MANET 기반 MD5 보안 라우팅에 관한 연구

이철승*

A Study on MD5 Security Routing based on MANET

Cheol-Seung Lee*

요 약

최근 독립된 네트워크의 구성 및 컨버전스 디바이스간 상호연결에 대한 요구로 MANET의 연구는 유비쿼터스 컴퓨팅 활용에 많은 주목과 고도의 성장을 보이고 있다. MANET에 참여하는 MN들은 호스트와 라우터 기능을 동시에 수행하여 네트워크 환경설정이 쉽고 빠른 대응력으로 임베디드 컴퓨팅에 적합하지만, 이동성으로 인한 동적 네트워크 토폴로지, 네트워크 확장성 결여 그리고 수동적·능동적 공격에 대한 취약성을 지니고 있어 지속적인 보안 서비스를 관리할 수 없다. 본 연구는 라우팅 단계에서 경로탐색 및 설정 시 악의적인 노드가 라우팅 메시지를 위·변조 하거나 적법한 MN으로 위장하는 공격을 방지하기 위해 AODV 라우팅 프로토콜에 MD5를 적용한 해시된 라우팅 프로토콜을 제안하여 안전성과 효율성을 개선하였다.

ABSTRACT

Recently demands in construction of the stand-alone networks and interconnection between convergence devices have led an increase in research on and much attention has been paid to the application of MANET as a Ubiquitous network which is growing fast. 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, such as lack of network scalability and dynamic network topology due to mobility, passive attacks, active attacks, which make continuous security service impossible. In this study, hashed AODV routing is used to protect from counterfeiting messages by malicious nodes in the course of path finding and setting, and disguising misrouted messages as different mobile nodes and inputting them into the network.

키워드

MANET, MD5, AODV

모바일 애드혹 네트워크, 메시지 다이제스트 알고리즘 5, 애드혹 주문형 거리벡터

Ⅰ. 서 론

MANET(Mobile Ad-hoc Networks)은 유비쿼터스 컴퓨팅 활용에 고도의 성장을 보이고 있다. 하지만 네트워크에 참여하는 MN(Mobile Node)들은 상호 신뢰한다는 가정 하에 연구가 되고 있으며, 라우팅 보안의 미비로 악의적인 노드의 공격 대상이 된다[1-2].

본 논문은 MANET의 라우팅 보안을 위해서 AODV(Ad-hoc On-demand Distance Vector) 라우팅 프로토콜에 MD5를 적용하여 안전성과 효율성이 증명된 보안 라우팅을 제안한다. 성능평가를 위해 NS2를 사용하였고, 해쉬된 AODV를 통해 악의적인 노드의

* 광주 여자대학교 교양·교직과정부(cyberec@kwu.ac.krl)

접수일자 : 2012. 06. 01 심사(수정)일자 : 2012. 07. 26 게재확정일자 : 2012. 08. 09.

위장, 도청에 대한 안전성을 확보하였고, 패킷 전달률과 라우팅 오버헤드를 측정하여 효율성을 증명하였다.

II. 본 론

2.1 AODV 라우팅 프로토콜

DSDV(Destination Sequenced Distance Vector) 기반의 AODV[3-4]는 유니 캐스트, 멀티 캐스트를 모두 지원하며 DN(Destination Node)의 순차번호를 이용하여 라우팅 루프를 방지하고, 불필요한 전송횟수를 줄일 수 있어 전체 네트워크 성능을 향상시킬 수 있다.

SN(Source Node)은 DN까지의 경로설정을 위한 메시지를 전송하고자 할 때, DN의 경로정보가 없다면 경로탐색을 실행하고 경로정보를 가지고 있다면 RREQ(Route Request) 메시지를 송신한다. RREQ를 수신한 NN(Neighbor Node)들은 순차번호와 RREQ를 보낼 때마다 증가하는 브로드캐스트 ID를 사용하며 주소 자동설정[5]을 통해 고유의 IP주소와 브로드캐스트 ID를 생성한다. RREQ를 받은 MN은 DN으로 RREQ를 전달하는 과정에서 자신의 라우팅 테이블에 첫 RREQ를 보내온 MN의 IP주소를 기록하므로 역방향 경로를 설정할 수 있고, DN은 NN을 통해 SN까지 RREP(Route Reply) 메시지를 유니캐스트 방식으로 응답할 수 있어 양방향 특성이 동일한 링크만을 지원한다. RREP를 수신한 MN들은 순방향 루트정보를 생성하여 저장하며 하나의 MN이 동일한 RREQ를 중복으로 수신한 경우 최초로 수신된 것만을 사용한다. 라우팅 경로내의 특정 링크에서 오류가 발생한 경우 MN들은 RERR(Route Error) 메시지를 SN으로 전송하여 루트 재탐색 절차[6]를 시작하게 되고, RERR을 수신한 MN들은 오류가 발생한 링크와 관련된 경로정보를 삭제한다.

