MANET 환경에서 MD5를 이용한 보안 라우팅에 관한 연구

이철승* · 정성옥** · 이준*

*조선대학교 전자·정보 공과대학 컴퓨터공학과

**광주여자대학교 의료정보학과

A Study on Security Routing using MD5 in MANET Environments

Cheol-seung Lee* · Sung-ok Jung** · Joon Lee*

*Dept. of Computer Engineering, Chosun University

**Dept. of Medical Information, Kwangju Woomen's University

E-mail : cyberec@chosun.ac.kr

요 약

최근 독립된 네트워크의 구성 및 다양한 컨버전스 디바이스간 상호연결에 대한 요구로 MANET의 연구는 IETF MANET WG, Bluetooth, HomeRF WG에서 활발하게 진행되고 있으며, 유비쿼터스 컴퓨팅 활용은 많은 주목과 고도의 성장을 보이고 있다.

MANET에 참여하는 MN들은 호스트와 라우터 기능을 동시에 수행하여 네트워크 환경설정이 쉽고 빠른 대응력으로 임베디드 컴퓨팅에 적합하지만 MN의 이동성으로 인한 동적 네트워크 토폴로지, 네트워크 확장성 결여 그리고 수동적·능동적 공격에 대한 취약성을 지니고 있어 지속적인 보안 서비스를 관리할 수 없다.

본 연구는 경로탐색 및 경로설정을 하는 라우팅 단계에서 악의적인 노드가 라우팅 메시지를 위·변조 하거나 적법한 MN으로 위장하는 공격을 방지하기 위해 AODV 라우팅 프로토콜에 MD5를 적용한 해시된 라우팅 프로토콜을 이용하여 안전성과 효율성을 향상 시켰다.

ABSTRACT

Recently demands in construction of the stand-alone networks and interconnection between convergence devices have led an increase in research on IETF MANET working group, Bluetooth, and HomeRF working group 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. For perfect MANET setting, routing is required which can guarantee security and efficiency through secure routing.

In routing in this study, hashed AODV 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, AODV, MD5

Ⅰ. 서 론

유비쿼터스 시대의 독립된 네트워크의 구성 및 다양한 컨버전스 디바이스간 상호연결에 대한 요구가 증가함에 따라 MANET(Mobile Ad-hoc Network)의 연구는 많은 주목과 고도의 성장을 보이고 있다.

MANET에 참여하는 MN(Mobile Node)들은 호스트와 라우터 기능을 동시에 수행하여 네트워크 환경설정이 쉽고 빠른 대응력으로 임베디드 컴퓨팅에 적합하지만 지속적인 라우팅 서비스와 MN

들을 상호 신뢰한다는 가정 하에 연구가 되고 있어 악의적인 노드의 공격 대상이 된다[1].

본 논문은 완전한 MANET 환경의 라우팅을 위해서 AODV(Ad-hoc On-demand Distance Vector) 라우팅 프로토콜에 MD(Message Digest)5를 적용하여 해시된 라우팅을 제공한다. 안전성과 효율성 측정을 위해 Linux 기반의 NS2를 사용하였고, 해시된 라우팅 프로토콜을 통해 악의적인 노드의 위장, 도청에 대한 라우팅 안전성과 패킷 전달률, 라우팅 오버헤드를 줄여 효율성을 향상시켜 안전한 MANEAT 환경의 라우팅 기법이라 할 수 있다.

II. 본 론

2.1 AODV 라우팅 프로토콜

AODV 라우팅 프로토콜[2]은 DSDV(Destination Sequenced Distance Vector) 라우팅 프로토콜 기반으로 유니 캐스트와 멀티 캐스트를 모두 지원하며 DN(Destination Node)의 순차번호를 이용하여 라우팅 루프를 방지한다.

