Regular paper http://dx.doi.org/10.13067/JKIECS.2014.9.4.433

MANET 환경에서 S-EKE를 이용한 라우팅 보안 인증

이철승*

A Routing Security Authentication using S-EKE in MANET Environments

Cheol-Seung Lee*

요 약

독립된 네트워크의 구성 및 컨버전스 디바이스간 상호연결에 대한 요구로 MANET의 연구는 유비쿼터스 컴퓨팅 활용에 많은 주목과 고도의 성장을 보이고 있다. MANET에 참여하는 이동노드들은 호스트와 라우터 기능을 동시에 수행하여 네트워크 환경설정이 쉽고 빠른 대응력으로 임베디드 컴퓨팅에 적합하지만, 이동성으로 인한 동적 네트워크 토폴로지, 네트워크 확장성 결여 그리고 수동적 공격, 능동적 공격에 대한 취약성을 지니고 있어 지속적인 보안 인증 서비스를 관리할 수 없다. 본 논문은 MANET의 무선 보안의 취약성과 현재 활용되고 있는 OTP S/Key와 DH-EKE를 분석하여, MANET 기반 강인한 인증을 위해 S-EKE 인증기법을 제안한다.

ABSTRACT

The demanding in construction of the stand-alone networks and interconnection between convergence devices have led an increase in research on MANET and the application of MANET has been paid much attention as a Ubiquitous computing which is growing fast in the field of computer science. With performance both as hosts and routers, easy network configuration, and fast response, mobile nodes participating in MANET are suitable for Embedded computing but have vulnerable points, about lack of dynamic network topology due to mobility, network scalability, passive attacks, and active attacks which make it impossible to manage continuous security authentication service. In this study, proposes S-EKE authentication mechanism for a robust authentication based on MANET and through identify wireless environment security vulnerabilities, currently being used in OTP S/Key and DH-EKE analyzes.

키워드

MANET, MD5, EKE Authentication
모바일 애드혹 네트워크, 메시지 다이제스트 5, 키 교환 인증

Ⅰ. 서 론

MANET(: Mobile Ad-hoc Networks)은 이동노드들이 호스트와 라우터의 기능 수행으로 유비쿼터스 컴퓨팅 활용에 적합하지만, 불안전한 링크, 데이터 전송에러, 네트워크 확장성, 서비스 거부 등 수동적·능동적 공격에 많은 보안상 취약성을 지니고 있다[1-2].

본 논문은 MANET에서 발생하는 보안 인증의 취약성을 해결하기 위해 라우팅 프로토콜과 인증기법을 분석하고, 보안 5요소를 제공하는 신뢰성이 강한

* 교신저자(corresponding author) : 광주 여자대학교 교양・교직과정부(cyberec@kwu.ac.kr)
접수일자 : 2014. 01. 21 심사(수정)일자 : 2014. 03. 21 게재확정일자 : 2014. 04. 11

S-EKE(: Session Key-Encrypted Key Exchange) 인증기법을 제안한다.

II. MANET 보안환경 및 인증기법

2.1 MANET 보안환경

최근 MANET 라우팅 프로토콜은 이동노드의 이동성을 연결 요청시마다 즉시 반영할 수 있고, 제어 트래픽에 의한 오버헤드를 줄일 수 있는 On-demand 방식의 연구가 주류를 이루고 있다[3-4].

On-demand 방식의 AODV는 DSDV(: Destination Sequenced Distance Vector) 기반으로 유니· 멀티 캐스트를 모두 지원하며 목적지 노드의 순차번호를 이용하여 라우팅 루프를 방지하고, 불필요한 전송횟수를 줄일 수 있어 전체 네트워크 성능을 향상시킬 수 있다[5]. 하지만 이동노드간 멀티 홉을 통해 데이터를 전송해주는 역할을 하므로 다양한 위협과 공격에 노출되어 있다[6-7]. 또한 악의적인 노드와 타협된 이동노드들이 정상적으로 동작하는 것처럼 위장하여 네트워크의 라우팅 구조를 왜곡시킬 수 있어 이동노드간 보안의 취약성이 존재한다[8].

