# 이동 애드혹망에서의 보안 라우팅 프로토콜

박준석° 조인휘
한양대학교 정보통신대학원
pk349°@ihanyang.ac.kr, iwjoe@hanyang.ac.kr

## Secure Routing Protocol for Mobile Ad-Hoc Networks

junseok park° inwhee joe
Graduate School of information and Communication, Hanyang University

**요 약**

보안은 유·무선 환경에서 가장 이슈가 되는 분야이다. 현재 이동 애드혹 망은 보안에 대한 고려 없이 진행이 되어있다. 고정된 기반구조를 가지고 있지 않기 때문에 보안은 이동 애드 혹 망에서 가장 취약한 점이며 많은 논문에서 ADOV혹은 DSR같은 프로토콜의 위협적인 요소들에 대해 문제점을 제시 하여왔다. 본 논문에서는 가장 가볍고 처리 속도가 빠른 메시지 인증 코드를 사용함으로써 AODV 라우팅(routing) 프로토콜(protocol)에 보안기능을 제안하였다.

## 1. 서 론

이동 애드혹 네트워크는 기지국 혹은 AP에 의한 중앙 집중화 된 관리나 표준화된 지원 서비스 없이 임시 망을 구성하는 무선 이동 단말 들의 집합으로, 그 특성상 임시 구성 망이나 재해, 재난 지역이나 전쟁터와 같이 기존의 기반 시설을 이용할 수 없는 환경에 적용하는 것으로 인식 되어 왔다. 이러한 이유로 이동 애드혹 네트워크에 대한 연구는 주로 군사용이나 대체 네트워크용으로 활용할 수 있는 방향으로 연구가 진행되어 왔다. 이동 애드 혹망은 고정된 기반 구조를 가지고 있는 것이 아니기 때문에 각 이동 단말들의 상태를 파악 하고 있어야 한다. 이동 네트워크 위상은 빠르고도 예측할 수 없게 변하기 때문에 이런 이동 단말들의 이동성 문제로 인하여 보안에 상당히 취약한 문제에 직면해 있다. 아직까지 애드 혹 네트워크를 위해 제안된 여러 종류의 라우팅 프로토콜에는 충분한 보안에 관한 알고리즘이 제시되지 못한 실정이다.

이동 애드혹 네트워크의 보안 요구조건은 다른 통신 네트워크에서 요구되는 것과 동일하다. 그러나 이동 애드 혹 네트워크에서는 노드의 신분이 서로에게 불확실한 경우가 많으며 멀티 홉 방식에 의해 라우팅을[1] 할 경우 악의적인 중간 노드에 의해 발생될 수 있는 데이터의 무결성 및 기밀성 문제가 존재한다. 특히 매체를 신뢰할 수 없는 상황에서 암호를 사용하므로 암호키에 크게 의존하게 된다. 따라서 키 사이에 신뢰할 수 있는 관계를 형성하고, 이를 이동 애드 혹 네트워크 전반에 분배하는 것이 주요 과제가 된다. 한편으로, 보안 문제가 확실히 해결되다 보면 컴퓨팅 문제가 발생되어 노드와 네트워크 전체에 심각한 부하를 주게 되므로, 이러한 trade-off를 고려한 이동 애드혹 네트워크에 적합한 알고리즘, 키 분배 및 인증 프로토콜 개발이 현실적으로 가장 필요하다.[1]

이 논문의 구성은 다음과 같다. 2장에는 제안 및 실습 하고자 하는 내용의 핵심 지식에 대한 간단한 소개, 3장에서는 제안하고자하는 프로토콜의 설계 방향 및 동작, 4장에서는 구현 테스트에 대한 내용과 마무리로 결론 및 향후 과제를 기술하였다.

## 2. 기본 배경

### 2.1 Secure Routing Protocol

현재 이동 애드혹 네트워크 보안의 연구는 크게 키 관리 기법과 라우팅 프로토콜 보안 등으로 나눌 수 있다.