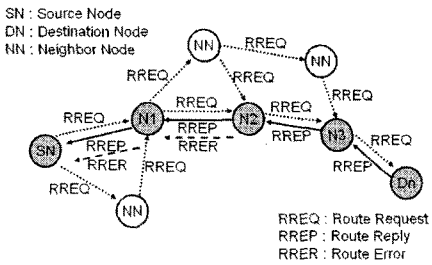

그림 1. AODV 라우팅 프로토콜

그림 1은 SN(Source Node)이 DN까지의 경로 설정을 위한 메시지를 전송하고자 할 때 SN이 DN의 경로정보를 가지고 있지 않다면, SN은 경로탐색 과정을 실행하게 되고, SN이 DN의 경로정보를 가지고 있다면 경로설정을 위한 메시지인 RREQ 메시지를 송신한다.

네트워크에 참여한 각 MN들은 순차번호와 RREQ를 보낼 때마다 증가하는 브로드캐스트 ID를 사용하며 주소 자동설정[3]을 통해 고유의 IP 주소와 브로드캐스트 ID를 생성한다. RREQ 패킷을 수신한 MN은 DN으로 RREQ를 전달하는 과정에서 자신의 라우팅 테이블에 첫 RREQ 메시지를 보내온 MN의 IP주소를 기록하므로 역방향 경로를 설정할 수 있다. RREQ 패킷이 DN에 도착하거나 N1, N2, N3노드들이 응답할 만큼 최근의 경로 정보를 가지고 있다면, DN은 이웃한 MN을 통해 SN까지 RREP 패킷을 유니캐스트 방식으로 응답하게 되므로, AODV 라우팅 프로토콜은 양방향 특성이 동일한 링크만을 지원한다. RREP 패킷을 수신한 MN들은 순방향 루트정보를 생성하여 저장하며 하나의 MN이 동일한 RREQ 메시지를 중복으로 수신한 경우 최초로 수신된 것만을 사용한다. 라우팅 경로내의 특정 링크에서 오류가 발생한 경우 MN들은 RERR 패킷을 SN으로 전송하여 루트 재탐색 절차를 시작하게 되고, RERR을 수신한 MN들은 오류가 발생한 링크와 관련된 경로정보를 삭제한다.

2.2 MANET 공격유형

MAENT은 SN과 DN사이에 단일 홉 데이터 전송도 가능하지만 멀티 홉을 통해 NN들이 데이터를 전송해주는 역할을 하므로 쉽게 악의적인 노드로부터 수동적 공격 및 능동적 공격을 받을 수 있다.

그림 2와 같이 수동적 공격은 악의적인 노드의 에너지를 절약하기 위한 목적으로 네트워크에서 수행해야할 협동 작업을 하지 않는 공격을 말한다. 능동적인 공격은 네트워크에 참여한 악의적인 노드가 패킷을 변조, 위조, 재생, 누락시켜 적법한 MN으로 위장하여 동일한 메시지를 수신하게 하거나 변조된 메시지를 전송하여 MN간의 메시지 흐름을 저하시키며 방해한다[4].

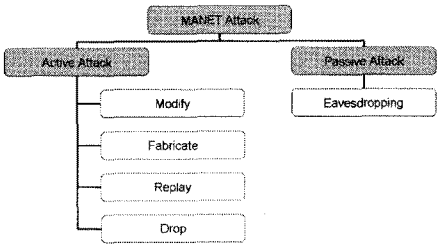

그림 2. MANET 공격유형

2.3 MD5 해시함수

MD5[5]는 빠른 속도의 소프트웨어 구현을 위해 가변길이의 입력으로부터 식 (2.1)을 이용하여 512비트 블록의 최종 결과 값인 128비트 메시지 다이제스트를 생성한다.

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

표 1. MD5 매개변수

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

MD5는 IEEE 802.11의 무선 디바이스 인증에

표준으로 사용되고 있으며 해시함수를 이용한 암호화된 패스워드인 OTP(One Time Password) 사용으로 안전한 MANET 환경을 구성할 수 있다.

OTP 생성을 위해 inversion, collision, forgery 등 견고한 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.

