 사용하는 이유는 다양한 경로를 통해 하나의 최적의 경로가 설정되기 때문에 그 경로를 찾는 과정중 브로드캐스트를 하기 때문이다. 다른 메시지 전달 과정들은 주고받는 대상이 정해졌기 때문에 노드간의 세션키를 사용하여 HMAC을 사용할 수 있다. CH_3을 통해 RREQ 메시지를 받은 $Node_3$은 RREP 메시지를 HMAC을 사용하여 차례로 $Node_1$에 전달한다. 최종적으로 $Node_1$은 CH_1, CH_2, CH_3을 거쳐 $Node_3$와 경로를 설정한다.

Ⅳ. 안전성 및 연산량 분석

다음은 제안하는 보안 라우팅 프로토콜의 안전성 분석에 대한 내용이다. 또한 기존의 보안 라우팅 프로토콜 및 클러스터 기반에서의 라우팅 프로토콜과 비교 분석한다.

4.1. Blackhole 공격[11-13]

Blackhole 공격은 블랙홀 노드가 라우팅 정보를 변경하여 모든 노드들이 자신에게 패킷을 전송하게 하는 공격이다. ARIADNE, 제안하는 방법은 블랙홀 노드가 출발노드와의 세션 키를 모르기 때문에 (H)MAC값을 만들 수가 없다. 따라서 공격에 안전하다. ARAN, Endaira, SAODV 방법은 디지털 서

명을 사용하여 공격에 강인하게 설계되었다. 반면 CRP는 메시지를 전송할 때 아이디의 수정이 가능하기 때문에 이 공격에 취약하다.

4.2. Reply 공격[12]

Replay 공격은 유효한 메시지를 골라서 기록해두었다가 나중에 재전송함으로써 자신이 정당한 노드라고 가장하는 공격이다. 시간간격상수를 사용하여 사용한 메시지는 일정 시간이 지나면 폐기 한다. ARIADNE, ARAN, SAODV, CRP, 제안하는 방법은 시간간격상수 또는 랜덤수를 사용하기 때문에 이 공격에 안전하다. 반면 Endaira 방법은 이와 관련된 정보가 없기 때문에 Replay 공격에 취약하다.

4.3. Correctness of distance property 공격[14]

Correctness of distance property 공격은 악의적인 노드가 RREP 메시지를 전송할 때 의도적으로 홉-카운트를 증가시키지 않고 전송하는 공격이다. 악의적인 노드가 홉-카운트를 증가시키지 않으면 출발노드는 악의적인 노드가 목적지 노드인줄 알고 착각을 해서 악의적인 노드와 데이터 메시지를 주고받게 된다. SAODV, CRP 방법은 홉-카운트의 수정이 가능하여 이 공격에 취약하다. 제안하는 것과 그 외의 방법들은 인증 방식이 홉-카운트 기반이 아니기 때문에 이 공격에 안전하다.

4.4. Hidden channel 공격[15]

Hidden channel 공격은 출발 노드가 RREQ 메시지를 목적지 노드까지 전송할 때 악의적인 노드가 경로를 수정하는 공격이다. ARIADNE 방법은 RREQ는 MAC을 사용하고, ARAN, SAODV, 제안하는 방법은 디지털 서명을 사용하기 때문에 경로 수정이 어렵다. 따라서 이 공격에 안전하다. 반면 Endaira, CRP 방법은 RREQ 메시지의 수정이 가능하기 때문에 이 공격에 취약하다.

다음 표 2는 기존의 방식과 제안하는 방식과의 비교를 정리한 것이다.

표 2. 기존의 방식과 제안하는 방식의 보안성 비교
Table 2. Comparisons of security among the proposed scheme and existing schemes.

Protocol / Attack	ARIADNE [16]	ARAN [17]	Endaira [18,19]	SAODV [20]	CRP* [8]	Proposed Scheme*
Blackhole	○	○	○	○	×	○
Replay	○	○	×	○	○	○
Correctness of distance property	○	○	○	×	×	○
Hidden channel	○	○	×	○	×	○

(○ - secure, × - insecure, * - cluster based routing protocol)

다음 표 3은 제안하는 보안 라우팅 프로토콜의 연산량에 대한 분석이다. 4개의 노드를 기준으로 전체 라우팅 프로토콜에서의 연산량을 분석하였다. CRP는 보안성을 고려한 라우팅 프로토콜이 아니기 때문에 연산량 비교에 포함하지 않는다. 제안하는 보안 라우팅 프로토콜은 상대적으로 연산량이 많은 디지털 서명 대신 HMAC을 사용하여 연산량을 최소화 하였다. 기존의 보안 라우팅 프로토콜과 비교해 볼 때 효율적이라고 볼 수 있다.

