보안공학연구논문지 *Journal of Security Engineering*
Vol.12, No.3 (2015), pp.239-246
http://dx.doi.org/10.14257/jse.2015.06.02

사물인터넷에서의 사생활 보호를 위한 IPv6 주소 설정

이종혁1)

IPv6 Address Configuration for Privacy Protection in the IoT

Jong-Hyouk Lee[1)]

요 약

사람과 사물, 사물과 사물 간의 초연결성을 바탕으로 새로운 인터넷 환경을 제공하는 사물인터넷에 대한 관심이 높아지고 있다. 본 논문에서는 사물인터넷에서 네트워크 프로토콜로 사용되는 IPv6의 사생활 보호 기법들에 대해 분석한다. 사물인터넷기기에 설정 된 IPv6 주소는 인터페이스 식별자를 생성하는 기법에 따라 사생활을 보호 할 수 있는 강도가 달라지며, 같은 기법이라 할지라도 인터페이스 식별자의 변경(재생성)에 따라 보호 강도가 달라진다.

핵심어 : 사물인터넷, 사생활 침해, 위치 추적, 차세대 인터넷 주소

Abstract

The Internet of Things (IoT), which provides the new Internet environment based on hyperconnectivity between human beings and things, and between things and other things, is gaining attention. In this paper, privacy protection mechanisms of IPv6, which is a network protocol for the IoT, are analyzed. The strength of privacy protection for an IPv6 address configured on an IoT device differs depending on interface identification generation mechanisms and the strength also differs due to a frequency of an interface identification change (regeneration) even in the same mechanism.

Keywords : Internet of Things, Privacy, Location Tracking, Next-Generation Internet Address

1. 서론

시장조사기관인 가트너는 2020년 사물인터넷(Internet of Things, IoT)기기가 260억대에 이를 것으로 예측하고 있다[1]. 사물인터넷 시대에는 가정에서 사용하는 가전제품에서 부터 도로 위를 달리는 자동차, 공장의 센서나 작동기까지 거의 모든 사물에 센싱과 컴퓨팅 능력이 부여 되고 통신 기능이 탑재 된다. 시장파괴적인 영향력을 가지는 사물인터넷은 해외 주요 IT 기업뿐만 아니라 가전, 기계, 항공, 금융 등 거의 모든 분야의 기업들이 구체적인 투자계획을 가지고 연구개발을 진행하고 있다. 국내에서도 사물인터넷에 대한 중요성을 파악하고 2014년 5월 미래창조과학부는 'IoT에

접수일(2015년05월01일), 심사의뢰일(2015년05월02일), 심사완료일(1차:2015년05월16일)
게재확정일(2015년06월04일), 게재일(2015년06월30일)

[1]330-720 충청남도 천안시 동남구 상명대길 31, 상명대학교 컴퓨터공학과.
email: jonghyouk@smu.ac.kr

* 본 논문은 2013학년도 상명대학교 교내연구비를 지원받아 수행하였음 (2013-A000-0319).

ISSN: 1738-7531 JSE

관한 기본계획'을 수립하고 2020년까지 국내 사물인터넷 시장을 30조원 규모로 육성하겠다고 발표하였다.

웨어러블기기(Wearable Devices)에서 부터 차량에 설치 된 각종 통신기기는 사물인터넷 시대에 사용자의 이동에 따라 그 편리함을 제공한다. 손목에 착용하는 스마트워치와 같은 웨어러블기기는 사용자의 혈압, 맥박수, 호흡수 등을 측정하고 병원의 헬스케어 센터와 같이 원격지로 실시간 전송할 수 있는 기능을 가진다. 지능형 교통 시스템의 핵심이 될 차량통신 기술은 효율적이고 안전한 차량운행을 위해 차량과 차량, 차량과 인프라간의 실시간 데이터 통신을 수행한다. 하지만 이러한 메시지들은 데이터통신 관점에서 본다면 어떠한 형태로든 식별자를 가져야 하며 이러한 식별자는 메시지를 주고받는 객체를 인식하고 추적하는데 사용 될 수 있다. 기존 인터넷 환경에서는 메시지를 주고받는 객체가 PC 와 같은 기기였지만, 사물인터넷 환경에서는 사용자와 밀접하게 상호작용을 하는 개인화 된 객체의 수가 증가하게 된다. 즉, 개인화 된 웨어러블기기나 차량에서 전송되는 메시지 식별자와 위치정보를 결합한다면 개인의 사생활을 손쉽게 침해 할 수 있다.