III. 보안 라우팅

MANET은 MN간에 패킷 데이터를 전송하는 동적 네트워크로 침입이나 오동작으로 인한 심각한 보안상 취약점을 지니고 있다. 네트워크 중간에 훼손된 MN이 발생되면 MN간 신뢰관계는 변하게 되고 신속하게 처리할 수 있는 MANET 보안 라우팅기법이 필요하다. 보안 라우팅을 위해 첫 세트를 반복적으로 MD5를 적용한 해시테이블을 생성하고 공개키 요소들의 여러 세트를 유도한다. 각 MN들은 해시된 라우팅 생성을 통해 기밀성과 무결성이 보장된 안전한 경로설정을 한다.

3.1 해시 테이블 생성

라우팅 보안을 위해 각 MN들은 라우팅 프로토콜에 개시되기 전에 OTP 키 생성을 위한 해시테이블을 생성해야 한다.

그림 3과 같은 해시테이블은 하나의 비트열 x로부터 해시체인을 생성한다. i가 1부터 길이 n일 때 $h^0(x)$은 x, $h^1(x)$은 $h(h^0(x))$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	$h^0(x_1)$	$h^0(x_2)$	⋯	$h^0(x_j)$	⋯	$h^0(x_n)$
1	$h^1(x_1)$	$h^1(x_2)$	⋯	$h^1(x_j)$	⋯	$h^1(x_n)$
2	$h^2(x_1)$	$h^2(x_2)$	⋯	$h^2(x_j)$	⋯	$h^2(x_n)$
⋮	⋮	⋮	⋯	⋮	⋯	⋮
k-i	$h^{k-i}(x_1)$	$h^{k-i}(x_2)$	⋯	$h^{k-i}(x_j)$	⋯	$h^{k-i}(x_n)$
k	$h^k(x_1)$	$h^k(x_2)$	⋯	$h^k(x_j)$	⋯	$h^k(x_n)$

그림 3. MN들의 해시테이블

3.2 경로 탐색 및 설정

안전한 통신 경로설정을 위해 SN이 DN까지 라우팅을 하고자 할 때, SN의 라우팅 테이블에 DN까지의 라우팅 정보가 없을 경우 이웃한 MN들로부터 DN까지 라우팅 경로 탐색을 위한 $H(RREQ)$ 메시지를 전송하여 경로탐색을 시작한다. SN은 전송하고자 하는 i번째 RREQ 메시지를 서명하기 위해 MD5를 적용하여 무결성이 보장된 $H(RREQ_i)$를 생성한다.

$H(RREQ_i)$는 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 $H(RREQ_i)$ 메시지에 추가하여 식 (3.1)과 같은 OTP를 생성하고 $H(RREQ)$ 메시지를 이웃한 MN들에게 전송한다.

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

$H(RREQ)$ 메시지를 수신한 이웃한 MN은 전자서명 검증을 위해 MD5를 적용하여 $H(RREQ_i)$를 얻고 $\log_2 n$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 $h^{i-i'}(r_j) = v_j$ 인지를 체크한다. $h^{i-i'}(r_j) = v_j$가 동일하다면 라우팅 정보의 무결성이 보장되었다는 것을 알 수 있으며, $H(RREQ)$를 검증한 MN은 다음 $H(RREQ)$ 메시지 탐색과 검증을 위해 v_j를 r_j값으로 갱신하여 SN에서부터 DN까지 포워딩 절차를 반복 수행한다.

SN으로부터 $H(RREQ)$ 메시지를 수신한 DN은 $H(RREQ)$에 대한 응답 메시지인 $H(RREP)$를 생성하여 SN에서 DN까지 생성된 역 경로를 통해 $H(RREP)$ 메시지를 전송한다.

