MANET에서 CBRP을 이용한 은닉 라우팅 프로토콜의 설계

이재식*, 민소연**, 전문석*
*숭실대학교 컴퓨터공학과
e-mail: j30231@ssu.ac.kr*, symin@seoil.ac.kr**
mjun@computing.ssu.ac.kr*

Design of Hidden Routing Protocol using CBRP in MANET

Jae-sik Lee*, So-Yeon Min**, Moon-seog Jun*
*Dept of Computer Science, Soong-sil University
**Dept of Information Communication, Seoil College

요 약

본 논문에서는 MANET 환경에서 악의적인 노드들로부터 데이터를 보호하고 안전하게 전달하는 방법으로 클러스터 기반의 라우팅 알고리즘인 CBRP를 이용하여 클러스터 헤더간의 데이터 교환처럼 데이터를 캡슐화 하여 데이터의 은닉효과를 주었다. 또한 Diffie-Hellman 키 교환 알고리즘을 이용하여 노드간에 전송되는 데이터를 암호화함으로써 악의적인 노드는 데이터를 습득하더라도 키를 가지고 있지 않기 때문에 어떤 내용인지 알기 어려운 특성을 지니고 있다.

1. 서론

유비쿼터스 컴퓨팅 환경에서 네트워크는 중요한 이슈중의 하나이다. 이러한 네트워크 통신 중 이동성을 가진 노드들로 구성된 MANET(Mobile Ad-hoc Network)은 망을 구성하는 노드들의 자유로운 이동성을 보장하며 AP(Access Point)와 같은 기반구조가 없는 망을 말한다. 이러한 MANET 환경에서 전송되는 데이터는 쉽게 도청을 당하거나 변조 당할 수 있다. 또한 노드의 이동으로 인한 핸드오프 문제도 발생할 수 있다. 이러한 문제점을 해결하기 위하여 기존의 유선망에서 사용하던 보안방안을 그대로 사용하기에는 문제가 있다.

따라서 본 논문에서는 MANET 환경에서의 이러한 취약점을 보안하기 위하여 클러스터 기반의 라우팅 프로토콜인 CBRP를 기반으로 전송되는 데이터의 주소를 클러스터간의 주소로 변환하여 악의 적인 노드가 데이터를 습득하더라도 어떤 노드간의 데이터 교환인지 알기 어렵게 하였다. 또한 교환되는 데이터는 Diffie-Hellman의 키 교환 알고리즘을 사용하여 공유된 키 값으로 암호화되어 전송되므로 암호화된 데이터를 습득한 악의적인 노드는 키 값을 알 수 없으므로 데이터를 사용하기 어렵다.

* 본 연구는 서울시 산학연 협력사업으로 구축된 서울 미래형 콘텐츠 컨버전스 클러스터 지원으로 수행되었습니다.

2. 관련연구

2.1 CBRP

CBRP(Cluster Based Routing Protocol)은 네트워크를 구성하는 노드들을 분포에 따라 여러 개의 중복되거나 분리된 클러스터로 나누어 관리한다. 그리고 하나의 클러스터에 클러스터 헤더가 정해져서 각 영역에 속한 노드들의 정보를 관리한다. 클러스터 사이의 라우팅은 각 클러스터 헤더가 가지고 있는 정보들을 이용하여 동적으로 이루어진다.

2.1.1 노드 상태요소

CBRP의 노드들은 다음과 같은 3가지의 상태를 가질 수 있다.

1) Undecided - 네트워크에 처음으로 참여하는 노드들은 기본적으로 Undecided 상태에 놓이게 되고, Clusterhead 로부터 HELLO 메시지를 받게 되면 해당 Clusterhead 의 Member 가 된다. 만

약 어떠한 그렇지 않다면 노드는 이웃 노드 테이블을 구성하여 Clusterhead 가 될 수 있다.

