# Ad hoc 환경에서의 안전한 라우팅 프로토콜을 위한 키 관리 기법

임정미*, 박창섭**
*단국대학교 전자계산학과
**단국대학교 전자계산과
e-mail:redpig3@dankook.ac.kr

# Key management mechanism for secure routing protocol in Ad hoc

Jeong-Mi Im*, Chang-Seop Park**
*Dept of Computer Science, Dan-Kook University
**Dept of Computer Science, Dan-Kook University

요 약

ad hoc 네트워크는 호스트와 라우터 역할을 동시에 하는 무선 노드들로 구성되고, 각각의 노드들의 이동성과, 제한된 특성으로 인하여 잦은 네트워크 토폴로지의 변화가 일어난다. 그러므로 ad hoc을 구성 하고 있는 노드들의 인증과, 경로 탐색에 사용되는 라우팅 정보의 무결성, 전송되는 데이터의 기밀성을 제공하는 방법이 기존의 유선 환경과는 다르다. 본 논문에서는 IPv6의 자동 주소 설정 방식과 IP 생성 방식 중 CGA(Cryptographically Generated Address) 방식을 이용하여, IP 주소에 대한 소유권(ownership) 문제를 해결하고, 중앙 집중적인 인증기관과 키 발급 센터가 없이, ad hoc에 참여한 노드 스스로 키를 생성하고, 인증하는 방식을 제안한다. 또한, SAODV 라우팅 프로토콜의 필드 값 중 공개키 값을 가지고, Diffie-Hellman 키 교환 방식을 적용하여, 안전하게 경로 설정이 된 후에 전송되는 데이터의 기밀성을 제공하는 방식을 제안한다.

## 1. 서론

ad hoc 네트워크는 유선의 base station이나 access point 등과 같은 유선 네트워크와 결합으로 구성된 것이 아닌, 네트워크 인프라를 갖추지 않은 환경에서의 무선 노드들로만 구성된 모바일 네트워크 형태이다.

ad hoc 환경에서의 각각의 무선 노드들은, 이동성을 갖는다. 각각의 모바일 노드들이 이동을 하면 전체적인 ad hoc 네트워크의 토폴로지의 변화를 가져오고, 중간 노드들이 라우터 역할을 하며 데이터를 소스 노드에서 목적지 노드까지 전송해준다. 즉, ad hoc 환경에서의 무선 노드들은 호스트와 라우터 역할을 동시에 하게 된다.

또한, ad hoc 환경에서의 노드들은, 제한된 자원의 사용으로 인하여 갑자기 노드가 사라지거나, 새로운 노드가 ad hoc에 참여하게 되어 네트워크 토폴로지의 변화를 가져온다.

위와 같은 특성으로 인한 잦은 토폴로지의 변화로 인하여, 데이터를 전송하고자 하는 소스 노드에서, 목적지 노드까지의 경로를 탐색, 유지해주는 프로토콜이 필요하다. ad hoc 네트워크의 라우팅 프로토콜은 주기적으로 노드의 라우팅 정보(routing information)를 주변 노드(neighbor node)에 전달하는 table driven방식과, 소스 노드에서 목적지 노드로 데이터 요청이 발생할 때, 경로 탐색을 시작하는 on demand 방식이 존재한다.

유선 네트워크 환경에서는 송/수신 측의 인증을 위하여, 전자서명, 미리 공유된 키를 이용한다. 예를 들어 인증기관인 CA를 이용하여 인증서를 발급받거나, 키 발급 센터를 이용하여 키를 공유하게 된다. 그러나 CA와 키 발급 센터는 중앙 집중적인 방식으로 앞에서 설명한 ad hoc 네트워크의 잦은 토폴로지의 변화를 유발하는 특성으로 인하여 ad hoc 환경에서는 사용할 수 없다. 기존의 연구들은 중앙 집

중적인 CA의 역할을 분산하는 방식으로, 이는 현실적으로 불가능하다.