-KEY MANAGEMENT 는 대표적인 연구를 들자면 Threshold cryptography를 사용한 관리 기법이 있다[2]. 이 기법은 어떤 임계 치를 두어서 노드들에게서 온 키가 같다면 올바른 키라고 생각하고 키를 적용한다. 그러므로 키가 변질 되거나 키를 효율적으로 관리 할 수 있다. 다른 방법들도 마찬가지로 효율적인 키 관리 메커니즘에 주제를 두고 있다.

- 라우팅 프로토콜 연구들은 공격에 대한 최적의 보안을 해주지만 프로토콜이 너무 덩치가 커지거나 보안에 믿을 만한 노드를 위주로 라우팅을 하기 때문에 만약 공격이 시도 되지 않는 상황이라면 최적의 라우팅 패스가 있는데 보안이 검증된 노드만이 통신 할 수 있다는 불필요한 점이 있다. 예를 들자면 각 노드가 신뢰할 수 있거나 공격을 막으려면 각 노드의 인증이 필요하며 인증키 혹은 암호화 키가 필요하다. 하지만 각 노드에서 처리하는 양이 많아짐으로서 노드들의 처리 속도와 전력 소비량이 증가 하였다.

요즘 추세는 일 방향 해쉬(Hash) 체인과 키 관리 매니지먼트(management)에[3] 대한 주제로 논문이 쓰이고 있다. 해쉬 체인은 웜홀(wormhole) 공격에 강한 면을 보이고 있기 때문이다.[4] 그 뿐만 아니라 기존 라우팅 프로토콜에서 성능 면에서도 많이 차이가 나지 않기 때문이다[5].

### 2.2 해쉬 함수

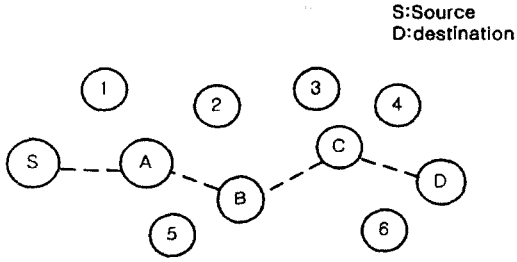
MAC(Message Authentication Code) 해쉬 함수, h()는 메시지의 작성자와 수신자만이 알고 있는 비밀키 k를 이용하여 메시지 m에 대한 인증자 MAC=h(k,m)을 계산해 낸다. 메시지와 함께 MAC이 수신자에게로 전달되면 수신자 측에서는 전달된 메시지를 이용하여 자기 자신이 계산한 MAC과 수신된 MAC을 비교함으로써 메시지에 대한 무결성을 확인하게 된다. 송신자와 수신자만이 k를 알고 있고, 수신된 MAC이 계산된 MAC과 일치한다면 수신자는 그 메시자가 정당한 메시지 작성자로부터 온 것이며 또한 전송 도중에 변조되어지지 않았다는 것을 확인할 수가 있게 된다. 능동적인 공격자는 비밀키 k를 모르기 때문에 메시지 변조를 수행할 수 있다고 할지라도 그 변조된 메시지에 해당하는 정확한 MAC을 계산해 내기는 계산적으로 거의 불가능하다.

## 3. 보안 프로토콜 설계

본 논문에서 구현하고자 하는 프로토콜은 해쉬(Hash)함수를 사용하는 방식이다. 보안에서는 흔히 메시지 인증 함수라 불리는 방식으로 그중에서 SHA-1을 사용하여 구현하였다.

### 3.1 기본적인 AODV동작

기본적인 AODV동작은 다음 그림과 같다




<그림1> AODV동작 과정

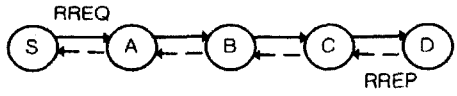
경로 획득은 노드들에게 패킷(packet)을 브로드 캐스트(broadcast)를 하면서 위치를 전달하고 목적지에 도달하면 여러 패스(path)중 최단 거리를 판단하여 온 길을 되돌아간다.

