Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.2, Apr. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.2.423

고정IP 기반의 IPv6를 이용한 사물인터넷 제품 추적 및 재고관리 시스템 제언

이 정 민,† 안 종 창,‡ 이 욱
한양대학교

The Proposal of IoT products tracking and inventory management system using IPv6 based on static IP

Jeong-min Lee,† Jong-chang Ahn,‡ Ook Lee
Hanyang University

요 약

IPv4 주소가 고갈됨에 따라 한계점을 해결하기 위해 나타난 IPv6 주소체계가 서서히 다양한 분야에서 활용되고 있다. 최근에는 다양한 사물과 네트워킹 할 수 있는 사물인터넷(IoT) 제품들이 등장하기 시작하였다. 사물인터넷이 많은 분야에 점차 적용되고 네트워킹 기술이 포함된 전자기기 보급이 증가함에 따라, 각 기기마다 IPv6의 IP주소를 부여받게 될 것이다. 사물조차도 주소를 가지게 되면서 IP주소 관리시스템이 더욱 중요하다. IP주소를 가지고 있는 전자기기가 더 이상 사용되지 않고 있을 때, 그 전자기기의 IP주소를 추적 및 회수하기 위한 보완된 물류관리시스템이 필요하다. 본 논문에서는, 사물인터넷 제품에 각각 고정된 IPv6의 IP주소를 할당하여 이러한 IP주소와 네트워크를 기반으로 한 위치기반서비스를 이용하여 각 제품의 현재 위치를 추적하고, 창고 내의 제품을 관리하고자 한다. 필요시 IP 주소를 회수할 수 있는 새로운 물류추적 및 재고관리 시스템을 제언한다.

ABSTRACT

The IPv6 which solved the exhaustion problem of IPv4's IP address is going to be used for many kinds of industries. As a result, there are some products which can be connected to other connectable things, it called Internet of Things (IoT). With growing new propagated products including networking, each product can get an IP address of IPv6, which means it is possible that things also have their own IP addresses. Thus, IP address management system is more important and needs tracking and collecting system for unused products with IP addresses. This study suggests new distribution tracking and inventory management system for IoT products, which offers a current location of things and manages stocks in the warehouse with the static IP address and the location-based service.

Keywords: IoT product, IPv6, Distribution and inventory management system, IP address management system, System security

I. 서 론

정보통신 기술의 비약적인 발달로 멀리 떨어져 있는 사람들 간의 네트워크가 빠르게 형성되어 서로 정보를 주고받으며, 최근에는 주변에 있는 사물들을 네트워크로 연결시킬 수 있는 기술이 생겨나기 시작했다. 1991년 미국의 마크 와이저(Mark Weiser)는 사용자가 네트워크 또는 컴퓨터를 의식하지 않고 장소에 구애받지 않고 자유롭게 네트워크에 접속할 수 있는 유비쿼터스 환경(Ubiquitous environment)

접수일(2015년 2월 12일), 수정일(2015년 3월 31일), 게재확정일(2015년 3월 31일)
† 주저자, ljm10047@gmail.com
‡ 교신저자, ajchang@hanyang.ac.kr(Corresponding author)

이 도래할 것이라고 주장하였다[1]. 정보통신 기술의 발달로 인하여 생긴 사람 대 사람의 다중 네트워크화를 이룬 오늘날에 있어서 이것은 현실로 실현되고 있다. 특히 유비쿼터스 환경의 발전을 더욱 가속화시키는 정보통신기술 분야의 개념으로 사물통신(Machine to Machine; M2M)과 사물인터넷(Internet of Things; IoT)이 새롭게 부상하고 있는데, 미국의 시장조사기관인 가트너(Gartner)에 따르면 향후 10년간 유망할 것으로 예상되는 미래의 IT 분야로 IoT를 선정한 바 있다[2]. 세계이동통신사업자협회(GSMA)는 2020년까지 240억 개 이상의 기기들이 상호 연결되어, 통신사업자들이 1조 달러 이상의 신규수익을 창출할 것이라고 전망하였다[3]. Machina Research는 '13년 현재 약 200억 달러 수준에서 '20년 약 1조 200억 달러 수준으로 시장규모가 성장할 것으로 예측하고 있다. IDC와 MarketsandMarkets는 '20년 각각 8조 8,520억 달러, 1조 4,231억 달러로 전망하였으며, 가트너는 3,000억 달러 수준으로 예측하고 있다[2,3]. IoT의 시장전망에 다소 차이가 있으나, 한 가지 공통점은 IoT 시장은 상당히 희망적인 전망을 가진다는 것이다.

IoT는 기본적으로 사람 대 사람 뿐만 아니라 사물 대 사물의 통신을 해야 하며, 전 세계에는 수백억 개의 사물이 존재하기 때문에, 사물간의 네트워크를 구성하기 위해서는 다량의 IP(Internet Protocol) 주소가 필수적이다. 그러나 2011년 방송통신위원회에 따르면 아태지역 인터넷주소자원관리기관(APNIC)이 2011년 4월 15일부로 제한적으로 IPv4(Internet Protocol version 4) 주소를 할당하는 '최종 할당방식'을 시행하게 됨으로써, 사실상 주소 할당이 종료된다고 밝혔다[4]. 기본적으로 IPv4의 IP 주소 수는 2^32개(약 43억 개)인데 전 세계 인구 1인당 한 IP 주소를 가질 수 없는 수량이다. 기존 IP 개수는 한계가 있기 때문에 사용하고 있는 IP주소와 다른 새로운 형태의 주소가 필요하게 되었는데, 이것이 1994년 국제인터넷표준화기구(IETF)가 채택한 IPv6(Internet Protocol version 6)이다. 이 IPv6의 등장으로 인하여 기존의 IPv4의 제한적인 주소 할당 문제를 해소할 수 있게 되었다.