본 논문은 사물인터넷 환경에서의 사생활 침해에 관해 연구한다. 특히, 사물인터넷의 기반 기술 중 하나인 IPv6 주소 인식/추적을 통한 사생활 침해와 이를 방지하기 위한 다양한 인터페이스 식별자 생성방법에 대해 살펴본다.

본 논문의 구성은 다음과 같다. 2장에서 사물인터넷에서 발생 할 수 있는 사생활 침해와 공격에 대해서 살펴보고 제 3장에서 사물인터넷에서 네트워크 프로토콜로 사용되는 IPv6에 대해 살펴본다. 제 4장에서 사생활 보호를 위한 IPv6 인터페이스 식별자 생성기법에 대한 분석을 수행하고, 제 5장에서 결론을 맺는다.

2. 사물인터넷에서의 사생활 침해와 공격

사물인터넷 환경에서는 실생활에서 쉽게 접할 수 있는 기기들이 주변정보를 센싱하고 가공하며 통신기능을 가지게 된다. 인간의 삶을 편리하고 윤택하게 만들 수 있는 이러한 기술은 반대로 공격자에 의해 악의적으로 이용 될 수 있다. 본 논문에서는 3가지의 예상되는 사생활 침해에 대해서 살펴본다.

웨어러블기기는 사용자가 착용하는 컴퓨팅 기기를 의미하며 갤럭시 기어, 애플 워치와 같이 손목에 착용하거나 구글 글래스와 같은 안경 형태의 기기, 전자문신과 같은 신체 부착형 등이 있다. 이러한 웨어러블기기는 신체 정보를 획득하거나 사용자에게 필요한 정보를 전달하는데 사용 될 수 있다. 특히, 블루투스나 근거리무선통신 기술이 탑재 되어 외부의 기기(예를 들어, 사용자의 스마트폰)와 데이터를 주고받게 된다. 하지만 웨어러블기기에서 전송 되는 데이터는 무선으로 브로드캐스트가 되기에 간단한 무선기기만 있다면 웨어러블기기에서 발생하는 데이터를 손쉽게 가로채 그 내용을 분석 할 수 있다. 최근 연구결과[2]에 따르면, 많은 웨어러블기기들이 데이터를 전송하는데 있어서 변경되지 않는 MAC 주소를 사용하고, 데이터를 암호화하여 전송하지 않기 때문에 기기의

식별자나 심지어 사용자의 이름까지도 무분별하게 노출이 된다. 이러한 정보를 바탕으로 웨어러블 기기를 착용한 특정 사용자의 이동을 실시간으로 파악 할 수 있으며, 축척된 이동정보를 바탕으로 사용자의 이동 패턴을 생성 할 수 있어 추가적인 범죄에 이용 될 수 있다. 또한, 암호화 되지 않은 체 데이터가 전송 된다면, 웨어러블기기로 부터 측정 된 사용자의 생체정보와 같은 주요 정보가 고스란히 노출 되어 심각한 사생활 침해를 가져 온다.