2.2 OTP S/Key 인증기법

MANET의 인증기법들은 CA의 존재 유·무에 따라 PKI기반과 OTP를 이용한 인증기법으로 나뉜다.

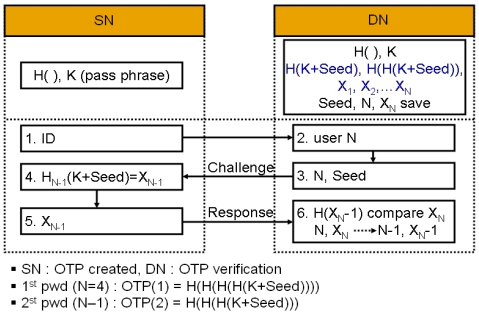

그림 1. OTP S/key 인증기법
Fig. 1 OTP S/key authentication technique

세션키를 사용하는 OTP S/key는 인증 시 발생할 수 있는 취약점 및 성능저하를 고려하여 연산과정이 단순하고, 이동성을 보장해 줄 수 있다. OTP는 MD5를 이용하여 항상 다른 해시코드를 생성하고, 추가계산을 한 후 목적지노드가 저장한 값과 일치여부에 따라 이동노드를 인증한다. OTP S/Key는 소스노드(SN)의 비밀키 K에 전적으로 의존하며, 전체 비밀정보는 H()로 암호화되어 저장된다. 또한 시간동기, 시도응답 인증기법에 비해 안전성, 실용성 그리고 간편성이 우수하지만, OTP를 이용한 인증기법들은 여전히 많은 문제점을 지니고 있다.

2.3 패스워드 기반 DH-EKE 프로토콜

DH(Diffie-Hellman)-EKE[9]는 세션키를 교환하는 방식으로 객체인증, 키 신규성, 키 확인, 키 동의가 이루어지며, EKE 프로토콜의 Denning-sacco 공격의 취약성을 개선하기 위해 네트워크 참여자가 각각 난수를 발생시켜 세션키를 생성하는 프로토콜이다.

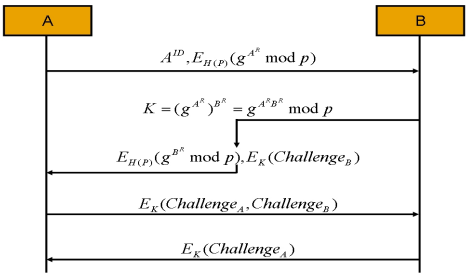

그림 2. DH-EKE 프로토콜
Fig. 2 DH-EKE protocol

그림 2와 같이 네트워크 참여자 A는 자신의 난수 A^R를 선택하고 큰 소수 p의 원시근 g에 A^R을 지수승하여 A^{ID}와 함께 B와 공유된 패스워드 $H(P)$를 이용하여 암호화한 후 B에게 전송한다. B는 수신된 메시지를 $H(P)$로 복호화하여 A^R을 구한 후 자신의 난수 B^R로 지수승하여 세션키 K를 생성한다. B는 자신의 공개키 g^{B^R}을 $H(P)$로 암호화 하고 검사값 $Challenge_B$를 K로 암호화하여 A에게 전송한다.

A는 수신된 메시지를 복호화하여 g^{B^R}을 생성한 후 A의 개인키 A^R을 지수승하여 $K = g^{B^R A^R}$를 생성하고 K를 이용하여 $Challenge_B$를 복호화 한다. A는 키 확인을 위해 자신의 검사값 $Challenge_A$와 $Challenge_B$를 K로 암호화하여 B에게 전송한다. B는 수신된 암호화된 메시지를 K로 복호화하여 B의 $Challenge_B$와 A로

부터 수신된 $Challenge_B$의 일치여부에 따라 동일한 세션키를 공유했음을 확인하고 A를 인증한다. 그리고 $Challenge_A$를 K로 암호화하여 A에게 전송하고, A는 수신된 $Challenge_A$의 일치여부를 확인한 후 B를 인증한다.