2.2 MANET 위협과 공격유형

MANET은 MN간 불안전한 링크, 한정된 주파수, 전송거리와 에너지 제약성 그리고 MN의 증가로 인한 전파간섭으로 악의적인 노드에 대한 물리적 방어가 결핍되어 있다. 또한 데이터의 무결성 및 기밀성 문제, 보안기법의 제약성과 CA(Certificate Authority) 부재로 다양한 위협과 공격에 노출되어 있다[7-8].

MANET의 외부위협은 잘못된 라우팅 정보의 삽입, 이전의 라우팅 정보의 재생, 라우팅 정보를 변형하는 위협으로 분류한다. 외부위협을 통해 악의적인 노드는 네트워크를 분할하거나 극심한 트래픽을 유발하여 전체 네트워크 장애를 발생시킨다. 내부위협은 훼손된 MN에서 발생하여 NN들에게 잘못된 정보를 제공하고 네트워크 장애를 유발한다. 외부위협과 내부위협을 효과적으로 대처할 수 있는 방법은 충분한 MN을 확보하여 훼손된 MN 주변을 우회할 수 있는 경로를 확보하는 것이다.

그림 1과 같이 MAENT은 멀티 홉을 통해 NN들이 데이터를 전송해주는 역할을 하므로 수동적·능동적 공격 유형을 지니고 있다. 또한 악의적인 노드와 타협된 MN들이 정상적으로 동작하는 것처럼 보이나 네트워크의 라우팅 구조를 왜곡시킬 수 있어 MN간 보안상 취약성이 존재하며[9], 신뢰성 있는 MANET 보안 라우팅 기법들이 필요하다.

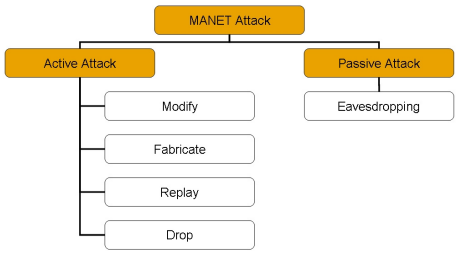

그림 1. MANET 공격유형
Fig. 1 MANET Attack Pattern

2.3 MD5 해시함수

MD5는 가변길이 입력으로부터 식 (2.1)을 이용한 512비트 블록의 최종 결과 값인 128비트 난수를 생성한다. OTP를 이용한 암호화된 패스워드 생성에 사용되며 inversion, collision, forgery와 같은 방어책이 있어야 한다. inversion는 주어진 해시 값으로부터 메시지를 알아내는 것이고, collision는 두개 이상의 서로 다른 메시지가 같은 해시 값을 갖는 것이다. 그리고 forgery는 비밀키에 대한 지식 없이 MAC(Message Authentication Code)을 산출하는 것이다. 그리고 IEEE 802.11의 무선 디바이스 인증 표준으로 사용되고 있으며 해시함수를 이용한 암호화된 패스워드 사용으로 신뢰성 있는 MANET 환경을 구성할 수 있다.

$$A \leftarrow B+((A+g(B,C,D)+X[k]+T[i])<<<s) \quad (2.1)$$

표 1. MD5 매개변수
Table 1. Parameters in MD5

매개변수	내 용
A, B, C, D	MD5 버퍼
g	해시함수 *F, G, H, I* 중의 하나
<<< s	s비트에 의한 32비트 매개변수의 순환 좌 쉬프트
X[k]	메시지의 512비트 블록 중에서 *k*번째 32 비트
T[i]	행렬 *T*에서 *i*번째 32비트
+	2^{23} 덧셈

III. 보안 라우팅

본 논문은 MANET의 보안 라우팅을 위해 AODV를 분석하고 경로설정을 위한 라우팅 보안과 동적 네트워크 토폴로지에 즉시 대응할 수 있는 신뢰성 있는 라우팅 기법을 제안한다. 라우팅 단계에서는 전자서명이 사용된 공개키 요소의 첫 세트를 반복적으로 MD5에 적용하여 해시테이블을 생성한 후, 해시테이블로부터 공개키 요소들의 여러 세트를 유도한다. 각 MN들은 제안된 보안 라우팅을 통해 기밀성과 무결성이 제공된 안전한 경로설정을 한다.

