# IPv6 주소 자동 설정 방식의 프라이버시 문제 연구

오지수*, 김호연**, 임헌정**, 정태명*
성균관대학교 정보통신공학부*, 성균관대학교 전자전기컴퓨터공학과**
e-mail : *{jsoh, hykim, hjlim99}@imtl.skku.ac.kr, **tmchung@ece.skku.ac.kr

# A Study on Privacy Issue for IPv6 Stateless Address Auto-configuration

Ji-Soo Oh*
Ho-Yeon Kim*, Hun-Jung Lim*, Tai-Myuong Chung**
* School of Information Communication Engineering, Sungkyunkwan University
** Dept. of Electrical and Computer Engineering, Sungkyunkwan University

**요 약**

IPv4 의 주소 고갈 문제를 해결하고 더 개선된 서비스를 제공하기 위해 IPv6 가 개발되었다. IPv4 와 달리 IPv6 는 보안을 고려하며 설계되어 기본적으로 IPSec 를 제공한다. 하지만 IPv6 에도 보안상의 취약점이 있어서 여러 공격과 보안 문제에 노출되어 있다. 그 중에서도 프라이버시 침해 문제가 존재하는데, 이 문제는 IPv6 에서 제공하는 주소 자동 설정 방식(Stateless address auto-configuration)에서 발생한다. 이 주소 자동 설정 방식은 주소 공간의 효율적인 관리를 위해 제안되었다. 주소 자동 설정 방식에서 프라이버시 침해 문제가 발생하는데, 개인 식별 프라이버시와 위치 프라이버시로 분류할 수 있다. 본 논문에서는 프라이버시 위협과 그에 따른 해결 방안을 기술하고, 해결 방안에 따라 고려해야 할 사항들을 설명함으로써 프라이버시 침해 문제를 해결하는 데 도움을 주고자 한다.

## 1. 서론

기존에 사용했던 IPv4 는 32 비트 주소 체계로 되어 있었다. 약 43 억 개의 주소를 할당할 수 있지만, 비효율적인 주소 할당과 인터넷의 발달 등의 이유로 주소 공간이 부족하게 되었다. Internet Engineering Task Force(IETF)는 2008 년에서 2011 년 사이에 IPv4 주소가 고갈될 것으로 예측했으며, 최근에는 Internet Assigned Numbers Authority(IANA)에서 IPv4 의 주소 잔여분이 고갈되어 전세계적으로 주소할당을 중지함을 발표했다. 이러한 주소 고갈 문제를 해결하기 위해 IPv6 가 제안되었다. IPv6 는 IETF 공식 규격으로, 128 비트 주소체계를 지원하여 무한대에 가까운 주소를 할당할 수 있다. IPv4 에서 IPv6 로의 가장 주된 변화는 주소 아키텍처의 변화이지만 그 외에도 IPv4 의 단점을 개선하면서 새로운 기능도 개발되었다. IPv6 에서 개선된 점 중에 하나가 보안이다. IPv4 가 처음 정의될 때는 보안이 주된 고려사항이 아니었기 때문에 이후에 IPSec 가 옵션으로 적용되었지만, IPv6 는 IPSec 를 기본적으로 제공하도록 개발되었다. 따라서 데이터 기밀성과 데이터 무결성, 인증 등이 지원되어 보안 효율이 향상되었다. IPv4 에 비해서는 보안 문제가 많이 개선되었지만, IPv6 에도 여전히 취약점은 존재하고 있다.

여러 보안상의 문제가 존재하지만, 본 논문에서는 프라이버시 문제에 초점을 두었다. 프라이버시는 위치 프라이버시(Location Privacy)와 개인 식별 프라이버시(Identity Privacy)로 나누어진다. 위치 프라이버시는 호스트의 위치 정보를 다루고, 개인 식별 프라이버시는 호스트 IP 의 익명성을 보장한다.

IPv6 는 방대한 주소 공간을 효율적으로 관리하기 위해서 주소 자동 설정 방식(stateless address auto-configuration)을 제공한다[4]. 주소 자동 설정 방식은 관리자의 수동적인 조작 없이 호스트에서 자동으로 주소를 설정함으로써 많은 편리함을 제공하지만, 여기에서 프라이버시에 위협이 발생한다. 호스트에서 IPv6 주소가 설정될 때 인터페이스 주소를 사용함으로 NIC 가 교체되지 않는 한 계속 동일한 주소가 설정되는 문제가 발생할 수 있고, IPv6 주소에 네트워크 주소가 암호화나 수정 없이 그대로 사용됨으로써 위치 정보가 노출 될 가능성이 생겼다. 주소의 동일성과 네트워크 주소 사용이 개인 식별 프라이버시와 로케이션 프라이버시 두 부분 모두를 위협할 수 있게 된 것이다. 이 위협에 대한 해결책으로 Dynamic Host Configuration Protocol version 6 (DHCPv6), Cryptographically Generated Addresses (CGA), Privacy Extensions(PE), Cryptographically Protected Prefixes(CPP) 가 있다[2][5][6][7]. 본 논문에서는 각 기술의 특징과 고려사항을 분석함으로써 프라이버시 침해 위협을 줄이는데 도움을 주고자 한다.