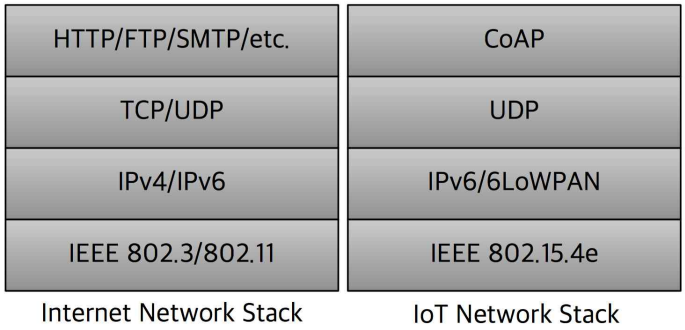
가정 내 모든 기기들이 내부적으로 연결 되고 인터넷을 통해 원격 모니터링, 제어가 가능케 하는 스마트홈(Smart Home)은 사물인터넷을 구성하는 대표적인 기술이다. 퇴근 시간이 되면 거주자의 위치정보를 바탕으로 집에 도착하기 직전에 따뜻한 밥을 취사하여 준비하고 목욕물 또한 준비한다. 냉장고에 우유나 달걀과 같은 식료품이 떨어지면 자동으로 주문을 하는 기능도 도래하게 될 스마트홈에서는 일상화 된다. 또한 장기간 출장 시에는 자동으로 환기를 시키거나 냉난방을 조절하는 기능 등을 제공하게 된다[3]. 하지만, 이러한 스마트홈의 편리성은 공격자에게도 편리함을 가져다준다. 예를 들어, 스마트홈의 냉난방, 전기 사용 모니터링 시스템의 해킹을 통해 집안에 사람이 있는지 없는지 확인이 가능하며 가정 침입을 위해 창문을 개방 시키는 공격을 수행 할 수 있다. 혹은 냉장고와 연결 된 식료품 자동 주문 시스템을 해킹하여 불필요한 주문을 일으키거나 결재 정보를 획득하여 악의적으로 사용 할 수도 있다.

차량네트워크는 교통을 원활하게 하고 안전한 차량 운행이 이루어질 수 있도록 차량과 차량 사이의 통신과 차량과 인프라간의 통신을 수행한다. 차량에서 전송 되는 메시지는 차량의 이동방향, 속도, 종류 등의 정보와 함께 차량 식별자 정보를 포함하게 된다. 이러한 정보는 공격자로 하여금 간단한 무선송수신기만 있다면 특정 차량에서 발생하는 메시지를 수집, 분석함으로써 차량을 식별하고 이동경로를 추적 할 수 있게 한다[4]. 또한 차량 간 전송되는 메시지가 암호화 되지 않고 전송 된다면 메시지를 악의적으로 변조하여 차량이 급정거하게 만들거나 임의의 악성코드를 넣어 차량의 운행을 멈추도록 할 수 있다.

3. 사물인터넷과 IPv6

사물인터넷의 주요한 동작 특성은 기기가 주변을 센싱하고 센싱 된 데이터를 직접 가공하거나 자신과 연결 된 다른 기기에 전송한다. 이렇게 전송 되는 데이터는 기존 인터넷과는 다른 초연결성을 지니는 새로운 형태의 네트워크이다. 사물인터넷을 네트워크 관점에서 본다면, 기존 인터넷과 다른 네트워크 스택을 가지게 된다. 아직까지 전세계적으로 표준화 된 사물인터넷 네트워크 스택은 없지만, IEEE, IETF, ITU-T 등의 국제표준화단체에서 이러한 표준 네트워크 스택과 연동기술을 만들기 위해 작업이 진행 중이다. [그림 1]은 기존 인터넷 네트워크 스택과 IEEE, IETF에서 제안하고 있는 프로토콜로 이루어진 사물인터넷 네트워크 스택의 차이를 보여 준다[5].

ISSN: 1738-7531 JSE



[그림 1] 기존 인터넷과 사물인터넷의 네트워크 스택 비교

[Fig. 1] Comparison of the Internet Network Stack and IoT Network Stack

기존 인터넷 환경과 달리 사물인터넷은 경량화 된 기기(노드)로 이루어지기 때문에 저전력을 소모하면서도 경량화 된 메시지 구조를 가져야 한다. 그에 따라, 물리계층과 링크계층을 정의하는 IEEE 802.15.4e 표준[6]과 IPv6로 대표되는 네트워크 계층와의 연동을 제공하는 6LoWPAN[7]이 사용된다. 전송계층에서는 자원을 많이 소요하는 TCP가 아닌 UDP를 사용하며, 응용계층 프로토콜로 CoAP[8]를 사용한다. 사물인터넷 환경에서는 HTTP 기반 웹데이터 전송 보다는 저전력을 지향하며, 주로 센서에 의해서 수집된 데이터를 전달 할 목적으로 개발 된 CoAP 프로토콜을 사용한다. CoAP는 HTTP에 비해 경량화 된 메시지 구조와 동작을 가지는 것 이외에도 비동기적인 요청과 응답 구조로 통신의 유연함을 제공한다.