IoT의 시장성과 IPv6의 등장으로 정보통신기술은 새로운 국면을 맞고 있으며, 여러 하드웨어 기술이 등장하거나 기존의 기술이 재조명받으면서 다양한 분야에서 IoT를 응용하려는 움직임이 나타나고 있다. 또한 IoT가 점차 많은 분야에 적용되고 네트워킹 기술이 포함된 전자기기의 보급이 증가됨에 따라 각 기기마다 IPv6의 IP주소를 부여받게 됨으로써, 사용자뿐만 아니라 사물들조차 주소를 가지게 되면서 IP주소 관리시스템이 더욱 중요시되고 있다. 또한 IP주소를 가지고 있는 전자기기가 더 이상 사용되지 않을 때, 그 전자기기의 IP 주소를 추적 및 회수하기위한 보완된 물류관리시스템이 필요하다.

본 논문에서는 먼저, IoT의 현황과 IPv6에 대한 배경 지식 및 전체적인 동향을 살펴보고, 현재 물류관리시스템에서 사용되고 있는 주요 기술이 가지고 있는 문제점을 파악한다. 이어서 IPv6의 IP주소와 위치기반서비스(LBS)를 이용한 보안을 고려한 새로운 물류추적 및 재고관리 시스템을 제언하고자 한다. 이를 위해 서론에 이어 IoT, IPv6 그리고 위치기반서비스의 이론적 배경 및 동향을 살펴보고, 다음으로 관련된 기존연구를 분석하며, 새로운 시스템을 제언하고 결론을 맺는다.

II. 관련 현황

2.1 사물인터넷

2.1.1 사물인터넷의 정의

IoT 개념은 전 세계적으로 여러 국가기관, 관련학계뿐만 아니라 IoT에 관심을 가지고 있는 다양한 산업분야에서 여러 관점으로 정의를 내리고 있다. 국제전기통신연합(ITU)은 기존의 정보통신기술이 가지고 있는 특징인 사람과 사물 간에 언제(Anytime), 어디서나(Anywhere) 정보를 주고받는 것을 넘어서 무엇(Anything)이라는 새로운 개념을 추가하여, 사람 대 사물, 사람 대 사람, 사물 대 사물 간의 연결 및 통신이 가능하게 해주는 기술이라고 정의한다[5]. 이때 무엇이라고 정의된 Anything은 단순히 물리적인 공간에 있는 사물을 말하는 것이 아니라 가상공간에서 식별 및 저장되어 있는 정보도 포함하고 있다고 할 수 있다. IERC(European Research Cluster on the Internet of Things)는 IoT를 기본적으로 상호 운용적이며, 물리적/가상적인 정보가 물리적 속성과 가상적인 특징을 가지고 있으며, 지능적인 인터페이스를 사용하고 정보네트워크가 균일하게 통합된 통신 프로토콜을 기반으로 하여 스스로 정보를 교환할 수 있는 능력을 가진 광대역 동적

네트워크 인프라로 정의하고 있다[6]. 또한 국내에서는 M2M과 유사한 개념으로 사람 대 사물, 사물 대 사물간의 지능통신 서비스를 언제 어디서나 안전하고 편리하게 실시간으로 이용할 수 있는 미래 방송통신 융합 ICT 인프라로 미래창조과학부에서 정의하고 있다[7].

여러 관점의 정의를 종합할 때, IoT란 기존의 유선 혹은 무선통신을 기반으로 한 인터넷이나 모바일 인터넷보다 진화된 단계로, 인터넷에 연결된 기기가 사람의 개입 없이 상호간에 알아서 정보를 주고받아 처리하여 사물이 인간에 의존하지 않고 자율적으로 데이터 통신 및 정보의 교환이 가능한 유/무형 플랫폼의 형태라고 할 수 있다. 또한 모든 사물이 각각의 아이덴티티(Identity)를 가지며, 서로 식별할 수 있으며 이를 네트워크를 통해 전송하고 데이터를 수신하여 처리하는 컴퓨팅 능력을 지니고 있다고 할 수 있다[8].

2.1.2 사물인터넷의 기본 규약

IoT는 다양한 서비스를 제공하기 위해 다음과 같은 통신서비스 원칙을 충족시켜야 한다. 우선 서비스와 디바이스 혹은 게이트웨이 간의 통신을 지원해야 하며, 복수의 통신기술도 사용가능해야 한다. 또한 네트워크에 연결된 객체는 다른 객체와 통신이 가능해야 하며, 보안을 위해 네트워크 구조로부터의 서비스 독립성을 반드시 제공하여야 한다.

이러한 점들을 바탕으로 한 IoT 통신 규약은 다음과 같다[9]. 1) 대기 모드 환경에서도 통신이 가능해야 한다. 2) Anycast, Unicast, Multicast, Broadcast를 지원해야하며, Broadcast는 부하 감소를 위해 가능한 경우 Multicast나 Anycast로 대체할 수 있어야 한다. 3) 메시지 전송 스케줄링을 지원하며 전송지연 허용범위를 항시 인식할 수 있도록 해야 한다. 4) 서비스는 최적화된 메시지 통신경로를 선택할 수 있어야 하며, 통신이 실패할 경우 이를 알릴 수 있는 기능이 포함되어야 한다. 5) 다양한 객체 간 통신지원을 위해 이종망간 통신이 가능해야 하며, 확장성, 이동성, 무결성, 연결성 등을 보장할 수 있어야 한다.