2) Clusterhead - Clusterhead 에 놓인 노드는 주기적으로 HELLO 메시지를 전송하게되며 만약 다른 Clusterhead 로부터 HELLO 메시지를 전송받게 되면 Lower ID 알고리즘을 이용하여 ID가 더 낮은 노드가 Clusterhead 가 된다.

3) Member - 만약 클러스터에서 Clusterhead 가 사라지게 되고 lowest ID 이면Member 상태의 노드는 Clusterhead 상태로 바뀌게 된다. 그렇지 않은 경우는 Undecided 상태로 바뀌게 된다.

2.1.2 라우팅

CBRP는 다음과 같은 두 가지 데이터구조를 가지고 있다. 하나는 CAT(Cluster Adjacency Table)이고, 다른 하나는 2홉 토플로지 데이터베이스이다. CAT는 이웃 클러스터들의 정보를 저장한다. 이웃 클러스터들이 양방향 링크로 연결되었는지, 혹은 단방향 링크로 연결되었는지를 저장한다. 2홉 토플로지 데이터베이스는 HELLO 메시지를 통하여 생성된다. 2홉 거리에 있는 모든 노드들의 정보를 포함한다. 라우팅은 경로 발견과 발견한 경로로 패킷을 보내는 두 단계 과정으로 진행된다.

경로 발견은 다음과 같이 진행된다. CBRP는 ClusterHead 만이 RREQ(Route Request Package)를 전송한다. RREQ를 전달 받은 노드 N 은 그림 1과 같은 알고리즘을 따른다.

```
IF N is member
    IF D is in the neighbour table
        send RREQ to D
    ELSE IF N is gateway to clusterhead C
        forward RREQ to C
    ELSE
        discard RREQ
    ENDIF
ELSE IF N is clusterhead
    IF RREQ already seen
        discard RREQ
    ELSE
        record ID in cluster address list of RREQ
        IF D is neighbour OR D is two hops
            away send RREQ to D
        ELSE
            FOR EACH neighbouring clusterhead C DO
                IF NOT C in address list of RREQ
                    record C in cluster address list of RREQ
                ENDIF
                ENDFOR
            ENDIF
            broadcast RREQ
        ENDIF
    ENDIF
ENDIF
```

그림 1. CBRP 알고리즘

2.2 Diffie-Hellman의 키 교환 알고리즘

Diffie-Hellman 키 교환 알고리즘을 사용하면 사전에 공개키를 교환하지 않아도 두 노드간의 비밀키를 교환 할 수 있다. 키 교환 알고리즘은 다음과 같다.

2.2.1 전제조건

p, g : 크기가 큰 정수들로서 메세지의 송수신에 참여하는 모든 사람들에게 공개되어있다. 그리고 특히 g값은 p보다는 작고 1보다는 크다.

2.2.2 알고리즘

1) 송신자는 비교적 크기가 큰 난수 x를 발생시키고 이 값을 보관한다.
2) 수신자 역시 비교적 크기가 큰 난수 y를 발생시키고 이 값을 보관한다.
3) 송신자는 다음의 계산을 하여 그 결과를 수신자에게 보낸다.
   X = g^x mod p
4) 수신자는 다음의 계산을 하여 그 결과를 송신자에게 보낸다.
   Y = g^y mod p
5) 송신자는 Y를 받아서 다음의 계산을 한 후 비밀키 KeyA를 얻는다.
   KeyA = (Y)^x mod p = (g^y mod p)^x mod p
6) 수신자는 X를 받아서 다음의 계산을 한 후 비밀키 KeyB을 얻는다.
   KeyB = (X)^y mod p = (g^x mod p)^y mod p

위의 5와 6에서 계산된 결과인 KeyA와 KeyB는 같은 값을 갖게 되고 이 값을 비밀키 값으로 사용한다.

3. 제안하는 방법

3.1 클러스터 형성 단계

네트워크의 노드들은 2.1절에서 설명한 CBRP 알

고리즘을 이용하여 클러스터를 형성하게 된다. 클러스터가 형성된 노드들은 주기적으로 HELLO 메시지를 전송하여 토플로지의 상태를 유지한다. (그림 2)는 총 3개의 클러스터로 구성되어 있다.