표 3. 기존의 방식과 제안하는 방식의 연산량 비교
Table 3. Comparisons of efficiency among the proposed scheme and existing schemes.

Protocol	ARIADNE [16]	ARAN[17]	Endaira [18,19]	SAODV[20]	Proposed Scheme*
Computation (Four-hop)	$4\,T_H$	$6\,T_{sig}$	$3\,T_{sig}$	$2\,T_{sig}$	$1\,T_{sig}+5\,T_H$

(T_{sig} : Digital Signature, T_H : HMAC, *: cluster based routing protocol)

V. 결 론

규모가 큰 애드혹 네트워크에서 네트워크의 안전성과 효율성을 향상시키기 위해 클러스터 구조를 가진 애드혹 네트워크가 대두되고 있다. 공격에 강인한 보안 라우팅 프로토콜이 일반 애드혹 환경에서는 연구가 많이 되었지만 클러스터 기반 애드혹

네트워크 환경에서는 아직까지 미흡한 실정이다.

본 논문에서는 클러스터 기반 애드혹 네트워크에서 안전한 보안 라우팅 프로토콜을 제안하였다. 제안하는 기법은 디지털 서명과 HMAC을 사용하여 라우팅 메시지의 무결성을 보장하였다. 네트워크의 효율성을 위해 디지털 서명을 최소화 하였고 HMAC을 사용하여 연산량을 감소하였다. 제안하는 방법은 Blackhole 공격, Replay 공격, Correctness of distance property 공격, Hidden channel 공격 등에 안전하다. 제안하는 보안 라우팅 프로토콜은 대규모 군사 작전지역, 재난 지역 등과 같은 환경에 안전하면서도 효과적으로 적용될 수 있다.

References

[1] M. S. Corson and J. Macker, “Mobile ad hoc networking(MANET): routing protocol performance issues and evaluation considerations,” *RFC 250, Internet Engineering Task Force*, Jan. 1999.

[2] M. Abolhasan, T. Wysocki, and E. Dutkiewicz, “A review of routing protocols for mobile ad hoc networks,” *Ad Hoc Networks*, vol. 2, no. 1, pp. 1-22, Jan. 2004.

[3] M. J Kim and Y. I Eom, “Efficient route maintenance scheme for wireless ad-hoc network environments,” *J. The Korean Institute of communications and Information Sciences(KICS)*, vol. 30, no. 8A, pp. 639-648, Aug. 2005.

[4] C. E. Perkins and P. Bhagwat, “Highly Dynamic Destination Sequenced Distance Vector Routing (DSDV) for Mobile Computers,” *Newslett. ACM SIGCOMM Comput. Commun. Rev.*, vol. 24, no. 4, pp. 234-244, Oct. 1994.

[5] C. E. Perkins, “Ad hoc on demand distance vector (AODV) routing,” *IETF Internet Draft*, July 2003.

[6] C. E. Perkins, “Ad hoc on demand distance vector (AODV) routing,” in *Proc. IEEE Workshop on Mobile Computing Systems and Applications (WMCSA)*, pp. 90-100, LA, USA, Feb. 1999.

[7] Z. J. Hass and M. R. Pearlman, “The Zone Routing Protocol(ZRP) for Ad Hoc Networks,” *draft-Ietf-manet-zone-zrp-02.txt*, June 1999.

[8] M. Rezaee and M. Yaghmaee, “Cluster based Routing for Mobile Ad Hoc networks,” *J. comput. sci.*, vol. 8, no. 2, pp. 30-36, June 2009.

[9] S. Gupte and M. Singhal, “Secure routing in mobile wireless ad hoc networks,” *Ad Hoc Networks*, vol. 1, no. 1, pp. 151-174, Jan. 2003.

[10] Y. C. Hu and A. Perring, “A survey of secure wireless ad hoc routing,” *IEEE, Security & Privacy*, vol. 2, no. 3, pp. 28-39, June 2004.

[11] L. Tamilselvan and V. Sankaranarayanan, “Prevention of Blackhole Attack in MANET,” in *Proc. IEEE Int. Conf. Wireless Broadband and Ultra Wideband Commun.*, pp. 21-26, Sydney, NSW, Aug. 2007.

[12] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour “A survey of routing attacks in mobile ad hoc networks,” *IEEE Wireless Commun.*, vol. 14, no. 5, pp. 85-91, Oct. 2007.