2.1.3 사물인터넷의 주요 구성 요소

IoT의 주요 구성요소는 인간, 사물 그리고 서비스로 나눌 수 있다. 그중 '사물'은 유무선 네트워크에서의 종단장치뿐만 아니라 현실에서 실제로 보고 느끼고 만질 수 있는 모든 유형적 사물에서부터 사용자가 실제로 느끼거나 만질 수는 없으나 특정 서비스를 수행하는 주체 혹은 특정 기능을 수행하는 가상 객체와 같은 무형적 사물도 포함할 수 있다. '서비스' 요소는 일반적으로 쉽게 적용할 수 있는 홈네트워크 시스템이나 물류관리/유통관리 시스템, 교통관제시스템 및 소방방재시스템이 있다. 서로 다른 분야에 사용되는 IT 융합도 이 요소에 포함된다고 할 수 있다. 또한 센서 및 GPS 시스템을 이용한 정보를 가공하여 한 사물의 다양한 정보를 제공하는 서비스도 존재하고 있다.

IoT는 '인간'에 의지하지 않고 자율적으로 정보를 얻고 데이터 통신하는 플랫폼으로 정의되었으며, 이에 따른 몇 가지 사례를 보면 다음과 같다[10].

1) 사물 대 사물 통신 : 센서와 통신기능을 가진 사물이 통신 및 상호작용하여 더욱 정교하거나 복합적인 정보를 얻는다. 예를 들어, 가정 내의 오염정도를 측정할 수 있는 센서노드와 로봇청소기 혹은 공기청정기가 데이터를 주고받으며 통신하여, 해당 지역에 대한 먼지제거 및 청소업무를 수행하는 경우다.

2) 사물 대 서비스 통신 : 사물의 특정 기능을 수행하는 서비스간의 통신 및 상호 작용으로, 예를 들어, 전력 부족량을 모니터링 하는 서비스와 스마트그리드의 송배전 스위치 장치간의 상호작용을 통해 특정지역에 전력을 안정적으로 공급하는 경우다.

3) 서비스 대 서비스 통신 : 서비스와 서비스간의 통신 및 상호작용을 통해 좀 더 가치 있는 서비스를 창출할 수 있다. 예를 들어, 환자의 건강상태를 모니터링 하는 헬스케어서비스(서비스 A)와 온도나 습도 등 해당 환자의 거주지 혹은 여행지의 외부환경을 모니터링 하는 서비스(서비스 B)의 상호작용을 통해 환자의 건강상태를 최적으로 유지할 수 있도록 하는 서비스가 이에 해당된다.

2.1.4 사물인터넷 서비스와 플랫폼

IoT 서비스는 크게 서비스 대상과 제공을 하는 주체에 따라 유형화할 수 있는데, IoT 관련 장치를 직접 구입하여 서비스를 제공받는 개인 IoT서비스, 정부에서 사회문제 해결을 위한 서비스나 전 국민에게 동시에 서비스를 제공하기 위해 인프라를 구축하는 공공 IoT서비스, 그리고 기업이 관련 사업의 경

쟁력을 강화하고 정보시스템의 효율성을 위해 도입하는 산업 IoT서비스 등으로 분류할 수 있다[11,12].

또한 IoT플랫폼은 다양한 IoT서비스를 위해 다양한 사물과 사물 사이, 혹은 다수의 사용자와 사물 사이의 중재자 역할을 위한 것으로, 단순히 하나의 어플리케이션에 종속되지 않으면서 사물 간 네트워킹, 센서에 의한 데이터 수집과 이를 이용한 데이터 분석 및 지능형 서비스 등을 제공하는 공통의 시스템을 의미한다[11,13].

과거부터 이동통신사업자들은 이동통신단말기를 통해 인터넷에 연결을 하기 위해 유럽통신표준기구(ETSI), 3GPP 등을 통해 M2M 플랫폼을 개발해 왔다. 또한 글로벌 표준을 통해 시장규모를 확대하기 위해, oneM2M 표준화에 적극적으로 참여하고 있다. 외국에서는 자사의 인터페이스를 이용하여 웹에 연결할 수 있는 서비스 플랫폼이나 센서와 같은 사물들이 웹을 통해 연동하거나 SNS(Social Network Service)와의 연동을 통해 사물들을 활용할 수 있는 서비스가 등장하였다. 또한 IT서비스 업체에서도 각 회사의 장점을 기반으로 IoT 플랫폼의 기술 확보 및 시장선점에 주력하고 있다. 국내에서도 역시 이동통신 사업자와 관련 서비스 업체와의 협력으로 ETSI의 표준을 기반으로 IoT연결 플랫폼을 개발하고 있다. 대표적으로 ETRI에서 개발된 Coweb (Collaborative Web of Things) 플랫폼과 개방형 시멘틱 USN서비스플랫폼(Common open semantic USN service platform; COMUS)이 있다[12].

2.2 IPv6

2.2.1 IPv6의 정의, 배경, 특징

한국인터넷정보센터(KRNIC)에 따르면, 2014년 11월 24일 기준으로 전 세계의 잔여 IPv4 주소는 2.8%만 남아 있으며, 그 숫자는 약 1억 2천개 정도이다. IPv4 주소의 소모는 해를 거듭할수록 기하급수적으로 빨라지고 있으며, 이것은 인터넷에 접속되는 컴퓨터 혹은 네트워크 접속이 가능한 디바이스의 수도 역시 기하급수적으로 증가하고 있다는 의미이다. 이러한 이유로 급격히 소모되고 있는 IP주소를 해결하기 위해 하나의 주소에 더 많은 네트워크를 할당하기 위한 네트워크 단편화(network fragmentation)도 역시 증가하고 있어 라우터에 많은 부담을 주고 있는 실정이다.