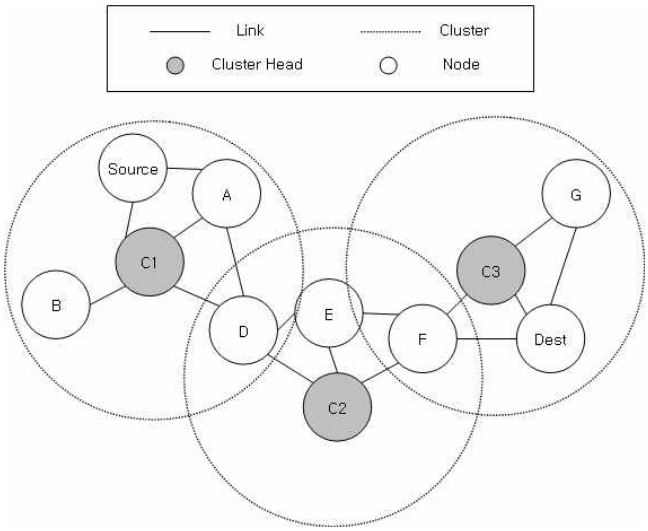

그림 2. 클러스터 형성 단계

3.2 비밀키 공유 단계

비밀키의 공유는 소스 노드와 목적지 노드간의 최초 데이터 교환시 발생하며, 소스와 목적지 노드는 교환된 비밀키를 이용하여 데이터를 암호화/복호화 한다. Diffie-Helman 알고리즘에 의하여 모든 노드는 사전에 정의된 {p, g} 값을 가지고 있어야 한다. 소스 노드와 목적지 노드간의 비밀키 공유는 2.2절에서 설명한 Diffie-Helman 절차에 의하여 공유된다.

3.3 Head 정보 등록 단계

비밀키를 공유한 소스 노드와 목적지 노드는 다음과 같이 ClusterHead 정보를 등록한다.

1) 소스 노드는 자신이 속해있는 ClusterHead 정보를 비밀키를 이용하여 암호화 하여 목적지 노드로 전송한다.
2) 목적지 노드는 해당 데이터를 복호화 하여 소스 노드가 속해 있는 ClusterHead 정보를 클러스터 정보 테이블에 저장한다.
3) 목적지 노드는 자신이 속해 있는 ClusterHead 정보를 비밀키를 이용하여 암호화 하여 소스 노드로 전송한다.
4) 소스 노드는 해당 데이터를 복호화 하여 소스 노드가 속해 있는 ClusterHead 정보를 클러스터 정보 테이블에 저장한다.

3.4 데이터 전달 단계

ClusterHead 정보의 등록까지 마친 소스 노드와 목적지 노드는 다음과 같이 데이터를 송수신한다.

1) 소스 노드는 Source IP는 소스 노드가 속한 ClusterHead 로 설정하고, Destination IP는 목적지 노드가 속한 ClusterHead로 설정하여, 다음 정보(소스 노드의 IP Address, 목적지 노드의 IP, Data)를 암호화 하여 Data 로 설정한다.
2) 1에서 설정된 Data는 CBRP 알고리즘에 따라서 목적지 노드가 존재하는 ClusterHead 까지 도착하게 된다. 목적지 노드의 ClusterHead 는 자신의 비밀키를 이용하여 Data를 복호화 한다. 만약 목적지 노드의 IP 가 ClusterHead의 IP와 같다면 이 Data는 ClusterHead 의 Data 이므로 Data를 상위 레이어로 전송한다. 만약 ClusterHead가 비밀키를 가지고 있지 않거나 복호화 한 Data 의 IP가 ClusterHead 의 IP 와 다른 경우 ClusterHead는 해당 Data를 Broadcast 한다.
3) 목적지 노드는 Destination IP 주소가 목적지 노드가 속한 ClusterHead 인 Data를 전송 받으면 자신이 가진 비밀키를 이용하여 해당 Data 를 복호화 한다. 만약 복호화된 Data의 IP 주소가 목적지 노드의 IP 주소와 같다면 해당 Data를 상위 레이어로 전송한다.