3.1 보안 라우팅 요구사항

MANET의 라우팅 프로토콜 연구는 MN을 신뢰한다는 가정 하에 수행되고 있지만, 각 MN들은 패킷 포워딩, 라우팅, 네트워크 관리기능을 수행하므로 부정행위를 할 수 있는 기회가 증가한다[10].

보안 라우팅을 위해 MN은 특정 DN의 라우팅 정보를 받을 경우 신뢰도순으로 순위를 매김 할 수 있어야 하며, 라우팅 경로설정이 정확하지 않을 경우 이를 삭제할 수 있어야 한다. 또한 정적 네트워크 토폴로지를 구성할 때에도 각 MN이 주기적으로 라우팅 메시지를 주고받기 때문에 높은 네트워크 오버헤드를 부담해야 하고, 악의적인 노드로부터 MN간 전송되는 라우팅 메시지의 각 필드의 위·변조와 스푸핑에 대한 위장 공격에 안전해야 한다.

그림 2와 같이 제안기법의 라우팅 단계에서는 AODV에 OTP를 결합한 *H(AODV)* 라우팅 프로토콜을 사용한다. OTP는 라우팅 메시지를 인증하고 악의적인 노드로부터 메시지의 위·변조에 대한 기밀성과 무결성을 제공하고, 각 MN들은 해시테이블 생성 후 해시체인을 통해 *H(RREQ)*와 *H(RREP)*를 통해 경로 설정을 한다. 메시지의 검증을 OTP 전자서명과 동일한 방법으로 수행하여 MN간에 홉 카운터 정보를 보호하였으며, 안전한 통신경로를 확보할 수 있었다.

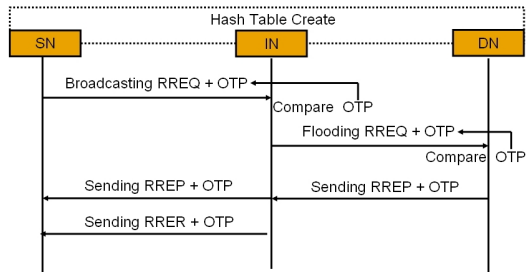

그림 2. 보안 라우팅 단계
Fig. 2 Step of security routing

3.2 해시 테이블 생성

그림 3과 같은 해시테이블은 하나의 비트열 x로부터 해시체인 $h^0(x)$, $h^i(x)$, ·, $h^n(x)$을 생성한다. i가 1부터 길이 n일때 $h^0(x)$은 x, $h^1(x)$은 $h^0(x)$에 한번 더 해시한 $h(h^0(x))$이고, $h^i(x)$는 $h(h^{i-1}(x))$이다. 그리고 각 MN들은 n비트인 k개의 메시지를 OTP를 이용하여 해시테이블을 생성한다. 각 MN들은 해시테이블을 생성하기 위해 j가 1부터 길이 n일 때 비밀키 요소인 x_j를 선택하고 n개의 비밀키 요소에 대해 길이가 k인 해시체인을 생성한다. SN은 공개키 기반 암호화 시스템을 사용하여 해시테이블의 k번째의 비밀키로 메시지를 서명하여 전송하고, 이웃한 MN들은 SN으로부터 전송된 $h^k(x_j)$값을 검증한 후 j가 1부터 길이 n인 v_j를 MN의 OTP 공개키 요소로 사용되며, $h^k(x_j)$는 라우팅 단계의 OTP로 사용된다.

0	$h^0(x_1)$	$h^0(x_2)$	$h^0(x_3)$	⋯	$h^0(x_j)$	⋯	$h^0(x_n)$
1	$h^1(x_1)$	$h^1(x_2)$	$h^1(x_3)$	⋯	$h^1(x_j)$	⋯	$h^1(x_n)$
2	$h^2(x_1)$	$h^2(x_2)$	$h^2(x_3)$	⋯	$h^2(x_j)$	⋯	$h^2(x_n)$
⋮	⋮	⋮	⋮	⋯	⋮	⋯	⋮
k-i	$h^{k-i}(x_1)$	$h^{k-i}(x_2)$	$h^{k-i}(x_3)$	⋯	$h^{k-i}(x_j)$	⋯	$h^{k-i}(x_n)$
k	$h^k(x_1)$	$h^k(x_2)$	$h^k(x_3)$	⋯	$h^k(x_j)$	⋯	$h^k(x_n)$

그림 3. MN들의 해시 테이블
Fig. 3 Hash table of MNs

3.3 경로탐색·설정 및 유지관리

안전한 경로설정을 위해 SN이 DN까지 라우팅을 하고자 할 때, SN은 IN(Intermediate Node)들로 부터 DN까지 경로탐색 메시지를 전송한다.