[13] R. H. Khokhar, M. A. Ngadi, and S. Mandala “A review of current routing attacks in mobile ad hoc networks,” *Int. J. Comput. Sci. and Secur. (IJCSS)*, vol. 2, no. 3, pp. 18-29, June 2008.

[14] A. Burak and M. Ufuk, “A formal security analysis of secure AODV using model checking,” in *Proc. ISCN*, pp. 38-44, Istanbul, June 2008.

[15] B. Swetha and S. A. Kummar & TVS P. Gupta, “Flaws in Endair-A secure routing protocol for manets,” *Special Issue of Int. J. Comput. Sci. & Inform. (IJCSI)*, vol. 2, no. 1, pp. 127-132, Jan. 2012.

[16] Y. C. Hu, A. Perring, and D. B. Johnson, “Ariadne: A secure on-demand routing protocol for ad hoc networks,” *J. Wireless Networks*, vol. 11, no. 1-2, pp. 21-38, Jan. 2005.

[17] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, "A secure routing protocol for ad hoc networks," in *Proc. IEEE Int. Conf. Network Protocols*, pp. 78-87, CA, USA, Nov. 2002.

[18] D. Benetti, M. Merro, and L. Vigano', "Model checking ad hoc network routing protocols: ARAN vs. Endaira," in *Proc. IEEE Int. Conf. Software Engineering and Formal Methods (SEFM)*, pp. 191-202, Verona, Italy, Sep. 2010.

[19] A. F. A. Abidin, N. S. M. Usop, and N. H. N. Zulkifli, "An analysis on Endaira," *Int. J. Comput. Sci. and Eng.*, vol. 2, no. 3, pp. 437-442, Mar. 2010.

[20] M. G. Zapata and N. Asokan, "Securing ad hoc routing protocols," in *Proc. WISE*, pp. 1-10, NY, USA, Sep. 2002.

[21] R. Poosarla, H. Deng, A. Ojha, and D. P. Agrawal, "A cluster Based Secure Routing Scheme for Wireless Ad Hoc Networks," in *Proc. IEEE, Int. Conf. Perform., Comput., and Commun.*, pp. 171-175, OH, USA, April 2004.

[22] M. H. Guo, H. T. Liaw, D. J. Deng, and H. C. Chao, "Cluster-based secure communication mechanism in wireless ad hoc networks," *Institution of Engineering and Technology Information Security*, vol. 4, no. 4, pp. 352-360, Dec. 2010.

민 성 근 (Sung-geun Min)

2011년 2월 경북대학교 산업전자전기공학부 학사 졸업
2011년 3월~현재 경북대학교 전자전기컴퓨터 학부 석사과정
<관심분야> 정보보호, 네트워크보안

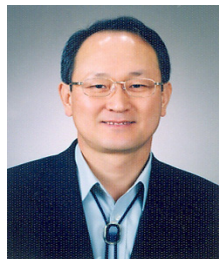
박 요 한 (Yo-han Park)

2006년 2월 경북대학교 전자전기컴퓨터 학부 학사 졸업
2008년 2월 경북대학교 전자공학과 석사 졸업
2008년 3월~현재 경북대학교 전자공학과 박사과정
<관심분야> 정보보호, 무선통신보안, 네트워크보안

박 영 호 (Young-ho Park)

1989년 2월 경북대학교 전자공학과 학사 졸업
1991년 2월 경북대학교 전자공학과 석사 졸업
1995년 8월 경북대학교 전자공학과 박사 졸업
1996년~2008년 상주대학교 전자전기공학부 교수
2003년~2004년 Oregon State Univ. 방문교수
2008년~현재 경북대학교 산업전자공학과 교수
<관심분야> 정보보호, 네트워크보안, 모바일 컴퓨팅

문 상 재 (Sang-jae Moon)



1972년 2월 서울대학교 공업교육(전자전공)과 학사 졸업
1974년 2월 서울대학교 전자공학과 석사 졸업
1984년 6월 미국 UCLA 전기공학과 박사 졸업
1984년 7월~1985년 6월 UCLA Postdoctor 근무
1984년 7월~1985년 6월 미국 OMNET 컨설턴트
1997년 9월~1998년 8월 경북대학교 전자전기공학부 학부장
1974년 12월~현재 경북대학교 IT대학 전자공학부 교수
2000년 8월~현재 경북대학교 이동네트워크 정보보호기술연구센터장
2002년 2월~현재 한국정보보호학회 명예회장
<관심분야> 정보보호, 디지털 통신, 이동 네트워크