또한 기존 주소체계의 한계성과 시간이 갈수록 증가하는 주소개수 충족을 위한 NAT(Network address translation) 등의 기형적 발전, 그리고 차세대 인터넷을 위한 수용능력 부족 등이 본격적으로 표면에 나타나 새로운 주소체계가 필요해 왔다. 1994년 팔로알토연구소에서 개발하고, 1995년 국제인터넷표준화기구에서 RFC 2460 기술문서로 정식으로 채택하여 IPv6가 등장하였다. 2014년 11월 24일 기준으로 약 20만개가 특수용도를 제외하고 할당되어 있다.

IPv4와 비교하여 IPv6의 가장 큰 차이점은 IP 주소의 길이가 기존의 32비트에서 128비트로 대폭 확대되었다는 점이다. 이는 폭발적으로 늘어나는 인터넷 사용에 대비하기 위한 것이며, 앞으로 1인 한 IP주소가 아닌 3~4개 이상의 IP주소를 가질 수 있는 시대와 부합한다고 할 수 있다. 또한 IPv6는 개발 당시부터 기존의 IPv4와의 호환성을 최대로 하는 방향으로 설계됨과 동시에 기존의 IP주소 보다 더 많은 기능을 제공하도록 설계되었다. 대부분의 네트워크 수준 상위 프로토콜들은 큰 수정 없이 IPv6 상에서 동작할 수 있도록 개발되었다. IPv6의 주요 특징은 확장된 주소 공간, 호스트주소 자동설정, 패킷 크기 확장, 효율적인 라우팅, 향상된 서비스 지원, 인증/보안기능 강화로 요약할 수 있다[14,15].

2.2.2 ICMPv6와 NDP

ICMP(Internet control message protocol)는 네트워크 상태에서 메시지를 주고받을 수 있도록 동작하는 프로토콜이며, IPv4와 IPv6와 동일한 네트워크 계층에서 이루어진다. 그 중 ICMPv6 (ICMP Version 6)는 기존의 ICMPv4를 발전시킨 형태로 ICMPv4에 IGMP(Internet group management protocol), ARP(Address resolution protocol)를 통합하여 정의한 프로토콜이며, RARP(Reverse ARP)는 삭제되었다[16].

NDP(Neighbor discovery protocol)는 IPv6 환경에서 인접한 IPv6 노드들이 서로 검색하고 통신할 수 있다. 또한 현재 모든 IPv6 장비에는 기본적으로 NDP가 구현되어 있고 ICMPv6에 포함되어 있으며, IPv4 환경에서 사용하던 ARP의 기능을 대신한다[17].

2.2.3 IPv6환경에서 IP주소 설정

IPv6는 사용자가 인터넷에 접속 할 때, 주소를 직접 설정하지 않는 자동주소설정 기능이 있으며, 이 기능은 Stateless 방식과 Stateful 방식이 존재한다. 또한 IPv4와 동일하게 IP주소를 고정적으로 주는 방식도 사용할 수 있다. IPv4에 비해 강력한 장점중 하나인 IPv6의 주소 자동설정 기능은 Stateless 방식을 말하는 것으로 이는 NDP와 ICMPv6 메시지를 이용하는 방식이며[18], 호스트가 라우터의 네트워크 정보와 자신의 인터페이스 정보를 이용하여 자체적으로 IPv6 주소를 생성한다. 이 방식은 일반적인 IPv6에서 유비쿼터스 환경과 모바일 환경에서 네트워크 자원을 도울 수 있으며, 별도의 서버가 필요 없다는 장점을 가지고 있다. 그러나 이로 인해 인가되지 않은 호스트의 접근이 용이하며, 이로 인한 보안문제가 발생할 수 있는 단점을 가지고 있다[19].

Stateful 방식은 DHCPv6(IPv6 for dynamic host configuration protocol) 서버로부터 필요한 모든 네트워크 정보를 받는 방식으로 IPv4에서 사용되고 있는 자동설정방식이다. 이 방식은 이미 IPv4에서 사용하고 있는 방식이기 때문에 IPv6의 새로운 기술이라고 할 수는 없으나, 인증을 통한 보안관리가 현 네트워크 보안체제와 비슷하며, DHCPv6는 네트워크의 Prefix만 아니라 호스트 부분의 인터페이스까지 일괄적으로 관리하기 때문에[20], 주소관리의 용이성이 장점이라고 할 수 있다.

이외에도 IP를 자동으로 설정하는 방식이 아닌 사용자가 직접 IP주소를 설정하여 사용하는 방법도 가능하다. 그러나 이 방법은 기존의 IPv4의 주소보다 길게 구성되어 있는 IPv6와 맞지 않는 방법이며, 또한 일반적인 사용자가 사용하였을 때 IP주소 충돌과 같은 문제가 발생할 수 있다. 하지만 고정주소 할당 방식은 사설 이용자 보다는 공공기관이나 혹은 사기업 내부 네트워크를 사용할 때 많이 사용되는 형태이며, 주요 포털사이트는 주소를 계속 유지해야 하기 때문에 고정주소할당 방식을 사용한다.

2.3 IPv6와 사물인터넷의 관계

2.3.1 사물인터넷 환경에서 IPv6의 필요성

다수의 사물들을 연결할 필요성에 의해 각각의 사물(장비)이 무엇인지 식별하는 것은 중요한 문제 중 하나이다. 시스코에 따르면 2013년 기준 인터넷에 연결되는 장비는 1인당 한 개 수준에서 2018년에는 1.5개로 전망하고 있다[21]. 그러나 단일 네트워크 수준을 포함하였을 때 실제로 인터넷에 연결되는 객체의 수는 기하급수적으로 증가할 것으로 보인다[22]. 이와 같이 인터넷에 연결되는 사물의 수가 기하급수적으로 증가하면, 식별에 관련된 문제가 따른다. 이러한 문제에서 IPv6의 거의 무한에 가까운 주소 수는 거의 무한에 가까운 사물의 식별정보를 생성할 수 있다. 또한 IPv6는 기존의 IPv4와 충분히 호환가능하며, 동일한 네트워크 구조를 따르기 때문에 IoT에 관련된 새로운 서비스 및 네트워크 기술에 필수적이라고 할 수 있다.