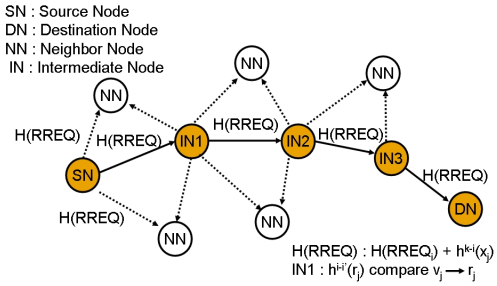

그림 4. 라우팅 경로탐색
Fig. 4 Routing path searching

그림 4와 같이 SN은 전송하고자 하는 i번째 경로탐색 메시지를 서명하기 위해 *448 mod 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 식 (3.1)과 같은 OTP를 생성하고 $H(RREQ)$를 NN들에게 전송한다.

$$H(RREQ) = H(RREQi) + h^{k-i}(x_j) \quad (3.1)$$

$H(RREQ)$ 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. $H(RREP)$는 Type을 2로 설정하고 프리픽스 사이즈, 해당 노드의 홉 카운트, DN의 IP주소, 순차번호, SN의 IP주소, 라이프 타임, 카운터 그리고 응답 메시지의 OTP를 포함한다.

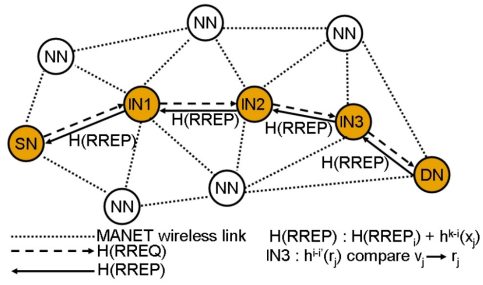

그림 5. 라우팅 경로설정
Fig. 5 Routing path setting

그림 5와 같이 DN의 i번째 $H(RREP_i)$를 받은 IN3는 $H(RREQ)$와 동일한 방법으로 OTP를 생성하고 전자서명 검증을 하게 되어 무결성이 보장된다.

$$H(RREP) = H(RREP_i) + h^{k-i}(x_j) \quad (3.2)$$

$H(RREP)$를 검증한 IN3는 다음 $H(RREP)$ 탐색과 검증을 위해 v_j를 r_j값으로 갱신하여 IN3부터 SN까지 포워딩 절차를 반복 수행한다. 이를 통해 악의적인 노드가 다른 MN으로 위장하여 거짓된 라우팅 정보를 유포하거나, $H(RREP)$에 대한 재생 공격을 막을 수 있어 안전한 라우팅 경로가 확보된다.

Type = 1 //H(RREQ)
Hop Count = 0
Broadcast ID += 1
Destination IP Address
Destination Sequence Number = Last Destination Sequence Number
Source IP Address
Source Sequence Number = Last Destination Sequence Number + 1
One Time Password

Type = 2 //H(RREP)
Hop Count = 1 //Destination Node
Hop Count = Destination Hop + 1 //Intermediate Node
Destination IP Address
Destination Sequence Number = last Destination Sequence Number + 1 //Destination Node
Destination Sequence Number = last Destination Sequence Number //Intermediate Node
Source IP Address
Lifetime = Routing Effective Time
One Time Password

그림. 6 *H(AODV)* 경로설정 과정
Fig. 6 *H(AODV)* path setting process

경로설정 이후 각 MN들은 라우팅 경로가 유효한지를 확인하기 위해 NN들에게 주기적으로 확인 메시지를 전송한다. MN들은 라이프타임 동안 경로상의 트래픽 발생이 없다면, MN의 라우팅 테이블에 경로가 활동하지 않는다고 체크한다. 그러나 유효하지 않는 경로로부터 데이터가 전달되거나, 경로상의 링크가 단절된 경우도 *H(RRER)*를 생성하여 전송한다. *H(RRER)*가 OTP로 서명되어 있기 때문에 악의적인 노드가 적법한 MN으로 위장하여 *H(RRER)*를 생성하는 공격을 막을 수 있다.