3.5 핸드오버 절차

MANET 환경에서의 노드는 이동성이 크다. 따라서 소스 노드나 목적지 노드는 핸드오버가 발생할 수 있다. 이때 핸드오버가 발생한 노드는 자신이 속한 ClusterHead 가 변경 될 수 있다. ClusterHead가 변경된 노드는 변경된 ClusterHead 정보를 3.3절의 1-4 절차를 통하여 갱신한다.

4. 성능 평가

4.1 암호화를 통한 은닉 라우팅 효과

본 논문에서 제안하는 방법은 ClusterHead 간의 데이터 이동만 보인다. 따라서 어떤 노드들이 통신을 하는지 알기 어렵고, Data의 내용 또한 어떤 내용인지 알기 어렵다. 비밀키를 이용하여 암호화된 Data가 전달되므로 공개키 기반의 암호화 방식에 비해 빠르게 암/복호화를 할 수 있으며 프로세서의 전력 또한 절약 될 수 있다. 또한 ClusterHead 정보

의 등록단계에서도 노드는 자신의 노드 정보를 암호화하여 전송하므로 공격자가 노드 정보를 가로 채더라도 어떤 노드인지 알 수 없다. 따라서 전송되는 노드간의 Data를 가로 채더라도 어떤 노드 간의 Data 전송인지 추측하기 어렵다.

4.2 ClusterHead가 Data 전송에 참여하는 경우

클러스터들을 오가는 패킷들은 3.2절에서 설명된 비밀키를 이용하여 캡슐화 된 Data가 암호화되어 전송된다. 따라서 ClusterHead 가 통신을 실제로 하는 것인지 아닌지 알 수 없으므로 공격자는 패킷을 가로채어도 비밀키를 가지고 있지 않기 때문에 캡슐화 된 Data를 복호화 할 수 없다.

4.3 클러스터 변경 시 정보 업데이트를 통한 핸드오버

노드간의 이동이 발생하여 핸드오버가 일어나는 경우 Data를 전송중인 노드는 클러스터가 존재하지 않는 지역의 ClusterHead로 Data를 전송할 수 있다. 따라서 3.5절에서 설명한 절차를 통하여 변경된 정보를 업데이트함으로써 위와 같은 핸드오버 문제를 해결 할 수 있다.

5. 결론

유비쿼터스 환경에서 네트워크 보안은 중요한 이슈중의 하나이다. 본 논문에서는 MANET 이라는 네트워크 환경 속에서 노드들 간의 데이터를 안전하게 보호하기 위하여 CBRP라는 클러스터 기반의 라우팅 알고리즘을 이용하여 노드들 간의 데이터 교환을 클러스터들 간의 데이터 교환인 것처럼 은닉하는 효과를 가지고 있다. 또한 전송되는 데이터는 Diffie-Hellman 알고리즘을 이용하여 공유된 키 값으로 암호화되어 전송되므로 중간에서 데이터를 가로채더라도 그 내용을 알기 어렵도록 설계하였다. 본 논문에서 제안된 방법을 통하여 보다 안전한 MANET 환경에서의 통신이 가능할 것으로 예상된다.

참고문헌

[1] Mingliang Jiang, Jinyang Li, Y.C., Cluster Based Routing Protocol(CBRP). Internet Draft, MANET Working Group, Tay, 14, August, 1999.

[2] Tim Daniel Hollerung, The Cluster-Based Routing Protocol, project group 'Mobile Ad-Hoc Networks Based on Wireless LAN', winter semester 2003/2004

[3] E. Rescorla, Diffie-Hellman Key Agreement Method, Internet proposed standard RFC 2631, June 1999.

[4] W. Diffie and M.E. Hellman, New directions in cryptography, IEEE Transactions on Information Theory 22 (1976), 644-654.