본 논문의 구성은 다음과 같다. 1 장 서론에 이어, 2 장에서는 IPv4 에서 IPv6 로의 개선점을 다루고, 그 중 주소 자동 설정 방식의 특징과 그에 따라 발생하는 프라이버시 위협 문제에 대해 기술할 것이다. 3 장에서는 이 프라이버시 위협 문제를 해결할 다양한 방안들과 고려사항을 기술하고 마지막 4 장에서 해결방안의 차이점으로 결론을 맺는다.

## 2. 주소 자동 설정 방식

IPv4 의 주소고갈 문제가 IPv6 개발의 주된 이유이지만, 그 외에도 여러 부분이 개선 되었다.

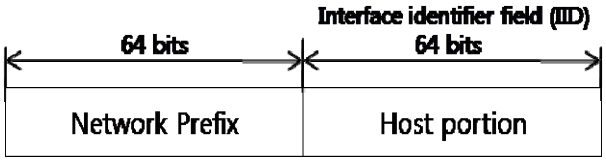
먼저, IPv4 의 복잡한 헤더 형식이 단순화 되었다. IPv4 에서는 사용하지 않거나 불필요한 헤더들이 존재했는데, IPv6 에서는 이 부분을 제거하고 헤더 길이를 40 바이트로 고정시켰다. 대신 확장헤더를 사용해서 옵션을 유연하게 사용할 수 있게 했고, 이로 인해 규격이 개선되어 처리 효율이 높아졌다. 또, 라우팅 테이블의 간소화와 라우팅 최적화로 IPv4 의 라우팅 문제가 해결되었다. 프로토콜이 확장 가능하게 설계 되어, 미래에 추가적인 옵션의 정의가 용이해 진 부분도 IPv6 의 개선점 중에 하나이다. 이외에도 QoS(quality of Service)지원이 개선되었으며, 플로우 레이블링(flow labeling) 개념이 도입되어 특정 플로우에 속한 패킷을 분류할 수 있게 되었다. 또한 패킷 크기가 확장 가능해져서 임의로 크기가 큰 패킷을 주고받을 수도 있게 되었고, 이로 인해 대역폭이 넓은 네트워크를 더 효율적으로 활용할 수 있게 되었다. 이외에도, IPv4 에서는 부가적 기능이었던 IPSec(IP Security)를 기본 제공 함으로써 데이터 기밀성과 데이터 무결성, 인증 등을 지원해 보안 서비스의 효율을 향상시켰다.

IPv4 에서 IPv6 로 발전되면서 생긴 장점들이 많지만, 그 중에서도 자동 주소 설정 방식이 IPv6 의 주요 개선점 중에 하나이다. IPv6 로 늘어난 주소 공간의 효율적인 관리를 위해 ND(neighbor discovery)에 의한 상태 비보존형 자동 주소 설정 방식(stateless address autoconfiguration)이 제공되었는데, 이로써 사용자가 직접 주소를 설정하거나 DHCP(dynamic host configuration protocol)를 이용하지 않고도 주소를 설정할 수 있게 되어 사용자와 네트워크 관리자에게 편리성이 증가하였다. 여기서 ND 프로토콜은 IPv4 에서 Address Resolution Protocol(ARP)를 대체하고, Internet Control Message Protocol version 6(ICMPv6) 메시지를 이용한다. IPv6 에서 일반적으로 사용하는 이 자동 주소 설정 방식은 유비쿼터스 환경과 모바일 환경에서 네트워크 지원을 돕는 등 꼭 필요한 기능이지만, 이 기능의 몇 가지 특징이 프라이버시 침해의 원인이 되었다.