IoT서비스를 효과적으로 실현하기 위해서는 다양한 기술들이 요구된다. 특히 IoT의 가장 기본적인 이슈이면서 가장 중요한 요소는 사물 간에 서로 유기적인 네트워크 구축이기 때문에, 신뢰성 있는 통신과 지능적인 네트워킹 등이 필수적으로 요구되고 있다. 그러나 IoT의 특성상 기존에 사용하고 있던 네트워크와 달리 저 전력이 요구됨에 따라, 상당히 제한적인 환경에서 통신을 수행해야하는 상황이다. 이러한 환경에서 사물 간 무선통신을 실행해야함에 따라 통신의 범위, 비용, 전력이 무엇보다 중요하게 작용하게 된다. 이에 따라 현재 가장 많이 사용되는 Wi-Fi 뿐만 아니라 NFC, RFID, 블루투스 및 Zig-Bee 등 상대적으로 사용빈도가 낮았던 다양한 네트워크 기술이 재조명받고 있다.

2.3.2 IPv6와 사물인터넷 표준화

IPv6의 무수한 주소자원과 개선된 장점이 IoT가 요구하는 부분과 맞아 떨어지면서, 국내외 많은 단체들이 표준화를 진행해 왔다. IETF는 IPv6를 기본규격으로 표준 제정을 한 이후에도 IPv6 멀티캐스트 주소설정 기법(RFC 4489)이나 터널링 기법(RFC 5969), 기존 IPv4에서 전환을 하기 위한 전환기법(RFC 6145/6146) 등 현재 네트워크를 구성하고 있는 IPv4에서 IPv6로 전환하는 표준화를 제정하였다. 또한 저전력 네트워크상에서의 IPv6 설계표준(RFC 6568/6606)이나 IoT 환경에서의 IPv6 적용과 관련된 표준개발이 진행되고 있다. 국내에서도 이미 TTA를 중심으로 IoT기술 표준화를 진행하고 있으며 학계에서도 기술 표준화를 지원하고 있다[22].

2.4 위치기반서비스

위치기반서비스(LBS)란 휴대폰이나 PDA와 같은 장비에 이동통신망과 IT기술을 종합적으로 활용한 위치정보기반의 시스템 및 서비스를 통칭하며[23],상품정보뿐만 아니라 교통정보, 위치추적 등 생활 전반에 걸쳐 다양한 정보를 제공하는데 활용할 수 있는 서비스이다. 크게 이동통신 기지국을 이용하는 Cell 방식과 위성항법장치를 활용한 GPS (Global Positioning System)방식으로 나누어진다. Cell 방식의 경우 이동통신사업자의 기지국을 활용한 방법으로 각 지역에 분포되어 있는 기지국 3개를 이용하여 삼각측량을 하는 방식으로 위치를 파악할 수 있으며, 중계기와 같은 서브(sub) 장비를 이용하여 건물 내부나 혹은 지하와 같은 음영지역의 위치도 찾을 수 있는 장점이 있다. 그러나 오차범위가 1km에서 5km까지 범위가 넓어 대략적 위치만 파악할 수 있는 단점이 있다. GPS 방식의 경우 앞의 Cell 방식보다 정확한 위치추적이 가능하며, 기존 방식보다 불과 10m에서 150m 사이의 오차로 인해 비교적 정확한 위치를 찾을 수 있는 장점이 있다. 위성에서 사용하는 위성신호의 특성상 1,000Mhz 이상의 고주파를 사용하며, 이는 신호의 반사 및 굴절에 영향을 많이 받는 고층건물이나 혹은 실내에서는 사용효율이 떨어진다.

스마트폰이 활성화되고, 무선인터넷의 확산 및 GPS가 탑재된 다양한 단말기가 확대됨에 따라 위치기반서비스도 변화하고 있다. 최근에는 GPS와 Wi-Fi 망을 함께 활용하여 실외에서는 GPS를 사용하고, 실내에서는 Wi-Fi망을 사용한 개선된 위치기반서비스도 등장하고 있다. 이것은 단말기 사용자의 개인 취향에 맞춘 서비스를 제공하는데 용이하며, 또한 SNS나 모바일 광고 등 다양한 서비스와 결합하여 핵심적인 플랫폼으로 떠오르고 있다. 개인화된 서비스뿐만 아니라 교통, 치안 혹은 구조요청 등과 같은 공공부문 및 공공사회안전망으로서도 활용도가 높아지고 있다[23].

III. 선행 연구

3.1 IP 주소관리시스템 관련 연구

3.1.1 IP 주소관리시스템의 설계 및 구현 연구

이희찬 등의 연구[24]는 네트워크의 설정을 변경하지 않으면서 사용자의 특별한 개입 없이 IP주소를 관리 및 모니터링하고 중요 서브의 IP 사용을 보호할 수 있는 에이전트 기반의 시스템을 개발하기 위한 연구이다. 여기서 말하는 에이전트는 각 Broadcast 도메인을 단위로 한 하나의 집단을 말하며, PM(Primary Master)모드로 동작하는 에이전트는 시작 시 IP 관리서버에 연결하여 차단해야 할 IP 주소-MAC 주소 맵핑 표를 가져오게 된다. ARP패킷을 캡처하면서 차단해야 할 IP주소의 ARP를 발견하였을 경우 MAC주소를 검사하여 등록된 것과 다르면 불법적인 IP주소를 사용하는 것으로 간주하여 그 호스트를 차단하게 된다. 차단 기법은 Gratuitous ARP 프로토콜과 이 프로토콜이 실패한 경우를 대비하여 사용되는 ARP Spoofing을 이용하는 방법을 채택하였다.