### 3.2 S-AODV(Secure-AODV)

S-AODV는 이동 애드혹 망의 취약점인 보안을 추가시킨 방법이다. 각 노드는 서로 간에 신뢰를 할 수 없으므로 인증을 하면서 각 노드사이에 악의적인 공격자가 끼어들지 혹은 데이터를 가져가지 못하도록 보안을 추가시킨 방법이다.

기본동작은 AODV방법과 비슷하지만 인증 여부의 계산이 추가된다.

<그림2>에는 패킷 방향이 그려져 있다. 처음 시작노드에서부터 브로드 캐스트 하는데 보내지는 패킷은 RREQ(Route Request)라 하며 목적지에 RREQ가 도착하면 RREP(Route Reply)가 소스(source)에 보내어 지게 된다.




<그림2> 패킷 전달 방향

<표1> 간단한 패킷 형식

| RREQ | RREP |
|---|---|
| 소스 주소 | Broadcast ID |
| 목적지 주소 | 소스 주소 |
| Hi=(Hi-1,브로드캐스트 주소, 전 노드 주소) | Hi |
| TimeStamp | TimeStamp |

i=1,2,3,..(노드에 따라 증가)

<표1>은 구현중인 S-AODV 실행에 필요한 간단한 패킷 형식을 기술하였다.

RREQ 패킷에는 소스 주소와 목적지 주소 그리고 MAC(Message Authentication Code)과 MAC을 만들기 위한 요소들 그리고 타임 스탬프(TimeStamp)가 사용된다. MAC값은 해쉬 체인에 의해 생성되며 해쉬 체인은 이전 노드에서 온 MAC값과 브로드 캐스트 주소, 그리고 전 노드의 주소로 이루어진다.

이 세 개의 값으로 MAC을 만드는 이유는 S->A, A->B.., 로 각 2개의 쌍으로 묶어 에러 찾기에 유리하게 하기 위함이다. 처음 소스S에서 보내는 패킷은 이전 노드가 없으므로 h0은 소스와 목적지 주소로 만들어지며 그 값으로 S->D에 보내지는 MAC값 H1=(H0,S,S)이 만들어진다. 그리고 다음 노드에서는 브로드 캐스트 노드와 전 주소 노드로 MAC값 H2=(H1,S,A)가 만들어진다.

RREP패킷은 목적지에서 생성되는 MAC값과 목적지 주소와 소스 주소로 구성된다. 예를 들면 D에서는 C에서 생성된 MAC값(h3라 칭함)과 자기 주소 그리고 전 노드인 C의 값이 들어가는데 그 값을 D에서 C로 보내주었을 경우 C는 D가 보낸 것을 알고 있으므로 자기가 가지고 있는 h3 와 C,D로 MAC값을 생성한 후 D에서 보낸 패킷에서 인증 부분을 비교한 후 변경이 안 된 것을 확인한다.

<표2> Route Discovery 예제

| |
|---|
| S->A: S , D , H1, (H0,S,S) , TimeStamp(12:11) |
| A->B: S , D , H2, (H1,S,A) , TimeStamp(12:12) |
| B->C: S , D , H3, (H2,S,S) , TimeStamp(12:13) |
| C->D: S , D , H4, (H3,S,S) , TimeStamp(12:14) |
| D->C: D , S , H4 , TimeStamp(12:15) |
| C->B: C , S , H3 , TimeStamp(12:16) |
| B->A: B , S , H2 , TimeStamp(12:17) |
| A->S: A , S , H1 , TimeStamp(12:18) |

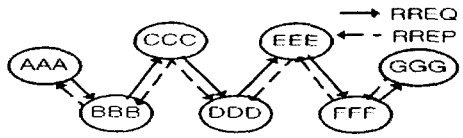
TimeStamp는 키를 결정할 때 사용된다. hash function은 기본적으로 비밀키가 필요하다. 그러므로 S->D까지의 라우팅에 노드들은 비밀키를 가지고 있어야 하는데, 그 키는 키 관리 테이블에서 관리하고, 각 시간구간별로 정해진 키를 사용하여 인증을 확인하는데 사용이 된다. 예를 들어 S->A에서 패킷에 보내진 시간을 보면 MAC값에 사용된 비밀키를 알게 되므로 인증을 할 수 있다. <표3>는 key 테이블로써 10초 간격으로 할당되었다.