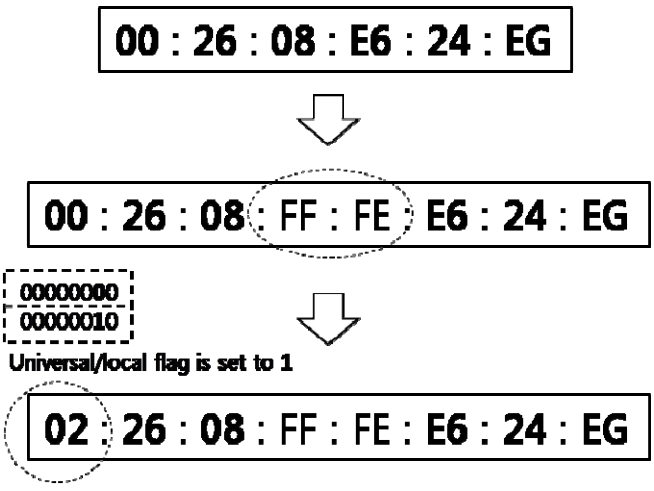
(그림 1)을 보면 IPv6 주소가 두 부분으로 나누어져 있음을 알 수 있다. 처음 64 비트는 네트워크 프리픽스로, 호스트가 로컬망의 라우터에서 전송받은 프리픽스 주소부분이다. 라우터는 링크와 관련된 서브넷을 식별하는 프리픽스를 호스트에 제공한다. 그리고 나머지 64 비트의 호스트 부분(host portion)은 48 비트의 Media Access Control(MAC) 주소의 확장된 값을 사용한다.

48 비트 MAC 주소를 64 비트로 확장시키는 방식 중에 extended unique identifier(EUI-64) format 이 있다. 먼저 MAC 주소를 24 비트씩 두 부분으로 나눈다. 그 다음 16 진수로 0xFFFE 인 16 비트 값을 그 두 부분 가운데에 넣어 64 비트를 형성한다. 64 비트 중 왼쪽에서 7 번째 비트에 위치한 universal/local flag 를 1 로 설정해주면 IPv6 주소의 호스트 부분이 된다. (그림 2)는 위의 과정을 보여주고 있다.

IPv6 주소의 네트워크 프리픽스가 변경되어도 호스트 부분은 변경되지 않는다. 이 점은 사용자의 개인 식별 프라이버시를 위협할 수 있는 요소가 된다. 또한, 네트워크 프리픽스 부분도 주소가 변하지 않는 점에서 개인 식별 프라이버시의 위협요소가 될 수 있다. 주소의 동일성이 개인 식별 프라이버시의 위협이 되는 이유는, 같은 주소를 계속 사용하는 경우 도청이나 트래픽 분석이 가능해지고 IP 의 익명성에 문제가 발생할 수 있기 때문이다. 네트워크 프리픽스는 개인 식별 프라이버시도 위협하지만, 네트워크 주소를 그대로 사용한다는 점에서 위치 프라이버시 문제도 발생할 수 있다. 네트워크 프리픽스가 호스트가 속한 네트워크의 주소이고, 이러한 정보가 호스트의 지리적 위치를 찾는 수단이 될 수 있기 때문에 위치 프라이버시도 침해될 수 있다.




(그림 1) IPv6 128 비트 주소 형식




(그림 2) 64 비트 Extended Unique Identifier (EUI-64) format

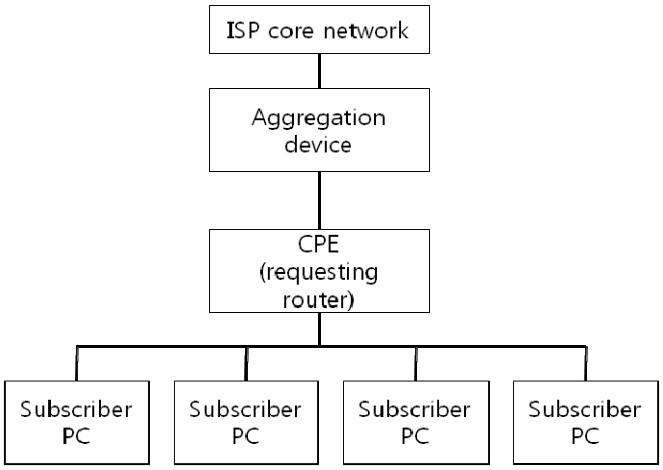
## 3. 프라이버시 문제 해결책

### 3.1 DHCPv6

DHCP 는 DHCP 서버를 통해 제공되는 어드레스와 기타 구성 정보들을 디바이스에 제공해준다. 상태 보존형 주소 자동 설정(stateful autoconfiguration protocol) 방식으로서, 앞서 설명했던 IPv6 의 일반적인 주소 자동 설정 기능의 단점들을 보완할 수 있다. DHCPv6 는 IPv6 네트워크 환경에서 네트워크 설정을 제공해 주는데, 기본적인 기능은 DHCPv4 와 유사하다. DHCPv6 는 여러 옵션을 통해 이러한 네트워크 설정 정보를 종합적으로 제공한다. 그 중 프리픽스 할당 옵션은 DHCPv6 서버를 이용하여 IPv6 프리픽스들을 자동으로 할당한다. 네트워크 관리자의 도움 없이 자동으로 요청라우터(requesting router)의 프리픽스 요청 시 IPv6 프리픽스 옵션을 이용하여 프리픽스를 할당할 수 있다.