DH-EKE는 공개키와 K 사용으로 패스워드 추측공격, Denning-sacco 공격에 안전하지만, 패스워드 사전공격, Stolen-verifier 공격에 취약하며, 이를 MANET에 적용할 경우 라우팅 보안과 상호인증이 제공되는 신뢰성이 강한 세션키 교환 인증기법이 필요하다.

III. 세션키 교환 인증기법

본 논문은 MANET 라우팅 보안 인증을 위해 해시 라우팅과 OTP S/Key에 DH-EKE 적용으로 동적 네트워크 토폴로지에 즉시 대응할 수 있는 신뢰성이 강한 세션키 교환 인증기법이다. S-EKE는 안전한 통신경로 확보를 위한 라우팅 단계와 이동노드 인증을 위한 검증 및 키 교환 단계로 패스워드 암호화를 이용한 인증체계로 구성하였다.

이동노드들은 라우팅이 개시되기 전 OTP 생성을 위한 해시테이블을 생성하고 해시테이블로부터 공개키 요소들의 여러 세트를 유도한다. 각 이동노드들은 AODV에 OTP를 결합한 H(AODV)[10]를 통해 패스워드 검증자 $H^n(P)$로 암호화된 라우팅 메시지의 무결성을 확보한 안전한 경로설정을 한다. 이동노드들의 인증을 위한 검증 및 키 교환 단계에서는 MD5로 해시된 패스워드 검증자 $H^n(P)$를 등록하는 단계와 세션이 연결될 때 마다 이동노드들 사이의 세션키를 교환하는 공통적인 방식을 적용하였다.

3.1 안전한 통신경로 확보를 위한 라우팅

안전한 통신경로 확보를 위해 SN은 이웃한 노드를 통해 DN까지 경로탐색 메시지를 전송한다. 그림 3과 같이 SN은 전송하고자 하는 i번째 경로탐색 메시지를 서명하기 위해 $448 \bmod 512$를 적용하여 무결성이 보장된 $H(RREQ_i)$를 생성한다.

SN의 메시지의 각 비트를 서명하기 위해 하나의 비밀키 x와 하나의 공개키 y를 생성하여 서명할 메시지의 추가비트를 구성하기 위해 $\log_2 n$비트가 메시지에 추가된다. $H(RREQ_i)$에서 0의 비트수를 계산하여 $H(RREQ_i)$에 추가하고 n비트의 비트 스트링 g를 갖게 된다. j번째 비트 스트링 g_j가 1인 모든 j에 대하여 각 MN에서 생성된 해시테이블의 $(k-i)$번째 행에서 $h^{k-i}(x_j)$ 해시 값을 찾아 $H(RREQ_i)$에 추가하여 OTP를 생성하고 $H(RREQ)$를 NN들에게 전송한다.

$H(RREQ)$ 메시지를 수신한 NN은 전자서명 검증을 위해 MD5를 적용하여 $H(RREQ_i)$를 얻고 $\log_2 n$을 계산한 후 메시지의 비트열의 0의 개수를 계산하여 $H(RREQ_i)$에 추가한 후 n비트 스트링 g값을 생성한다. j번째 비트 스트링 $g_j=1$인 모든 j에 대하여 $h^{i-i'}(r_j)=v_j$ 인지 체크한다. r_j는 현재 전송된 $H(RREQ)$의 OTP이고, v_j는 $H(RREQi')$번째 OTP이다. $h^{i-i'}(r_j)=v_j$가 동일하면 라우팅 정보의 무결성이 보장 되었다는 것을 알 수 있으며, $H(RREQ)$를 검증한 MN은 다음 $H(RREQ)$ 탐색과 검증을 위해 v_j를 r_j값으로 갱신하여 SN에서부터 DN까지 포워딩 절차를 반복 수행한다.