ad hoc 네트워크 환경에서는 다른 노드로 데이터를 전송하기 위하여 라우터 역할을 하는 중간 노드들이 라우팅 정보와, 데이터를 전달해 줘야한다. 이때, 라우팅 정보를 공격자가 수정하여 재전송 한다면, Dos 공격, 재생 공격 등이 발생하게 된다. 라우팅 정보를 변경하지 않게 하기 위하여 데이터를 주고받는 소스 노드와 목적지 노드, 또 중간 노드들 사이의 인증이 반드시 필요하며, 안전한 라우팅 프로토콜이 필요하다. SRP, Ariadnie, SEAD, SAODV 등과 같은 안전한 라우팅 프로토콜[]은, 이미 라우팅 정보를 주고받는 노드들이 이미 키 쌍을 안전하게 분배되었다는 가정하에서 각각의 알고리즘을 설명하고 있다.

본 논문에서는 ad hoc의 특성에 기반하여, ad hoc에 참여하는 노드 스스로가 자신의 키 쌍을 생성하고, 생성된 키 쌍으로 자신을 인증 받고, 부인봉쇄를 위하여, IPv6의 주소 할당(address auto-configuration) 기법[1]에서, 자신의 IP주소를 만드는 방법 중 공개키를 IP주소의 일부분으로 넣는 CGA(Cryptographically Generated Address) 기법[2]을 사용하고, 안전한 라우팅 정보를 교환과 안전한 데이터의 전송을 위하여 SAODV에 첨부된 공개키를 Diffie-Hellman 키 교환 방식을 이용하여 세션키를 생성하여 전송되는 데이터의 기밀성을 제공하도록 한다.

## 2. 관련연구

### 2.1 CGA(Gryptographically Generated Address)를 이용한 IPv6의 Auto-Configuration

IP는 네트워크상에서 각각의 호스트를 식별할 수 있는 식별자이다. IPv6에서는 IP 주소를 할당하는 방식으로, stateful 방식과, stateless 방식이 있다. stateful 방식은 IP를 할당받기를 원하는 호스트가 DHCP 서버로부터 주소와 다른 관련 정보를 얻는 방법이고, stateless 방식은 호스트가 자신의 IP 주소를 생성할 수 있다.

DAD(Duplicate Address Detection)은 중복 주소를 탐지하는 방식으로, 호스트가 자신의 IP를 생성하여 이웃 노드들에게 NS(Neighbor Solicitation) 메시지를 보내고, 같은 주소를 이미 사용하고 있는 호스트는 NA(Neighbor Advertisement)를 응답으로 보내게 된다. 즉, NS 메시지를 브로드캐스트 한 후, 일정 시간이 지난 후에 NA 메시지를 받게 되면, 호스트가 생성한 IP 주소는 중복되는 것이므로, 새롭게 생성하여야 하고, NA 메시지를 받지 못하면, 유일한 IP주소이므로 사용 가능하다.

CGA는 128비트의 IPv6의 IP주소를 암호학적으로 생성하는 방식으로 그림 1과 같이 뒷부분의 64비트를 공개키 값과 난수 값을 해쉬 함수를 이용하여 계산한다. 이때, 난수 값은 IP주소의 중복성을 방지하기 위하여 삽입한다. 이렇게 생성된 주소를 이웃 노드들에게 브로드캐스트하여 중복된 IP 주소 값을 가진 노드가 있으면 다시 난수 값을 변경하여 새로운 IP 주소를 만들어 낸다.

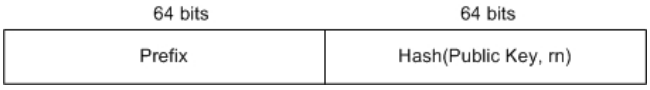


그림 1 CGA의 IPv6 주소 구조

### 2.2 SAODV

Ad hoc 네트워크에서 on-demand 방식의 라우팅 프로토콜 중 AODV[3] 방식은, 라우트 경로 탐색, 경로 유지 두 과정이 있다. 라우트 경로를 탐색하고, 탐색된 경로를 이용하여 데이터를 전송하게 된다. SAODV[4]방식은 AODV 방식의 확장된 형태로, 그림 2와 같이, AODV 필드에 해쉬 값과, 서명을 이용하여 보안을 추가한다.