그림 4와 같이 DN의 i번째 $H(RREP)$ 메시지는 $H(RREQ)$ 메시지와 동일한 무결성을 제공하기 위해 MD5를 적용하여 $H(RREP_i)$를 생성한다. $H(RREP_i)$ 메시지의 추가 비트를 구성하기 위해 $\log_2 n$비트가 메시지에 추가되며 $H(RREP_i)$에서 0의 비트수를 계산하여 $H(RREP_i)$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 $H(REEP)$ 메시지에 추가하여 OTP를 생성하고 $H(RREP)$ 메시지를 $H(RREQ)$의 역 경로를 통해 이웃한 MN들에게 전송한다. $H(RREP)$ 메시지를 받은 IN(Intermediate Node)3은 전자서명 검증을 위해 MD5를 적용하여 $H(RREP_i)$를 얻고 $\log_2 n$후 메시지의 비트열의 0의 개수를 계산하여 $H(RREP_i)$에 추가한 후 n비트 스트링 g값을 생성한다. j번째 비트 스트링 $g_j = 1$인 모든 j에 대하

여 $h^{i+i'}(r_j) = v_i$인지를 체크한다. $h^{i+i'}(r_j) = v_j$가 동일하다면 라우팅 정보가 기밀성과 무결성이 보장되었다는 것을 알 수 있다. *H(RREP)*를 검증한 IN3은 다음 *H(RREP)* 메시지 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 있으며, SN까지 DN이 보낸 *H(RREP)* 메시지가 전송되면 안전한 라우팅 경로가 확보된다.

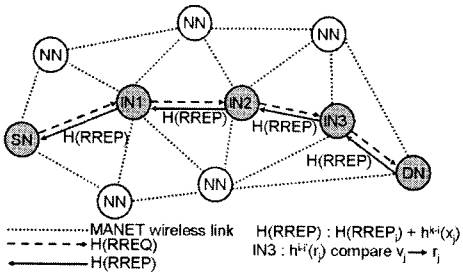

그림 4. 라우팅 경로설정

3.2 경로 유지 및 관리

경로설정 이후 각 MN들은 라우팅 경로가 유효한지를 확인하기 위해 이웃한 MN들에게 주기적으로 확인 메시지를 전송한다. MN들은 라이프타임 동안 경로상의 트래픽 발생이 없다면 MN의 라우팅 테이블에 경로가 활동하지 않는다고 체크한다. 그러나 유효하지 않는 경로로부터 데이터가 전달되면, MN은 SN으로 향하는 역 경로를 이용하여 *H(RRER)* 메시지를 생성하여 전송한다. 또한 MN들의 동적 특성으로 인해 경로상의 링크가 끊어진 경우도 *H(RRER)* 메시지를 생성하여 SN에게 전송한다.

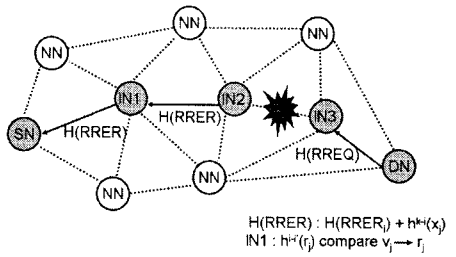

그림 5. 라우팅 경로유지

그림 5와 같이 *H(RRER)* 메시지가 SN에 도달할 때 까지 경로 상에 있는 MN들은 *H(RREQ)*와 *H(RREP)* 메시지와 동일하게 서명, 검증하고 다시 자신의 서명을 하여 메시지를 포워딩하는 절차를 반복적으로 수행한다. 악의적인 노드가 경로가 끊어졌다는 거짓된 *H(RRER)* 메시지를 위조하여 발송할 경우 악의적인 노드의 행동을 탐지하는 것은 어렵지만 *H(RRER)* 메시지가 OTP로 서명되어 있기 때문에 악의적인 노드가 다른 적법한 MN으로 위장하여 *H(RRER)* 메시지를 생성하는 공격을 막을 수 있다.

IV. 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 효율성이 증가하였다. 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.

참고문헌

[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, March, 2007.

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

[3] S. H. Seo, H. Lee, J. Lee, J. Ji, J. Song, "CPAA : Certificate based Predictable Address Auto-configuration Mechanism in Mobile Ad-hoc Networks", GESTS International Transactions on Computer Science and Engineering, Vol. 12, No. 1, June, 2005.

[4] 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, March, 2005.

[5] "The MD5 Message-Digest Algorithm", ftp://ds.internic.net/rfc/rfc1321.txt/