<표3>Key 테이블

| Time(sec) | MAC키 값 (20byte) |
|---|---|
| 0~9 | 9m37WFlDP+6ycBsT+G1FfjaWs70= |
| 10~19 | cKszLQmrDCf/GbcdEp+LYfL9c9E= |
| 20~29 | 6XzFe4S/cB4DSSIw8/0YDntZka0= |
| 30~39 | zs97AEq1NNZD2uQ3W/L7AcYDGKY= |
| 40~49 | LRb4dkUY7HClA+UHfyp9sbeKL9Y= |
| 50~59 | ECPg3d3zjzfQ6D2kEq7D+lGmXis= |

## 4. 구현 테스트

사용언어는 JAVA이고 개발 툴은 eclipse를 사용하였다. 현재 실습 코드의 MAC은 Sun의 JCE에서의 HMAC함수 중에서 SHA-1을 기반에 두고 있다.




<그림3> 실행 예

기본 가정으로 <그림 3>처럼의 진행 방향을 하도록 시나리오를 작성하였으며 각 노드가 Key 테이블을 가지고 있다고 가정하였다. <표4>에서는 간단한 RREQ 패킷을 적용하였는데 이전 노드의 키는 해쉬 체인을 이루기 위해서 필요하다 해쉬체인은 공격자가 볼 수 있다고 해도 그 값을 이루기위해선 각 노드를 거쳐 온 키들을 다 알아야 하기 때문에 보안에 강하다고 할 수 있다. <표5>에 대해서는 RREP 패킷으로 목적지에서 전 노드로 갈 때 전 노드는 누구에게서 왔다는 것으로 키를 생성할 수 있으므로 간단하게 구성되었다. <그림 4,5,6>은 처음과 목적지에서 전 노드로 그리고 소스에 도착했을 때의 상황을 캡처(Capture)한 그림이다.

<표4> RREQ 패킷 형식

| 소스 | 목적지 | MAC키 | 이전노드의 MAC키 | 이전노드 주 소 | 브로드 캐스트 주 소 | 타임 |
|---|---|---|---|---|---|---|

<표5> RREP패킷 형식

| 목적지 | 소스 | MAC키 | 이전 노드의MAC키 | 타임 |
|---|---|---|---|---|

<그림4> AAA->BBB 인증화면

<그림5> GGG->FFF 인증화면

<그림6> BBB->AAA 인증화면

## 5. 결론 및 향후 과제

위의 결과는 전송된 MAC구성요소들을 해쉬 함수로 값을 생성하여 전송된 MAC과 같은지를 판별하였다. 하지만 시나리오의 부족으로 아직은 보안의 검증이 되질 않았다는 단점이 있고 키 배포에 관한 문제점이 있다. 키 테이블은 항상 모든 노드들이 가지고 있어야 하는데 키 관리자가 있거나 혹은 다른 루트를 통해서 보내져야만 한다. 이러한 문제와 향후 다양한 공격 시나리오를 적용하여 검증 및 보안 하도록 하겠다.

## [참고문헌]

[1] 권혜연,신재욱,이병복,최지혁,남상우,임선배, "이동 Ad hoc 네트워크 기술 동향", 전자통신동향분석 제18권 제2호, 2003

[2] L. Zhou and Z. J. Haas. "Securing Ad Hoc Networks", IEEE Network Magazine, November 1999.

[3] Manel Guerreo Zapata, N. Asokan, "Securing ad hoc Routing Protocols", Wise'02 , Atlanta, Georgia, USA, September 28, 2002

[4] David B. Johnson, David A. Maltz, Yih-Chun Hu, and Jorjeta G. Jetcheva, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks", Internet-Draft,draft-ietf-manet-dsr-07.txt. Work in progress, February 2002

[5] Yih-Chun Hu, David B. Johnson, and Adrian Perrig,"SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks", Proceedings of the 4th IEEE Workshop on Mobile Computing Systems & Applications (WMCSA 2002), pp. 3-13, IEEE, Calicoon, NY, June 2002.