Ad hoc 네트워크에서의 공격은 데이터를 전송할 경로를 변경하여 정상적으로 데이터가 전송되지 못하게 하거나, 필요 이상으로 처리 과정을 반복하여 제한된 자원을 고갈시키는 것을 목적으로 이뤄진다. AODV 라우팅 프로토콜에서는 소스 노드로부터 목적지 노드까지의 최단 경로를 선택한다. 이때, 경로 요청을 하는 RREQ 메시지의 Hop Count는 소스 노드로부터의 거리를 나타낸다. 공격자는 Hop Count를 변경하여 DoS공격을 발생키시고, Sequence Number를 변경하여 재생 공격을 발생시킨다.

SAODV에서는 그림 2와 같이, 각 노드들에서 위의 라우팅 정보들이 변경되지 않음을 인증하기위하여, 해쉬 함수와, 서명을 이용한다. 이때, 각각의 노드에서 1씩 증가시키는, 즉 각각의 노드가 변경할 수 있는 Hop Count 값은 해쉬 함수를 이용하고, 나머지 라우팅 정보들은 모든 노드들에서 같게 나타나므로, 서명을 이용하여, 중간 노드에서 변경이 이뤄지지 않았음을 인증하게 한다. 그림 2의 각 필드가 나타내는 값은 표 1과 같다.

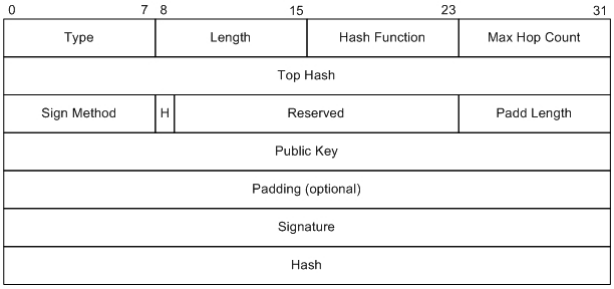


그림 2 SAODV의 RREQ/RREP

| 필드명 | 값 |
|---|---|
| hash function | 사용하는 해쉬 함수명 |
| Max Hop Count | TTL |
| Top Hash | $h^{(Max\,Hop count)-(Hop count)}(Hash)$ |
| Public Key | 노드의 공개키 |
| Signature | hop count를 제외한 AODV 필드를 개인키로 서명한 값 |
| Hash | seed |

표 2 SAODV의 필드 설명

라우팅 정보를 보낸 노드와, 라우팅 정보를 인증하는 방식은 다음과 같다.

첫째, SAODV의 형태가 아닌, 즉 AODV의 RREQ/RREP의 형식으로만 이뤄진 메시지는 버린다(discard).

둘째, SAODV 형태의 메시지가 수신되었다면, Hop Count의 무결성 검증은, 수신된 라우팅 정보에서, 식 1과 같이 Top Hash 값을 계산하여, 수신된 Top Hash 값과 같으면 된다. 또한 첨부된 공개키를 이용하여 서명 값을 풀어 AODV의 라우팅 정보 값을 인증할 수 있다

$$h^{(Max\,Hop count)-(Hop count)}(Hash) \qquad (식1)$$

위와 같은 방식으로 인증을 하여, 정상정인 인증이 이뤄졌으면 역경로(reverse path)를 만들고, 라우팅 정보를 업데이트하여 다시 브로드캐스트 한다.

## 3. 제안

ad hoc 네트워크 환경에서의 보안은 소스 노드에서 목적지 노드까지의 경로 설정을 위한 라우팅 정보 보안과, 설정된 경로상에서 안전하게 데이터를 전송하는 보안 두 가지로 나뉜다.