네트워크계층 프로토콜인 IPv6는 128비트의 주소공간을 제공한다. 기존 IPv4는 32비트의 주소공간을 제공하기 때문에 기하급수적으로 증가하는 컴퓨팅기기에 주소를 할당하기 제약사항이 있다. 그에 반면 IPv6는 약 3.4×10^{38} 개의 주소를 할당 할 수 있기에 거의 무한대라고 할 수 있다. 이러한 주소공간의 확장뿐만 아니라 IPv6는 IPv4와 비교하여 다음과 같은 특징을 가진다.

- 주소 자동 설정: DHCP 서버 등에 의해 주소를 할당 받는 것이 아니라, 네트워크에 접속하면 노드 스스로 IPv6 주소를 자신의 인터페이스에 설정한다. 이러한 주소 자동 설정 기능은 사용자가 수동으로 주소를 설정 할 수고를 덜어주며 DHCP 서버와 같이 특정 서버와 네트워크로 연결 되지 않는 상황에서도 노드 스스로 주소를 설정하고 통신이 가능케 한다.
- 효율적인 라우팅: 단순하고 고정 된 크기의 헤더를 가지며 라우팅에 필요한 추가적인 기능들은 확장헤더를 이용해 필요한 추가 기능들을 제공한다.
- 플로우 레이블링: 트래픽을 플로우로 구분하여 특정 플로우에 높은 우선순위로 처리하거나 서비스 품질을 높일수 있다.
- 강화된 보안: IPsec 적용으로 패킷의 출처 인증, 데이터 무결성 및 기밀성을 보장 할 수 있다.
- 이동성: MIPv6, PMIPv6 등을 이용해 호스트 혹은 네트워크기반의 이동성을 보장 할 수 있다.

사물인터넷 노드의 네트워크 스택을 구성하는 프로토콜들은 모두 식별자를 가지고 있지만, 특히

IPv6는 네트워크 계층의 프로토콜이기에 그 중요성이 높다. 예를 들어, 물리/링크계층의 식별자는 단일 홉 혹은 같은 네트워크 내에서만 사용이 가능한 식별자이며, 전송계층의 식별자나 응용계층의 식별자는 네트워크 계층에서의 보안 프로토콜을 이용해 암호화 할 수 있다. 하지만, 데이터 전달에 이용되는 네트워크 주소(즉, IPv6 주소)는 암호화 할 수 없으며 그 특성상 전 세계에서 유일한 주소로 식별이 가능하다.

4. 사생활 보호를 위한 IPv6 인터페이스 식별자

4.1 IPv6 주소에 대한 공격

사물인터넷에서의 노드들은 하나 이상의 IPv6 주소를 가지고 다른 노드들과 데이터를 주고받는다. 따라서 IPv6 주소는 다음과 같은 공격에 의해 사생활 침해를 유발 할 수 있다.

- 상관관계 분석
- 위치 추적
- 주소 스캐닝
- 노드 취약성 판별

노드의 IPv6 주소는 해당하는 노드를 식별 할 수 있는 식별자로 사용이 될 수 있으며, 식별자를 이용해 노드가 발생하는 트래픽 량을 모니터링하거나 어떠한 주기를 가지고 트래픽을 생성하는지 파악하여 실제 데이터 패킷의 내용이 암호화 되어 있다 할지라도 어떠한 용도로 사용되는 사물인터넷 노드인지를 유추 할 수 있다. 또한, 노드가 스마트폰, 웨어러블기기, 자동차와 같은 경우라면 실제 사용자의 이동을 추적하거나 이동 패턴을 분석하여 특정한 시간대에 어떠한 장소로 이동할지를 예측하는데 사용 될 수 있다. IPv6는 IPv4에 비해 약 2^{96}배의 주소공간을 가진다. 하지만 IPv6 주소 형성과정 특징(64비트 네트워크 프리픽스 정보와 64비트 인터페이스 식별자와의 결합)으로 인해 특정한 주소 영역에 포함되는 노드를 주소 스캐닝을 통해 찾아 낼 수 있다. 이러한 주소 스캐닝은 공격 대상이 되는 노드의 위치를 특정 지을 때 유용하게 사용 될 수 있다. IPv6 주소를 생성 할 때 사용되는 노드 식별자는 네트워크 인터페이스 생산업체의 정보뿐만 아니라 운영체제, 소프트웨어의 종류와 같은 정보를 제공 할 수 있으며, 이러한 정보는 해당하는 노드가 가지고 있는 취약성을 판별하는데 이용 될 수 있다.