시스템의 견고성 향상을 위해 Primary-Secondary 구조를 채용하였다. 이 구조는 에이전트가 자신의 Broadcast 도메인에 PM모드로 동작중인 에이전트가 없는지 검사를 한 이후, 만약 없다면 자신이 PM모드로 동작을 하게 된다. 이미 PM모드로 동작중인 에이전트가 있다면 자신은 대기모드로 동작을 시작하게 되며, PM모드의 에이전트가 수집한 IP 리스트 중에서 랜덤하게 하나의 호스트를 지정한 후 SM(Secondary Master)으로 지정한다. 이때 지정된 SM모드의 에이전트는 PM모드의 에이전트와 주기적으로 통신을 하여 PM보유 리스트를 저장하고, PM이 일정 시간동안 응답이 없을 경우 PM이 종료된 것으로 간주하고, SM모드의 에이전트가 PM모드로 전환하게 되는 구조이다. 즉 SM모드는 PM모드의 백업이라고 할 수 있다.

이 연구[24]에서 구현한 IP 주소관리시스템은 ARP 프로토콜을 사용하였으며 이는 IPv6 보다는 IPv4에 적용된 연구이다. 결과적으로 불법적으로 사용된 IP의 사용제한을 하는 것에는 성공하였으나, 필요한 메시지의 종류가 많이 세분화하지 못하였으며, 실제로 사용되는 네트워크 보다 훨씬 단순한 상태에서 진행되었다는 것을 확인할 수 있다.

3.1.2 IPv6 환경에서 호스트 탐색 및 네트워크 접속차단 에이전트시스템 연구

정연기 등의 연구[20]는 IPv6 환경에서의 주 기능인 자동주소설정 기능을 언급하면서, 주소를 각 호스트에 자동으로 할당할 경우 생길 수 있는 정보

의 보안 및 유지와 IP주소 조사에 어려움이 따른다고 제시했다. 또한, IP주소의 자동설정으로 인하여 일부 사용자가 악의를 가지고 아무런 제약 없이 네트워크 주요장비에 접근 할 수 있는 문제가 발생할 수 있으며, 이러한 사용자들에 대한 관리 및 차단이 필요하다고 언급하고 있다. 따라서 이 연구[20]의 주요 목적은 IPv6 환경에서 호스트를 탐색하고 인가되지 않은 호스트가 네트워크에 접속하는 것을 차단함으로써 네트워크의 주요 자원을 관리 및 보호할 수 있는 에이전트시스템을 제안하는 것이다.

IPv6에서 특정 호스트의 탐색을 하는 방법은 NS(Neighbor solicitation) 패킷과 NA (Neighbor advertisement) 패킷을 이용하는 방식이 있다. 특정 호스트를 차단하는 방식은 NDP의 동작 중에서 DAD(Duplicate address detection) 동작을 이용하여 구현하도록 하였다. 이때 DAD란 IPv6에서 어떠한 방법으로 IP주소를 구성하더라도(Stateful 또는 Stateless) 해당 IP가 이미 사용 중인지 아닌지 확인을 하는 동작이다.

이 연구[20]에서 구성된 시험망은 link local, site local, 고정IP 세 가지 IP주소를 설정하였으며, 미리 탐색/차단할 IP주소와 MAC 주소를 지정하였다. 그 결과, 대부분 상황에서 정상적으로 차단이 수행되는 것을 확인하였으나, 고정 IP를 설정한 경우 차단이 되지 않는 문제가 있었다. 고정 IP를 차단하기 위해서는 멀티캐스트 IP를 사용하지 않고 특정 호스트의 IP로 테스트한 경우에 정상적으로 차단되는 것을 확인하였다. 또한 구현한 에이전트시스템의 동작을 테스트한 결과, 차단 이후 설정된 IP에서 설정이 해제되는 결과를 나타냈다. 결국 실제 본래의 에이전트시스템을 이용하여 특정 호스트의 접속을 차단하려고 할 때에는 IP 주소가 아닌 MAC 주소로 차단 대상 호스트를 결정해야 된다[20].

3.1.3 IP 에이전트기반 통합 IP 주소관리 시스템 연구

이동일의 연구[14]에 의하면, IPv6의 자동주소설정 기능으로 인하여 야기될 수 있는 문제 중 악의적인 목적을 가지고 사용자가 주소를 얻고 접근할 수 있는 가능성에 대응하기 위한 IP주소 관리가 필요하다고 제시한다. 이 연구에서 제안하고 있는 것은 IPSec(Internet Protocol Security)이라는 보안요소를 탑재하고 주소공간을 확대, Flow label을 이용한 패킷별 품질제어 및 자동 주소설정의 기능이 추가된 인터넷 프로토콜을 이용함으로써, 관리자와 일반사용자의 편의성이 증대될 것이라는 기대를 가지고 있다.

IP 에이전트의 Master, Secondary, 그리고 Slave 노드를 통하여 Master research 메시지를 통하여 Master 부분이 서브 네트워크 호스트들의 주소를 습득하는 방법을 통하여 IP주소를 습득한다. 주소를 차단하는 방법으로는 DAD 과정을 이용하여, 변조 NA패킷을 통해 특정 호스트의 주소 획득을 차단하면서 동시에 이미 주소를 습득한 호스트의 경우 NA 웹페이지 유도를 통하여 에이전트를 설치하는 방법을 제시하였다. 이를 통해 주소 획득 이전의 특정 호스트를 차단하는 것과 동시에 이미 주소를 습득한 호스트 역시 에이전트를 통하여 관리할 수 있도록 하는 것이다.