안전하게 경로 설정을 하기 위해서는, 각각의 노드들이 인증과 노드들이 보내는 라우팅 정보의 무결성이 요구된다.

기존의 유선환경에서는 중앙집중적인 CA를 이용하여 인증을 받고, 키 분배 센터를 두고 키 쌍을 안전하게 분배 받았으나, ad hoc 환경에서는 이동성과 제한된 자원 등의 특성으로 인한 토폴로지의 갖은 변화 때문에, 유선 환경에서의 인증, 키 분배 방식을 사용할 수 없다. 즉, ad hoc에 참여하는 각각의 노드들이 스스로 키 쌍을 생성하고, 다른 노드들을 인증하여야 한다.

ad hoc 환경에 참여 하고자 하는 노드는 IPv6의 주소 자동 설정을 이용하여 자신의 IP 주소를 만든다. IP주소는 네트워크상에서의 유일한 식별자이므로, 다른 노드들과 중복되지 않아야 한다. 새롭게 참여하는 노드는 임시주소를 사용하며, 주소를 요청하는 AREQ 메시지를 통하여, 자신이 생성한 IP 주소를 이웃노드에게 알려야 한다. AREQ를 수신한 노드들은 자신이 쓰고 있는 IP 주소와 요청된 IP 주소가 같으면 이미 사용하고 있다는 AREP 메시지를 보내게 되고, 같지 않으면 아무런 메시지도 보내지 않고, 수신한 AREQ를 다시 브로드캐스트 한다. IP 주소의 중복을 확인하는 노드는 같은 AREQ를 몇 번 보내고 응답이 없으면 자신이 만든 IP 주소를 사용하면 된다. 이때 공격자가 자신이 사용하지도 않으면서 같은 IP 주소를 사용하고 있다고 단순히 응답 메시지만 보내게 되면, 소유권(ownership) 문제가 발생한다. 그런 문제를 해결하기 위하여 IP 주소 생성 시 CGA방식을 이용하여 생성하고, AREQ 메시지와 AREP 메시지를 그림 3, 그림 4와 같이 IP 주소 생성에 사용된 공개키 값과, 새롭게 생성된 IP 주소를 개인키로 서명한 값을 추가하여 AREQ, AREP 메시지를 보낸다.


그림 3 AREQ


그림 4 AREP

이때의 IP 주소의 소유권 문제와 노드의 인증은, 그림 5와 같이 확인된다. 첨부된 공개키를 해쉬값을 취하여 IP 주소의 후반 64비트와 비교하여, 인증 기관 없이 공개키를 인증할 수 있고, 첨부된 서명을

확인 하여, 첨부된 공개키의 주인이 정당한, IP 생성 자임을 확인할 수 있는 IP주소의 소유권(ownership) 문제를 해결할 수 있다.

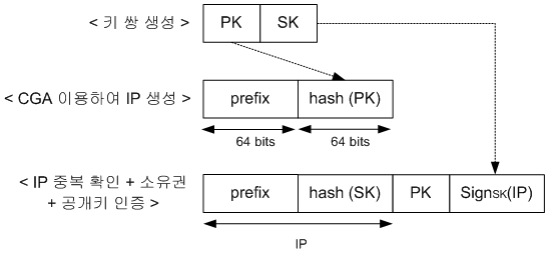


그림 5 IP 주소와 공개키 값의 인증을 위한 형태

AODV의 라우팅 정보의 무결성, 부인봉쇄는 기존의 SAODV를 이용한다.

라우팅 정보의 경우 메시지의 크기가 작으므로 공개키 방식을 사용하지만, 실질적으로 전송하고자 하는 데이터의 경우에는, 계산량을 줄이기 위하여, 대칭키 방식을 사용하여야 한다. 소스 노드와 목적지 노드는, 주고받은 SAODV의 RREQ 메시지와 RREP 메시지에 삽입된 공개키를 Diffie-Hellman 방식을 통하여 비밀키를 구한 후, 데이터를 암호화 하여 전송하여, 데이터의 기밀성을 유지한다.

