[전송통신] 상태 비보존형 IPv6 주소 자동설정 표준화 연구 동향

본고에서는 최근 국제 표준화 기구 IETF(Internet Engineer Task Force) 내 6MAN(IPv6 Maintenance) WG에서 RFC7219로 표준화가 완료된 새로운 상태 비보존형 IPv6 주소 자동설정(IPv6 Stateless Address Autoconfiguration, SLAAC) 기술을 소개하고 이와 관련하여 7월 체코 프라하에서 개최된 93차 IETF 회의에서 다뤄진 새로운 이슈 및 향후 전망을 소개하고자 한다.

IPv6 주소 자동설정 기술 개요

IPv6 주소 자동설정 기능은 휴대 전화, 무선 장치, 가전 기기 등과 같은 새로운 장치들에 대한 “플러그 앤 플레이” 인터넷 설치가 가능하도록 한다. IPv6 주소를 생성하는 자동설정 방식에는 두 가지가 있는데, DHCPv6(Dynamic Host Configuration Protocol version 6) 서버에서 테이블을 관리하면서 IPv6 주소를 분배하는 상태 보존형(Stateful) 자동설정과 특정서버가 관리하지 않고 라우터에서 제공되는 네트워크 프리픽스 64비트(상위)와 IEEE-defined 64-bit Extended Unique Identifier(EUI-64)기반의 인터페이스 식별자(Interface Identifier, IID) 64비트(하위)를 합하여 128비트 주소를 생성하는 상태 비보존형(Stateless) 자동설정이 있다.

이 중에서 본고에서 다루고자 하는 것은 IPv6 주요 기능으로 RFC4862로 표준화된 상태 비보존형 자동설정(SLAAC)이다. 네트워크 프리픽스와 EUI-64기반 IID를 이용한 SLAAC 방식을 아래와 같이 예들 들어 설명한다. 먼저, EUI-64 형식의 이해가 필요한데 이는 이더넷, 와이파이 등의 하드웨어 정보인 48비트 Media Access Control(MAC) 주소를 바탕으로 생성된다. 먼저, MAC 주소의 최상위 일곱 번째 비트를 0인경우 1로, 1인 경우 0으로 변경한다. 그 다음, MAC 주소의 중간 부분에 16진수 FFFE(16비트)를 삽입하여 EUI-64를 생성하고 이를 IPv6 주소 생성을 위한 하위 64비트, IID로 사용하는 것이다. 예를 들어, IPv6 호스트가 접속한 서브넷의 라우터에서 제공되는 네트워크 프리픽스가 “2001:1234:AD:5555/64”라 가정하고, IPv6 호스트의 MAC 주소가 “001C:C4CF:4ED0”이라고 가정하면, IID는 “021C:C4FF:FECF:4ED0”가 되어 최종 생성되는 IPv6 주소는 “2001:1234:AD:5555:21C:C4FF:FECF:4ED0”가 된다.

안정적인 IID 생성을 통한 새로운 SLAAC 표준화

SLAAC는 보안(Security) 및 사생활보호(Privacy) 측면에서 두 가지 문제점이 제기되어왔다. 첫 번째는, SLAAC 공격, 즉 거짓 라우터를 설정해 IPv6 호스트에 IP 주소 자동설정을 계속 요청하게 된다. 이런 경우 IPv6 호스트는 IPv6 주소를 생성하는데 프로세서 자원의 대부분을 사용해 다른 서비스를 지속할 수 없게 된다. 특히, IPv6 호스트가 중요한 서비스를 제공하는 서버라면 서비스거부(Denial of Service, DoS) 공격이 쉽게 이뤄질 수 있게 되는 것이다. 결국, IPv6는 IP 주소의 구성이 매우 복잡하기 때문에 자동생성이라는 기술을 필요로 하게 되었는데, 이 기술을 악용하면 쉽게 DoS 공격이 가능하게 되어 부작용을 낳게 된 것이다. 두 번째로, 이미 언급한대로 SLAAC는 IPv6 호스트의 MAC 주소, 즉 하드웨어 정보를 기반으로 하는 EUI-64 형식의 IID를 사용하다 보니 호스트의 활동 경로를 추적 가능하게 되는 문제도 발생하게 된다. 또한, IPv6 호스트의 경우 MAC 주소의 상위 24비트를 통해 사용 중인 기기의 종류를 판별할 수 있는 식별값, 제조사, 모델번호 등이 포함되어 있기 때문에 IPv6 주소를 통해 사용자의 의사와 상관없이 공격자에게 사용 중인 하드웨어의 특정 정보를 제공할 수 있으며 이를 통해 IPv6 주소의 특정 패턴을 검색하는데 걸리는 시간을 줄일 수 있게 된다. 이러한 두 가지 문제를 해결하고자 표준문서 RFC3041(Privacy Extensions for Stateless Address Autoconfiguration in IPv6)이 제정되었다.