SN으로부터 $H(RREQ)$를 수신한 DN은 응답 메시지인 $H(RREP)$를 생성하여 역 경로를 통해 전송한다. DN으로부터 DN의 i번째 $H(RREP_i)$를 받은 IN3는 다음 $H(RREP)$ 탐색과 검증을 위해 v_j를 r_j값으로 갱신하여 IN3부터 SN까지 포워딩 절차를 반복 수행하여 안전한 라우팅 경로를 할 수 있다.

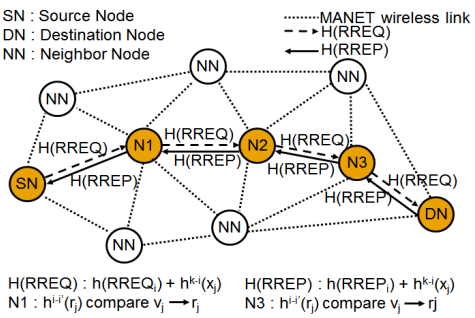

그림 3. H(AODV) 라우팅
Fig. 3 H(AODV) routing

3.2 인증을 위한 검증 및 키 교환

3.2.1 소스노드 등록 및 검증

등록단계에서 SN은 SN_id와 n번째 패스워드 검증자 $H^n(P)$를 DN에게 전송하고, DN은 수신된 SN_id와 $H^n(P)$를 패스워드 디렉토리 내에 저장한 후, SN과 DN사이에 인증을 위한 공개 패스워드 $H(g^s)$를 SN에게 송신한다. SN은 자신의 패스워드만 기억하고, DN은 SN의 $H^n(P)$만 기억하기 때문에 SN의 패스워드가 직접 노출되는 것을 막을 수 있다.

검증 단계에서는 SN과 DN의 등록과정 후 $H^n(P)$를 기반으로 SN이 패스워드를 증명하며 DN의 패스워드 디렉토리에 저장되어 있는 $H^n(P)$를 다음 세션의 검증자로 갱신한다. $H^n(P)$는 패스워드를 설정한 후 $i(i \le i < n)$번째 세션에서는 SN의 $H^{n-i+1}(P)$와 DN의 $H^{n-i}(P)$가 패스워드 검증자로 사용된다.

첫 세션에서 SN은 등록시킨 $H^n(P)$를 통해 DN과 세션을 공유하고 SN의 패스워드 소유를 증명하기 위해 $H^{n-1}(P)$를 암호화하여 전송한다. DN은 SN으로부터 수신된 $H^{n-1}(P)$에 한번 더 해시한 $H(H^{n-1}(P))$값과 DN의 패스워드 디렉토리 내에 저장되어 있는 $H^n(P)$의 일치 여부를 확인한 후 $H^{n-1}(P)$가 정당하게 생성되어졌으며 SN의 패스워드 값을 확인할 수 있다. DN은 $H^{n-1}(P)$를 디렉토리에 저장하고 $(n-1)$번째 통신까지 동일한 방법으로 검증하며 SN과 DN사이에 생성된 검증자를 통해 인증키 교환 단계를 수행한다.

3.2.2 인증키 교환 단계

인증키 교환 단계의 초기화 과정인 등록 단계와 검증 단계를 수행한 후 각 이동노드들의 해시테이블에 $H^n(P)$ 검증자를 저장하고, SN과 DN사이에 암호화를 수행하여 세션키를 생성한다.

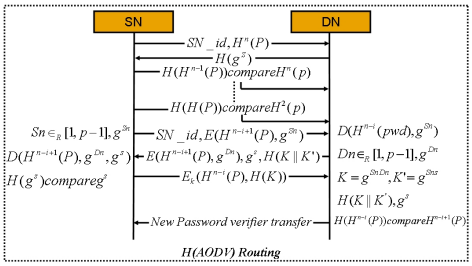

그림 4. S-EKE 인증절차
Fig. 4 S-EKE authentication process

SN과 DN사이의 i번째 세션과정은 그림 4와 같다. SN은 랜덤하게 생성된 $Sn \in_R [1, p-1]$과 세션키 생성을 위한 키값 g^{Sn}을 계산한 후, SN과 DN사이에 공유했던 $H^{n-i+1}(P)$로 g^{Sn}를 암호화하여 SN_id와 함께 DN에게 전송한다. DN은 SN_id, $E(H^{n-i+1}(P), g^{Sn})$를 수신한 후 패스워드 디렉토리에 저장된 SN의 $H^{n-1}(P)$를 이용하여 복호화한 후 g^{Sn}을 추출한다.