즉, 소스 노드와 목적지 노드는 각각 ( $S_{SK}$ , $g^{S_{SK}}$ ), ( $D_{SK}$ , $g^{D_{SK}}$ )의 키 쌍을 생성하고, 이렇게 생성된 키 쌍은, IP 생성은 물론, SAODV의 공개키 필드에 사용될 뿐 아니라, 식 2와 같이 안전한 데이터의 전송을 위한 비밀키 생성에도 사용된다.

$$sesson\ key = \left(g^{D_{SK}}\right)^{S_{SK}} = \left(g^{S_{SK}}\right)^{D_{SK}} = g^{S_{SK} \cdot D_{SK}} \quad \text{식(2)}$$

SAODV를 이용하여 안전한 경로 설정을 한 후, 세션키를 이용하여 안전하게 데이터를 전송한다.

위의 과정에서 전송되는 메시지를 순서대로 정리하고, 제공되는 보안 서비스를 정리하면 그림 6과 같다.

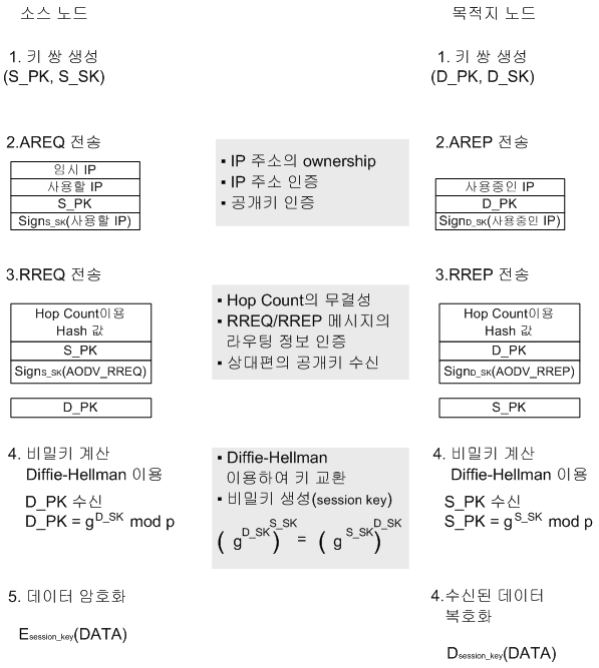


그림 6 순서에 따른 전송 메시지와 제공되는 보안 서비스

## 4. 결론

ad hoc 네트워크에서의 보안은 경로 탐색 과정에서 안전하게 라우팅 메시지를 전달하는 것과, 안전하게 만들어진 경로를 따라서 데이터를 안전하게 전송하는 것, 두 가지가 필요하다.

안전한 라우팅 프로토콜을 위하여 안전하게 키를 분배받고, 인증을 받기 위하여, ad hoc의 특성상 유선 네트워크에서의 인증 방식을 그래도 사용할 수 없으므로, 본 논문에서는 CGA 방식을 이용하여 노드 자체가 키 값을 생성하며, IP와 연결된 값이므로, 인증기관 없이 IP와 키 값의 인증을 가능하게 하고, IP주소의 소유권(ownership) 문제를 해결하였다. 또한 경로 탐색을 위해 전송되는 라우팅 메시지에 있는 키 값을 이용하여 비밀키를 생성하여, 데이터를 전송함으로서, 데이터의 전송에도 기밀성을 보장하였다.

## 참고문헌

[1] "IPv6 Stateless Address Autoconfiguration", RFC 2462

[2] "Cryptographically Generated Address(CGA)" draft-ietf-send-cga-06.txt

[3] "Ad hoc On-Demand Distance Vector (AODV) Routing" draft-ietf-manet-aodv-13.txt

[4] "Secure Ad hoc On-Demand Distance Vector (SAODV) Routing" draft-guerrero-manet-saodv-02.txt