(그림 3)에서처럼 IPv6 서비스 제공을 위한 ISP(Internet Service Provider)가 CPE(customer Premises Equipment, 고객과 ISP 네트워크 사이의 라우터 역할) 장비에 프리픽스를 할당해야 하는 경우 효과적으로 사용 가능하다.

IPv6 의 일반적인 주소 자동 설정 기능에서는 라우터에서 네트워크 주소를 그대로 네트워크 프리픽스로 제공하고, 또 그 주소를 계속해서 유지함으로써 위치 프라이버시와 개인 식별 프라이버시 두 부분 모두가 침해될 가능성이 있었다. DHCPv6 는 네트워크 주소를 그대로 제공하거나, 매번 같은 주소를 제공하지 않기 때문에 두 위협을 모두 제거할 수 있다.




(그림 3) DHCPv6 프리픽스 네트워크 구성모델

### 3.2 CGA

앞에서 IPv6 의 일반적인 주소 자동 설정 기능이 ND(neighbor discovery) 프로토콜에 의해 제공됨을 설명했다. 호스트는 라우터에서 제공받은 네트워크 프리픽스와 MAC 주소를 확장한 호스트 부분을 조합하여 IPv6 주소를 생성한 후, 반드시 그 주소의 유일성을 검사 해야 한다. 호스트가 자체적으로 IPv6 주소를 생성하는데 그 때 같은 네트워크에 있는 모든 노드들이 같은 네트워크 프리픽스를 사용하기 때문에 IPv6 주소가 동일할 가능성이 있다. IPv6 주소의 유일성을 검사할 때에도, 호스트의 주소가 계속 동일한 경우 개인 식별 프라이버시가 침해될 위협이 있는데 이 것을 막을 수 있는 ND 프로토콜 기능이 CGA 이다. CGA 는 공개키와 보조 파라메터 쌍을 입력값으로 하여 해쉬 연산을 한다. 그리고 그 해쉬 연산의 결과값에서 최상위 68 비트를 IPv6 의 IID 로 사용한다. 만약 매번 암호화의 결과가 동일하다면, 이 경우에도 개인 식별 프라이버시 침해 위협이 사라지지 않지만 CGA 의 경우 입력 값인 보조 파라메터가 랜덤한 값으로 바뀌게 되어 있기 때문에 개인 식별 프라이버시문제를 해결할 수 있다. 하지만 네트워크 프리픽스 부분은 암호화되지 않기 때문에 위치 프라이버시 문제는 해결되기 어렵다.

### 3.3 PE

PE 는 Interface identifier(IID)를 랜덤하게 구성하는 방식이다[5]. 이 방식은 주기적으로 랜덤한 IID 를 생성해 주는 것을 목적으로 한다.

PE 가 IID 를 랜덤하게 생성하는 방식은 저장공간(stable storage)이 존재하는지 여부에 따라 두 가지로 나뉘어 진다. 먼저 저장공간이 존재하는 경우, 상태 히스토리를 저장할 수 있어서 이전 상태(previous state)를 알고리즘의 반복(iteration) 연산 시에 입력 값으로 이용할 수 있다. 이전 상태가 없는 경우에는 랜덤한 값이 입력된다. 저장공간이 존재하지 않는 경우에는 이전 상태는 없지만, 유저 ID(user identity)나 시리얼 넘버같이 호스트의 고유한 구성정보를 이용하여 랜덤한 IID 를 생성한다.

일반적인 주소 자동 설정 기능에서는 호스트 자신의고 유한 MAC 주소를 64 비트로 확장하여 IID 를 구성함으로써 호스트 부분이 계속 동일하게 유지되었고, 그로 인해 개인 식별 프라이버시 침해 위협이 있었다. PE 의 경우 IID 를 랜덤하게 생성하여 주소의 동일성 문제를 해결 할 수 있다. 하지만, PE 도 네트워크 프리픽스 부분이 수정되지는 않기 때문에 위치 프라이버시 문제는 해결되기 어렵다.