DN은 랜덤하게 생성된 $Dn \in_R [1, p-1]$을 선택하여 세션키 생성을 위한 키 값 g^{dn}를 계산하고, g^{Sn}에 g^{dn}의 지수승 하여 세션키 K와 장기 비밀키 s를 이용하여 다음 세션에 사용될 패스워드 검증자 K'를 계산한 후, SN과 DN이 공통으로 생성한 키의 값의 일치여부를 검증하는 검증 메시지 $H(K \| K')$를 생성한다.

키 검증 메시지 생성 후 DN의 장기 공개키 g^s와 g^{Dn}을 SN과 공유했던 $H^{n-i+1}(P)$를 이용하여 g^{Dn}을 암호화하고, $H(K \| K')$와 함께 SN으로 전송한다. SN은 DN으로부터 메시지를 수신한 후 $E(H^{n-i+1}(P), g^{Dn})$를 자신의 패스워드 검증자로 복호화하고, DN의 장기 공개키 g^s에 해시함수를 적용하여 자신의 공개 패스워드 $H(g^s)$값과 일치여부에 따라 세션을 유지한다.

S-EKE의 키 교환 과정에서는 DH-EKE의 어려움에 근거하여 장기 비밀키 s를 모르면 g^{Sn}과 g^{Dn}를 악의적인 노드가 획득 했을지라도 $K' = g^{Sns}$를 계산하지 못한다. 따라서 DN이 키 검증 메시지를 제대로 생성하여 보냈다면 DN의 장기 비밀키 s를 올바르게 알고 있음을 증명한다.

SN은 $Sn \in_R [1, p-1]$을 이용하여 g^{Sn}과 세션키 $K = g^{SnDn}$ 그리고 $K' = g^{Sns}$를 계산한 후 키 검증 메시지 $H(K \| K')$값을 확인하고 검증한다. 그리고 다음 세션을 위해 $H^{n-i}(P)$와 세션키 $K = g^{SnDn}$를 해시함수에 적용한 메시지 $H(K)$를 K'로 암호화하여 DN에게 전송한다. $K' = g^{Sns}$는 SN의 다음 세션 패스워드 검증자를 DN에게 전송하기 위하여 사용된 인증키이며 SN과 DN만이 생성할 수 있는 값이다. 그러므로 악의적인 노드는 K'를 생성하지 못하기 때문에 다음 세션에 SN의 패스워드 검증자를 암호화하여 전송할 때 K'를 사용한다.

DN은 SN으로부터 K'를 이용해 복호화하여 $H(K)$를 확인하고 SN과 세션키 K를 올바르게 공유했음을 확인한다. 또한 수신한 패스워드 검증자 $H^{n-i}(P)$에 해시함수를 한번 더 적용하여 $H(H^{n-i}(P))$값과 $H^{n-i+1}(P)$값이 같은 값인지를 비교하여 두 값이 일치한다면,

DN은 SN이 패스워드를 올바르게 알고 있다는 사실을 인증하게 된다. SN과 DN이 적법한 인증절차를 수행했다면, DN은 SN의 패스워드 검증자 $H^{n-i}(P)$로 교체하여 디렉토리에 저장한다.

Ⅳ. 인증기법 실험 및 결과분석

S-EKE의 실험은 0~900/sec 동안 Linux 기반의 NS3를 사용하여 측정하였다. CBR(: Constant Bit Rate) 세션을 처음 시작한 SN이 512byte/sec 4개의 패킷을 생성하여 DN까지 전송된 데이터 패킷을 계산량, 지연시간 그리고 random waypoint를 사용하여 목적지를 무작위로 선택하고, 0~20m/sec의 속도로 목적지에 도달한 후 5초 동안 머물다 또 다른 목적지로 이동하도록 설계 하였다.