4.2 IPv6 주소 설정을 위한 인터페이스 식별자 생성 기법

IPv6 주소 형성과정에서 좌측 64비트는 네트워크에 의존적인 정보이기 때문에, 사생활 침해 공격을 방지하기 위한 기법들은 주로 우측 64비트 인터페이스 식별자를 생성하고 사용하는 것에 초

점을 맞추고 있다.

- IEEE 식별자[9]: IEEE 802 48비트 MAC 주소를 이용하거나 IEEE EUI-64 식별자를 이용해 64 비트의 식별자를 생성해 내는 기법
- CGA 식별자[10]: IPv6의 NDP 프로토콜[11]을 보호하기 위해 사용되는 SEND 프로토콜[12]과 함께 사용 되며 노드의 공개키와 다른 정보를 단방향 해시함수를 이용해 식별자를 생성
- 랜덤 식별자[13]: 윈도우 운영체제에서 사용되는 랜덤 식별자 생성 기법
- 임시 식별자[14]: MD5 를 이용해 랜덤 식별자를 만들어 내며 만들어진 랜덤 식별자는 주어진 시간 (예를 들어 24시간, 1시간, 10분 등)만 사용하고 다시 식별자를 생성하는 기법

[표 1] IPv6 인터페이스 식별자 생성 기법 비교

[Table 1] Comparison of IPv6 Interface Identification Generation Mechanisms

기법	상관관계 분석	위치 추적	주소 스캐닝	노드 취약성 판별
IEEE 식별자	가능	가능	가능	가능
CGA 식별자	가능	어려움	어려움	어려움
랜덤 식별자	가능	가능	어려움	어려움
임시 식별자	가능	어려움	어려움	어려움

[표 1]은 IPv6 인터페이스 식별자 생성 기법에 따라 달라지는 공격에 대한 대응을 나타낸다. [15]에서 나타나는 것처럼, 가장 기본적인 IEEE 식별자 생성은 모든 공격에 대해 취약함을 보인다. 한번 생성한 IEEE 식별자는 계속해서 사용되기 때문에 공격자에게 비교적 쉽게 상관관계 분석을 당하거나 위치 추적, 주소 스캐닝, 노드 취약성 판별에 사용 될 수 있다. 이에 반해, CGA 식별자 생성은 상관관계 분석에는 취약하지만, 위치 추적, 주소 스캐닝, 노드 취약성 판별에 강건한 모습을 보인다. CGA 식별자는 노드의 공개키와 노드가 가지고 있는 다른 정보들을 바탕으로 해시값을 만들고 만들어진 해시값을 이용해 64비트의 식별자를 만들어 사용한다. 따라서 상관관계 분석 공격은 식별자로 만들어진 IPv6 주소가 사용되는 기간이다. 하지만, 인증서를 사용하는 SEND 프로토콜과 함께 사용되기 위해서 만들어진 CGA 는 공개키가 요구 되며, 저전력 경량화 된 사물인터넷 노드에서는 그 사용이 제한적 일 수밖에 없다. 랜덤 식별자 방식은 표준화 되지 않은 방법으로 윈도우 운영체제에서 사용되고 있다. 주소 스캐닝과 노드 취약성 판별에는 강건하지만, 상관관계 분석 공격이나 위치 추적 공격에는 취약하다. 임시 식별자를 이용하는 방법은 오직 상관관계 분석 공격에만 취약한 모습을 보인다. 생성된 식별자는 임의의 식별자가 되며 오직 주어진 시간만큼만 사용 되고 새로운 식별자로 변경되기 때문에 다른 식별자 생성 기법에 비해 안전성이 높다고 할 수 있다.

임시 식별자를 이용해 새로운 주소를 주기적으로 생성해 낸다면 상관관계 분석 또한 어렵게 만들 수 있다. 하지만 새로운 식별자 생성을 통한 주소 변경은 이전 주소로 전송되는 데이터를 받지

못하는 상황을 만들어 내기에 패킷이 유실 되거나 상대방으로 하여금 연결이 끊기거나 노드에 이상이 있는 것으로 오판하게 할 수 있다. 따라서, [4]에서 소개하는 것과 같이 사생활 보호를 위해 새로운 식별자를 만드는 것과 데이터 통신 특성, 이동성을 가지는 기기라면 이동성까지도 고려하여 식별자를 생성하고 주소를 설정해야 한다.