이 연구[14]에서의 전체 시스템은 인가된 각 호스트에 설치된 IP 에이전트와 전체 네트워크의 주소를 관리하는 기능을 수행하는 IPMS(Internet protocol management system) 통합 주소관리 서버로 구성되어 있다. IPMS는 인가된 호스트의 MAC주소를 미리 수집했다는 가정 하에 각 서브네트워크들은 반드시 Master노드와 Secondary노드 하나씩을 가져야 하고 나머지는 모두 Slave노드로 구성되어야 한다. 이때, Master노드는 자신이 속해있는 서브 네트워크의 모든 노드들의 주소를 수집하는 기능과 IPMS는 모든 Master노드들의 주소를 가지고 있어야 하는 것과 동시에 노드의 차단 및 웹페이지의 redirection 기능도 포함되어야 한다고 제시한다. 이것은 이희찬 등의 연구[24]에 있는 Master-Secondary 시스템과 동일한 것이라고 볼 수 있으며, 시스템의 견고성 목적을 가지고 있다.

제시한 IPMS를 통합서버에 두고 각 서브네트워크에 Master노드를 두어 Secondary와 Slave 노드를 관리하고 에이전트를 설치하는 시스템을 통해 네트워크상에서 불필요한 패킷을 여러 번 전송하지 않고 주소를 수집하고, 에이전트를 설치하지 않은 호스트는 설치 유도 웹페이지를 전송함으로써, 결과적으로 접근하는 모든 호스트가 에이전트 관리 하에 인가된 IP를 부여하는 시스템을 제안하였다. 그러나 변조된 웹 페이지를 전송하는 경우, 호스트가 처음에 요청한 웹페이지가 에이전트 프로그램이 생성한 변조 웹페이지 보다 먼저 도달하는 경우에 생기는 문제점에 대해서는 대처하지 못하는 단점을 가지고 있다.

3.1.4 IPv6 호스트 접근제어를 위한 IPv6 주소 관리서버의 설계 및 구현 연구

한선영 등의 연구[25]에서도 IPv6의 자동주소설정 기능을 언급하면서 그 중에서 Stateless 방식으로 설정하였을 때 생기는 보안 및 관리 측면에서 운영이 어렵다고 제시한다. 이 연구에서 제안하는 방법은 ICMPv6 프로토콜을 이용한 주소제어 방법으로서 수집과정으로는 MLD(Multicast listener discovery) 프로토콜과 NDP를 이용하였으며, 차단방법으로는 NCT(Neighbor cache table)를 변조하는 방법을 이용하였다.

이 연구[25]에서는 IPv6 주소관리서버인 AMSv6(IPv6 Address Management Server)를 설계하고 구현하는 것이다. AMSv6는 호스트의 주소를 수집하는 '수집부'와 주소를 차단할 수 있는 '차단부'로 나뉘어 있다. 수집부는 기존의 네트워크에 무관하게 단순히 AMSv6를 설치하여 패킷들을 수집하는 방식으로 MLD와 NDP를 이용하는 방식 두 가지로 분류되었다. 차단부는 IPv6의 특성상 모든 호스트는 통신을 하기 위해 주변 이웃들의 NC(Neighbor cache)정보를 가지고 이를 주기적으로 갱신해야 하는데, 이 과정을 이용하여 NC정보를 변조함으로써 차단하는 방법을 사용한다.

이 연구[25]에서 테스트를 위해 네트워크 환경을 구축하였으며, Window7과 Ubuntu(Linux계열)를 OS 호스트로 지정하였다. 그 결과 수집과정에 있어 생길 수 있는 불필요한 트래픽의 증가 및 시스템 문제를 해소할 수 있었으며, 차단 방법의 경우에도 필요한 경우 올바른 NC 정보를 재전송함으로써 손쉽게 차단을 해제할 수 있는 장점이 있다. 그러나 이 연구는 호스트의 MAC 정보를 숨기는 기법이나 변조에 대해서는 고려하지 않아 지속적인 연구가 필요하다.

3.1.5 종합

IP 주소관리 시스템의 선행연구를 정리한 Table 1은 대체적으로 IP 주소의 Stateless 방식의 자동주소설정 방법에 대해 가장 문제가 되고 있는 인가된 호스트와 비인가된 호스트의 구분을 짓기 위한 주소관리시스템이 필요하다는 것이 공통주제라고 볼 수 있다. 대체로 호스트를 탐색하는 것에 있어 유사성을 띄고 있으나, 트래픽 관련 개선사항을 볼 수 있다. 호스트 차단부분에서는 직접 웹페이지로 유도하여 에이전트시스템을 설치하는 형태와, NC 정보의 변조를 이용하여 차단하는 방법과 같이 여러 방법을 제안하고 있다. 그러나 외부 IP에 관한 호스트 정보의 자체적인 은닉 및 변조 부분까지 고려한 연구 사례는 아직 찾아 볼 수 없었다. 이러한 IP 주소관리 시스템의 대부분의 특징은 자동주소설정을 기반으로 하였다는 것을 알 수 있다.