Ⅴ. 성능 평가

제안기법의 성능평가를 위하여 NS2를 사용하여 MANET 모델을 구성하였다. 첫 번째, IEEE 802.11 링크계층과 TDMA(Time Division Multiple Access)에 따라 MN에서 이용하는 CSMA(Carrier Sense Multiple Access), MAC 프로토콜 사용으로 MN의 트래픽 에이전트와 응용 서비스를 결정한다. 두 번째, 트래픽 에이전트는 전송계층에서 이용할 UDP(User Datagram Protocol)를 결정한다. 세 번째 응용계층 프로토콜에서 전송하는 응용 서비스를 지정하는 작업으로 CBR(Constant Bit Rate), FTP, HTTP, Telnet과 같은 구체적인 트래픽 타입을 지정해 준다. 마지막 네 번째 과정은 시뮬레이션 시간을 0~900(sec)로 설정하고, $n/\log_2 n$ 패킷에 대한 오버헤드를 측정하였다.

제안기법은 식(3.1), (3.2)를 사용하기 때문에 MN간 홉 카운터와 메시지 필드가 변조되지 않는다. 네트워크에 참여한 악의적인 노드에 의해 라우팅 메시지가 변조 된다면, IN에 의해 탐지가 되며, 전송된 메시지는 삭제가 되어 무결성을 제공한다. 라우팅 메시지는 네트워크 참여시 자신의 공개키를 다른 MN에게 전송한 MN만이 위조할 수 있어 위조된 메시지를 통한 공격유형을 식별하는 것은 어렵다. 하지만 제안 기법은 악의적인 노드가 서명한 공개키를 통해 위조된 라우팅 메시지를 보낸 MN을 알 수 있으므로 추후 라우팅 과정중 악의적인 노드를 제외시킬 수 있으며, 적법한 MN으로 위장하여 행동할 수 없다.

4.1 패킷전달률과 라우팅 오버헤드

패킷전달률 측정은 AODV와 제안기법을 비교하여 CBR 세션을 시작한 SN이 512byte/sec 4개의 패킷을 생성하고, DN까지 전송된 데이터 패킷을 계산량, 지연시간 그리고 random waypoint를 사용한 MN의 움직임 (0~20m/sec)에 따라 측정한 것이다.

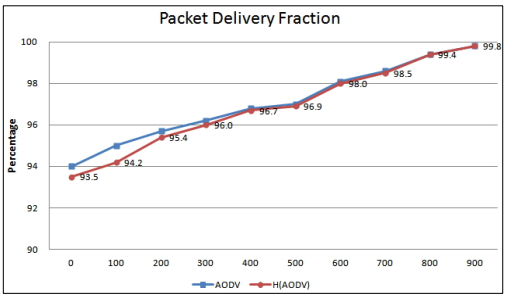

그림. 7 패킷전달률
Fig. 7 Packet delivery fraction

그림 7은 cbrgent.tcl를 통해 생성된 결과 값이다. 정지시간이 0인 경우 MN은 DN을 향해 이동하게 되고, AODV 라우팅 프로토콜에 추가적인 메시지 전송 과정 없이 OTP를 삽입한 *H(RREQ)*와 *H(RREP)* 메시지만을 전송한다.

AODV는 시뮬레이션 동안 94%이상의 패킷 전달률을 보였으며, 제안기법 또한 유사한 패킷 전달률을 보이고 있다. 하지만 시뮬레이션 시작시 93.5%로 AODV에 비해 경로를 탐색하기 위한 패킷 전달률은 떨어진다. 하지만 400초 이후 패킷 전달률이 점차 증가되는 것을 볼 수 있으며, 900초에서는 제안기법이 99.8%로 AODV와 0.1%정도의 오차를 보여 데이터 패킷을 송·수신하기 위한 경로를 탐색·설정하는 것이 효율적이고 정확하다는 것을 설명해 준다.