제안기법의 초기 패스워드 검증자 생성을 위해 MD5의 수행횟수를 4회로 설정하였으며, SN과 DN 사이의 큰 소수 p, g(p의 원시근)를 생성하였다. g는 p의 거듭제곱을 했을 경우 $[1, p-1]$까지를 랜덤하게 생성되고, 세션이 바뀔 때 마다 $Sn \in_R [1, p-1]$ 랜덤하게 생성된다.

4.1 안전성과 효율성 분석

S-EKE의 라우팅 안전성은 H(AODV)를 이용하여 이동노드간 홉 카운터와 메시지 필드의 무결성을 제공한다. 또한 인증을 위한 안전성은 $Sn \in_R [1, p-1]$, $Dn \in_R [1, p-1]$, $H^n(P)$를 통해 새로운 세션키를 생성하여 재전송 공격에 안전하고, 중재자 공격은 세션키 K와 세션키 검증자 K' 사용으로 중재자 공격을 방지할 수 있다.

SN의 세션키 K 생성이 SN의 공개키를 사용하지 않는 DH-EKE를 모태로 하기 때문에 Denning-sacco 공격을 방어할 수 있으며, 오프라인 추측 공격은 $H^n(P)$로 암호화된 메시지는 임의의 난수들로 추정가능 문이나 기지평문이 아니기 때문에 사전 공격을 통한 올바른 패스워드를 알아낸다는 것은 불가능하다. 만약 SN의 패스워드가 노출된다 하더라도 세션키의 안전성은 DLP와 Diffie-Hellman을 기반하고 있어 PFS(: Perfect Forward Secrecy) 보안성을 제공하고 Stolen-verifier 공격의 안전성을 제공한다.

그림 5는 cbrgent.tcl을 통해 생성된 패킷 전달률이며, 0/sec의 경우 MN은 DN을 향해 이동하게 된다. OTP S/Key는 0~900/sec 동안 평균 97.16%의 패킷 전달률을 보이고 있으며, S-EKE는 96.91%로 AODV와 유사한 패킷 전달률을 보이고 있다. 하지만 S-EKE는 시뮬레이션 시작시간인 0/sec에서는 93.0% 경로를 탐색하기 위한 패킷 전달률은 떨어지지만, 500/sec 이후 패킷 전달률이 점차 증가되는 것을 볼 수 있다. 900/sec에는 99.8%로 데이터 패킷을 송·수신하기 위한 경로를 탐색하고 설정하는 것이 매우 효율적인 것을 증명해 준다.

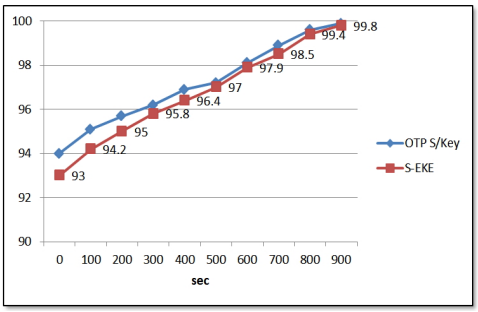

그림 5. 패킷 전달률
Fig. 5 Packet delivery rate

라우팅 오버헤드는 CBR 세션동안 소요되는 하나의 제어 패킷수를 말한다. 그림 10은 네트워크에 참여한 50개의 노드 중 30개의 노드를 연결하여 라우팅 오버헤드 측정값이다. S-EKE는 해시로 암호화된 2.31개의 라우팅 패킷을 가지고 있지만, 500/sec 이후에는 AODV 라우팅을 하는 OTP S/Key와 유사한 오버헤드를 보이고 있어 효율적이라 할 수 있다.