하지만 최근 들어, 두 번째 문제인 IID 측면에서 발생하는 보안 및 사생활보호 문제를 해결할 뿐만 아니라 IPv6 호스트가 접속된 서브넷에서 주소가 안정적으로 사용될 수 있도록 IPv6 호스트의 IID로 EUI-64 형식을 사용하던 것을 의사난수(Pseudorandom) 함수를 이용해 생성(Generating)하는 방식으로 표준화가 이루어졌고 2014년 4월에 RFC7217(A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration)로 제정되었다. 이 표준문서에서는, IPv6 호스트가 이동하여 다른 서브네트에 접속하여 다른 네트워크 프리픽스를 받게 되면, 자신이 가지고 있는 몇 가지 정보들과 의사난수 함수를 이용하여 IID를 랜덤으로 생성한다. 생성된 IID를 이용하여 보안과 사생활보호 문제를 해결할 수 있는 안정적인 IPv6 주소를 자동적으로 생성하게 되는 것이다.

새로운 SLAAC 표준 기술 적용을 위한 노력 및 향후 전망

RFC7217에서 제시하는 안정적인 IID 생성 기반 SLAAC 방식은 기존 RFC4862을 업데이트하거나 변경하는 것이 아닌 상호운용성(Interoperability)를 유지하는 또 다른 방식의 SLAAC이며, 기본 링크 로컬 주소, 글로벌 주소, 유니크 로컬 주소 생성에 모두 적용 가능하다. 6MAN WG에서는 이러한 내용을 다른 WG과 기존 표준 문서들에 권고(Recommendation)하기 위해 현재 WG 표준 문서인 “Recommendation on Stable IPv6 Interface Identifiers”를 작업 중에 있으며 이번 7월 체코 프라하에서 열린 93차 IETF 회의에서 이를 논의하였다.

아울러, 이번 회의에서는 안정적인 IID 생성에 대한 또 다른 이슈들도 논의 되었는데 그 중 하나가 마이크로소프트사에 의해 발표된 “Implications of Randomized Link Layers Addresses for IPv6 Address Assignment“ 기술이 있다. RFC7217의 IID 생성방식이 안정성(Stablity)에 중점을 두었다면 마이크로소프트사가 제안한 IID 생성 방식은 48비트 MAC 주소 자체를 난수화 함으로써 사생활보호(Privacy) 측면에서의 강화를 위한 새로운 표준 제안이라 할 수 있다. 아울러, IPv6 호스트가 어떤 특정 서브넷에 방문했을 때 익명성(Anonymity)을 보장하는 기능은 물론 동일한 서브넷에 있다 하더라도 주기적으로 MAC 주소를 난수화하는 함으로써 자기 자신을 숨기는 기능을 포함하고 있다.

향후 안정적인 IID 생성을 위한 추가적인 기술들이 제안될 것으로 예상되며 이러한 제안 기술들은 현재 논의 중인 WG 문서 “Recommendation on Stable IPv6 Interface Identifiers”의 내용에 포함되거나 별도의 WG 문서로 진행될 예정이다.

김평수 (한국산업기술대학교 전자공학과 교수, pskim@kpu.ac.kr)