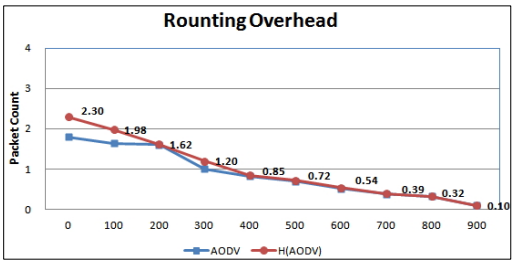

그림. 8 라우팅 오버헤드
Fig. 8 Routing overhead

라우팅 오버헤드는 하나의 데이터 패킷이 SN에서 DN까지 전송되는 CBR 세션동안 소요되는 제어 패킷 수이다. SN에서 DN까지 데이터를 전송하고자 할 때 사용되는 메시지는 에이전트 레벨, 라우팅 레벨, MAC 레벨에서 발생하며 에이전트 레벨의 메시지는 전송하고자 하는 CBR 데이터, 라우팅 레벨의 메시지는 CBR 데이터를 전송하기 위한 RTR_level 메시지, MAC 레벨의 메시지는 ARP와 같은 주소결정 프로토콜 메시지이며 네트워크에 참여한 50개의 노드 중 30개의 노드를 연결하여 라우팅 오버헤드를 측정하였다.

그림 8에서 AODV는 경로탐색을 위해 1.71개의 라우팅 패킷을 가지고 있고, 제안기법은 2.30개의 라우팅 패킷을 가지고 있으며, AODV 비해 더 큰 라우팅 패킷이 전송되고 있다. 하지만 500초 후에 AODV 라우팅과 유사한 오버헤드를 보이고 있어 효율적이라 할 수 있다.

Ⅵ. 결 론

MANET은 기존의 네트워크와 같이 인프라가 구축되지 않는 환경에서 MN들 상호간에 라우팅 수행으로 데이터를 송·수신 할 수 있는 형태의 네트워크를 말한다. 하지만 MN의 이동성으로 인한 동적 네트워크 토폴로지로 유선상의 네트워크보다 링크의 불안전성, MN의 물리적 보호의 한계, MN의 연결의 산재성 등 많은 보안상 취약점이 존재한다.

본 논문에서는 MANET 환경의 보안 라우팅을 위해 MD5를 적용한 OTP 사용으로 구조가 간단하고 안전성과 효율성을 증명하였다. MANET 성장성을 감안한다면 MANET의 보안 인식은 크게 증가될 것이며 보안 라우팅 기법은 가장 필요할 것이다. 유비쿼터스 환경과 MANET의 시장성을 고려한다면 더욱더 보안성이 강조된 라우팅 프로토콜과 보안기법의 개발과 상용화 연구가 필요할 것이다.

참고 문헌

[1] B. Kadri, A. M'hamed, M. Feham, "Secured Clustering Algorithm for Mobile Ad Hoc Networks", IJCSNS International Journal of Computer Science and Network Security, Vol. 7, No. 3, pp. 27, March, 2007.

[2] 김영동, "DDoS 침해가 있는 MANET에서 VoIP 트래픽의 성능", 한국전자통신학회논문지, 6권, 4호, pp. 493-494, 2011.

[3] M. S. Corson, J. P. Macker, "Mobile Ad hoc Networking(MANET) : Routing Protocol Performance Issues and Evaluation Considerations", RFC 2501, pp. 3-5, January, 1999.

[4] 김관웅, 배성환, 김대익, "MANETs의 AODV기반 향상된 견고한 라우팅 프로토콜", 한국전자통신학회논문지, 4권, 1호, pp. 14-15, 2009.

[5] K. Weniger, M. Zitterbart, "Address autoconfiguration in mobile ad hoc networks : current approaches and future directions, "IEEE Netw. Mag., Vol. 18, No. 4, pp. 6-11, Jul. 2000.

[6] Manel Guerrero Zapata, Manel Guerrero, "Secure Ad Hoc On-Demand Distance Vector (SAODV) Routing", IETF Internet Draft : draft-guerrero-manet-saodv-05.txt, pp. 12-13, February, 2005.

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

[8] 김영동, "다중침해가 있는 MANET에서 VoIP 트래픽의 전송성능", 한국전자통신학회논문지, 7권, 2호, pp. 258, 2012.

[9] A. Patwardhan, J. Parker, A. Joshi, A. Karygiannis, M. Iorga, "Secure Routing and Intrusion Detection in Ad Hoc Networks", Third IEEE International Conference on Pervasive Computing and Communications, pp.2-3, March, 2005.

[10] G. Montenegro, C. Castelluccia, "Statistically Unique and Cryptographically Verifiable

(SUCV) Identifiers and Address", NDSS' 02, pp. 1-2, February, 2002.

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