5. 결론

본 논문에서는 초연결성을 제공하는 사물인터넷에서의 사생활 침해와 IPv6 주소 생성 관점에서의 사생활 보호 기법들을 살펴보았다. IPv6의 주소 생성 특징으로 인해 우측 64비트를 차지하는 인터페이스 식별자 생성 방법은 통신상에서 이루어 질 수 있는 사생활 침해 공격에 직접적으로 연관 된다. 인터페이스 식별자 생성 방법에 따라 사생활 침해 공격에 대한 보안 강도가 달라지며, 같은 기법이라 할지라도 식별자의 변경(재생성)에 따라 보호 강도가 달라 질 수 있음을 알 수 있었다. 마지막으로 사물인터넷 네트워크 스택의 네트워크 계층은 IPv6 만이 단독으로 사용되지 않고 6LoWPAN이 함께 사용되기에 6LoWPAN과의 연동을 통해 더욱 강건한 IPv6 인터페이스 식별자 생성 및 주소 설정 기법이 요구 된다.

References

[1] https://www.gartner.com/doc/2625419/forecast-internet-things-worldwide-, November 18 (2013).

[2] http://www.realwire.com/releases/Sniffing-and-tracking-wearable-tech-and-smartphones, May 22 (2015).

[3] H.-J. Lee, Smart Home based on the Internet of Things, Information and Communications Magazine, (2015), Vol. 32, No. 4, pp. 44-49.

[4] J.-H. Lee, G. Lee, and S. Pack, Pseudonyms in IPv6 ITS Communications: Use of Pseudonyms, Performance Degradation, and Optimal Pseudonym Change, International Journal of Distributed Sensor Networks, (2015), vol. 2015, pp. 1-7.

[5] R. Sutaria and R. Govindachar, Making sense of interoperability: Protocols and Standardization initiatives in IOT, Proceedings of the International Workshop on Computing and Networking for Internet of Things (CoMNet-IoT), (2013) January 3-6; Mumbai, India.

[6] https://standards.ieee.org/findstds/standard/802.15.4e-2012.html, (2012)

[7] J. W. Hui and P. Thubert, Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks, IETF RFC 6282, September (2011).

[8] Z. Shelby, K. Hartke, and C. Bormann, The Constrained Application Protocol (CoAP), IETF RFC 7252, June (2014).

[9] M. Crawford, Transmission of IPv6 Packets over Ethernet Networks, IETF RFC 2464, December (1998).

ISSN: 1738-7531 JSE

[10] T. Aura, Cryptographically Generated Addresses (CGA), IETF RFC 3972, March (2005).

[11] T. Narten, E. Nordmark, and H. Soliman, Neighbor Discovery for IP version 6 (IPv6), IETF RFC 4861, September (2007).

[12] J. Arkko, J. Kempf, B. Zill, and P. Nikander, SEcure Neighbor Discovery (SEND), IETF RFC 3971, March (2005).

[13] https://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/sag_ip_v6_imp_addr7.mspx?mfr=true, (2015).

[14] T. Narten, R. Draves, and S. Krishnan, Privacy Extensions for Stateless Address Autoconfiguration in IPv6, IETF RFC 4941, September (2007).

[15] A. Cooper, F. Gont, and D. Thaler, Privacy Considerations for IPv6 Address Generation Mechanisms, draft-ietf-6man-ipv6-address-generation-privacy-05, April (2015).

Author

이종혁 (Jong-Hyouk Lee)

2010년 2월 : 성균관대학교 컴퓨터공학과 박사
2009년 6월 ~ 2012년 2월 : 프랑스 국립연구소 INRIA 연구원
2012년 3월 ~ 2013년 8월 : 프랑스 그랑제꼴 TELECOM Bretagne 조교수
2013년 9월 ~ 현재 : 상명대학교 컴퓨터공학과 조교수
관심분야 : 인증, 프라이버시, 멀웨어, 모바일 네트워크