### 3.4 CPP

[7]은 위치 프라이버시 침해를 막기 위해 네트워크 프리픽스 영역을 안전하게 암호화시키는 CPP 를 제안했다. CPP 는 IPv6 주소에서 처음 64 비트인 네트워크 프리픽스 부분을 암호화한다. 이 암호화는 라우팅 도메인의 라우터만 해독할 수 있다. 적절한 키를 가진 라우터만 패킷의 CPP 목적지 주소를 알 수 있어서 그 패킷을 어떻게 이동시킬 지 결정할 수 있다.

CPP 가 위치 프라이버시를 제공하는 영역은 privacy domain(PD)로 표현할 수 있다. CPP 는 PD 의 라우터들이 협의(compromise)되어 있는 한 계속해서 위치 프라이버시를 제공한다.

CPP 라우터는 새로운 키를 주기적으로 획득할 수 있어서 네트워크 프리픽스의 동일성은 줄일 수 있지

만, 호스트 부분은 계속 동일하게 유지될 가능성이 있다. 따라서 트래픽 분석의 여지가 남게 되고, 개인 식별 프라이버시에의 위협 요소들이 완벽하게 제거되기 어렵다.

## 4. 분석

<표 1> privacy 문제 해결방안

| | 특징 | Location privacy | Identity privacy |
|---|---|---|---|
| DHCPv6 | 서버 사용 | O | O |
| CGA | IID 암호화 | X | O |
| PE | 주기적으로 랜덤한 IID 생성 | X | O |
| CPP | 네트워크 프리픽스 암호화 | O | X |

<표 1>에서는 앞서 나왔던 프라이버시 문제의 해결방안별 특징이 나와있고, 그에 따라 해결되는 프라이버시 문제의 종류에 대해 체크되어 있다.

DHCPv6 는 주소 이용 효율성이 증가하고 위치 프라이버시와 개인 식별 프라이버시를 모두 지킬 수 있지만 따로 서버가 필요하며 구성 관리가 복잡하고, 대규모의 데이터 베이스를 구축해야 하는 단점이 있다.

CGA 는 IID 를 랜덤하게 암호화해서 개인 식별 프라이버시 침해 위협을 줄였지만 네트워크 프리픽스는 그대로 유지되어 위치 프라이버시에서는 위협이 그대로 남게 되었다.

PE 는 주기적으로 랜덤한 IID 를 생성함으로써 개인 식별 프라이버시 문제를 해결했지만, 이 방식도 위치 프라이버시 문제는 해결되지 않았다.

CPP 는 네트워크 프리픽스 부분을 암호화해서 위치 프라이버시를 지켰지만, MAC 주소를 이용한 호스트 부분은 동일성이 유지되어 개인 식별 프라이버시에 문제가 남았다. 또, 퍼포먼스가 감소하는 점과 CPP 서버가 추가적으로 필요하다는 것이 단점으로 작용할 수 있다.

## 5. 결론

지금까지 본 논문에서는 주소 자동 설정 방식에서 발생하는 프라이버시 문제와 그 해결방안에 대해 살펴 보았다. 각각의 해결방안들은 각각 장단점이 있어, 관리자의 관리환경에 적합한 기술을 사용하는 것이 관리자의 중요한 선택이 될 것이다.

또한 개인 식별 프라이버시와 위치 프라이버시 두 문제를 동시에 해결하면서, 기존에 제시된 프라이버시 해결문제의 단점을 보완할 수 있는 새로운 기술에 대해 적극적인 연구가 필요할 것이다.

## ACKNOWLEDGMENT

본 논문은 중소기업청에서 지원하는 2010 년도 산학연공동기술개발사업(No. 00044301)의 연구수행으로 인한 결과물임을 밝힙니다

## 참고문헌

[1] 김정욱, “IPv6 보안 취약점에 대한 분석 및 시나리오 기반 실험”, 전남대학교대학원, 석사학위논문, 2008

[2]박기태, “IPv6 의 보안기능을 강화하는 Secure ND protocol 구현”, 정보과학회지 2(1) 13-18, 2005

[3] Stephen Groat, “The privacy implications of stateless IPv6 addressing” , CSIIRW , 2010

[4] S. Thomson, “IPv6 Stateless Address Auto configuration” RFC2462, Dec 1998

[5] T. Narten, “Privacy Extensions for Stateless Address Autoconfiguration in IPv6” RFC3041, Jan 2001

[6] 이상도, “IPv6 프리픽스 할당 메커니즘에 관한 기술 분석”, 전자통신동향분석 제 19 권 제 1 호 통권 85 호 (2004. 2) pp.43-51 1225-6455, 2004

[7] Jonathan Trostle, “Cryptographically protected prefixes for location privacy in IPv6”, LNCS 746-748, 2005