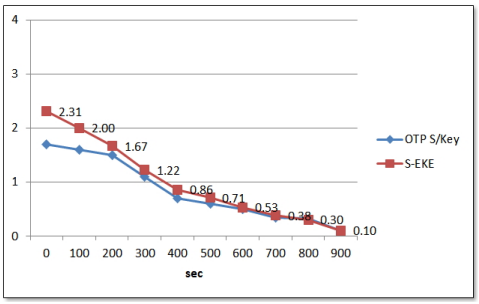

그림 6. 라우팅 오버헤드
Fig. 6 Routing overhead

Ⅴ. 결 론

MANET은 네트워크 인프라가 구축되지 않는 전시, 재난과 같은 환경에서 이동노드들이 라우터와 호스터 역할을 상호간에 수행하는 동적 네트워크 구조를 말한다. 하지만 동적 네트워크 구조로 인해 링크의 불안전성과 다양한 수동·능동적 공격에 노출이 되어 있어 많은 보안상 취약점이 존재한다.

본 논문에서는 MANET 환경의 보안 라우팅과 암호화된 세션키 교환을 통해 구조가 간단하고 안전성과 효율성을 증명하였다. MANET 성장성을 감안한다면 다양한 분야에서 MANET 융합기술이 전개되어 유비쿼터스 환경에서 각광을 받을 것이다. 하지만 이로 인해 보안성이 강조된 라우팅과 인증기술이 필요할 것이며, 향후 상용화 연구에 많은 노력을 기울여야 할 것이다.

참고 문헌

[1] B. Kadri, A. M'hamed, and M. Feham, "Secured Clustering Algorithm for Mobile Ad Hoc Networks," *Int. J. of Computer Science and Network Security IJCSNS*, vol. 7, no. 3, Mar. 2007, pp. 27-34.

[2] Y.-D. Kim, "Performance of VoIP Traffics over MANETs under DDoS Intrusions," *J. of The Korea Institute of Electronic Communication Sciences*, vol. 6, no. 4, 2011, pp. 493-498.

[3] X. Jia, J. Wu, and Y. He, "Mobile Ad-hoc and Sensor Networks," *Proc. Lecture Notes in Computer Science First International Conference MSN 2005*, vol. 3794, Springer, 2005, pp. 164-174.

[4] R. Zheng and R. Kravets, "On-demand power management for Ad Hoc networks," *Twenty-Second Annual Joint Conf. of the IEEE Computer and Communications Societies 2003 (INFOCOM 2003)*, vol. 1, Mar. 2003, pp. 481-491.

[5] K. Kim, S. Bae, and D. Kim, "An Enhanced Robust Routing Protocol in AODV over MANETs," *J. of The Korea Institute of Electronic Communication Sciences*, vol. 4, no. 1, 2009, pp. 13-18.

[6] C.-K. Toh, "*Ad Hoc Mobile Wireless Networks Protocols and System,*" Prentice Hall, Jan. 2004, pp. 200-252.

[7] Y.-D. Kim, "Transmission Performance of VoIP Traffics over MANETs under Multi Intrusions," *J. of The Korea Institute of Electronic Communication Sciences* vol. 7, no. 2, 2012, pp. 258-263.

[8] A. Patwardhan, J. Parker, A. Joshi, A. Karygiannis, and M. Iorga, "Secure Routing and Intrusion Detection in Ad Hoc Networks," *Third IEEE Int. Conf. on Pervasive Computing and Communications*, Mar. 2005.

[9] V. Boyko, P. MacKenzie, and S. Patel, "Provably secure password authenticated key exchange using Diffie_Hellman," *Advances in Cryptology-Eurocrypt 2000*, May 2000, pp. 14-18.

[10] C.-S. Lee, "A Study on MD5 Security Routing based on MANET," *J. of The Korea Institute of Electronic Communication Sciences,* vol. 7, no. 4, 2012, pp. 797-803.

저자 소개

이철승(Cheol-Seung Lee)

2001년 광주대학교 공과대학 컴퓨터학과 졸업(공학사)

2003년 조선대학교 대학원 컴퓨터공학과 졸업(공학석사)

2008년 조선대학교 대학원 컴퓨터공학과 졸업(공학박사)

2012년~광주여자대학교 교양·교직과정부 교수

※ 관심분야 : MANET Security, Android Security Wireless Network Security