Table 1. The prior research of IP address management system

Research	Attributes	Merit	Demerit
[24]	Using PM-SM	High stability	Based-on simple network IPv4
[20]	Using manipulated NA	Ease of protection from automatic IP address	Un-completion of static IP screening, and presenting installation clearing result from installed IP after screening
[14]	Using PM-SM, and supposing to gather MAC address in advance	High stability	When requested webpage is faster than forged webpage, it's impossible to protect it.
[25]	Address control using ICMPv6 protocol	Lessening effect of unnecessary traffic and ease of clearing protection	Impossibility to prepare in case of hiding or forging MAC information

3.2 사물인터넷 응용서비스 연구

IoT와 비즈니스 기회 연구[26]는 미래에 나타날 새로운 상호작용패턴으로서 SIRW(Smart Interaction with Real World) 혹은 실세계와의 스마트한 상호작용과 같은 패턴으로 보고 있다. 이것은 사용자가 스마트 디바이스를 활용하여 현실세계와 상호작용한다는 것을 의미하며 이러한 것을 충족시킬 수 있는 인프라가 바로 IoT라고 제시하고 있다. 예를 들어 미술관, 갤러리 혹은 박물관과 같

이 여러 물건이나 작품을 전시하는 장소에서 중요한 것 중 하나는 전시 작품이나 물건에 관한 정보를 제공하는 것이다. IoT를 이용하기 전에는 관련된 정보를 단순히 전시물 근처에 간단하게 배치하였지만, 방문자에게 제공할 수 있는 정보는 분명 한계가 있었다. IoT 기술을 이용하여 정보를 제공할 수 있는 RFID 같은 전자 태그나 혹은 전시 공간 내의 블루투스 모듈을 설치함으로써, 방문자가 가지고 있는 스마트 디바이스를 이용하여 원하는 정보를 제한 없이 받을 수 있도록 시스템을 설계할 수 있다. 또한 이러한 시스템을 통해 얼마나 많은 사람이 방문 하였는가와 같이 전시관련 업종의 관계자나 작품전시 작가들이 방문자들과 유기적으로 커뮤니케이션할 수 있는 공간을 생성할 수 있는 기회를 가질 수 있다.

IoT는 새로운 인프라를 구축할 수 있는 여건이 마련되면서 각 분야의 여러 기업에서 여러 가지 새로운 사업적 모델을 만들어 내고 있다. 1) 기존의 제품을 IoT을 통해 더욱 발전시켜 제품의 가치를 올리는 고부가가치화를 지향, 2) 이미 존재하는 서비스의 불편함을 개선하기 위해 IoT 기술을 더하여 서비스의 범위확장을 지향, 3) IoT 영향으로 불리한 시장변화에 대응하기 위해 IoT을 적용하는 부분, 4) 기존제품의 불편함으로 인하여 사용되지 않던 제품에 IoT를 더하여 관련 서비스를 제공함으로써 새로운 고객유치를 도모하는 방법, 5) 단순한 제품이 아니라 어떠한 장소나 공간에서 사용할 수 있는 고객관계관리(CRM)의 유기적 커뮤니케이션을 위해 IoT를 도입하는 방법 등이 있다[26].

3.3 위치기반서비스 관련 연구

정창훈 등의 연구[27]는 스마트폰에 내장되어 있는 위치기반서비스의 배터리 자원 효율을 올리기 위한 방법에 대한 연구로, 여기에서 제안하는 프로세스는 모바일 자원의 낭비를 줄이기 위해 특정한 위치에 따라 위치기반서비스의 주기를 변경시키는 기법을 제안하고 있다. 이 기법을'동적 위치인지'기법이라고 설명하고 있다. 이는 사용자의 현재 위치와 임의의 목적지 사이에 n개의 중간 지점을 얻어, 중간 지점들을 인지함에 따라, 기존에 일정했던 GPS를 사용하는 위치기반서비스의 주기를 목적지까지 남은 거리에 비례하여 재구성 할 수 있다. 결과적으로 GPS와의 통신주기를 줄일 수 있는 효과가 있음을 제시한다.

Fig.1.은 동적 인지기법 기술의 개념으로, 사용자의 출발 지점과 도착지점 간에 1/2^n 위치 지점을 얻어 인지하여 현재의 위치와 도착지점의 위치 사이에서의 경도데이터 차이와 위도데이터 차이를 각각 제곱하여 더한 값의 루트 연산을 한다. 이 방법은 두 개의 점 사이의 거리를 구하는 공식과 동일하다는 것을 알 수 있다. 이러한 방법으로 하나의 사이클을 돌리고 이후에 다음 사이클로 넘어가면서 반복하는 방법을 취하고 있다. 이러한 결과를 통해 얻은 각 사이클을 통해 LBS 수신주기를 재구성하는 방식으로 디바이스 자원의 낭비를 줄이는 효과를 기대하고 있다. 이 연구의 실험을 통해 한정된 자원을 가진 디바이스를 좀 더 효율적으로 이용할 수 있다는 것을 확인할 수 있었다. 그러나 도착지점이 미리 지정되어 있어야 하며, 만약 불규칙한 도착지점이 생기는 경우에 발생할 수 있는 문제에 대해서는 언급하지 않았다.

남선미 등의 연구[23]에 따르면, 위치정보와 관련된 다양한 서비스가 확대되고 있으며, 이에 따라 전 세계적으로 위치기반서비스 시장이 활성화 되고 있다는 점을 언급하면서, 동시에 개인의 위치 정보에 관련된 침해사례도 늘어나고 있다는 점을 밝혔다. 국내에서는 전 세계적으로 유일하게 위치정보와 관련한 독립적인 '위치정보보호법'이 2005년 1월 제정되어 7월에 시행되었다. 이 법은 사업자가 개인의 위치정보와 관련된 사업을 진행할 경우, 그에 맞는 정보보호 수단을 갖추고 방송통신위원회에 신고 및 허가를 받아야 한다. 이 서비스를 이용하는 개인은 자신의 위치정보 수집 및 이용중지를 사업자에게 요구할 수 있으며, 사업자는 이를 거절할 수 없고, 위치정보사업자는 서비스 제공 후 위치정보 수집/이용

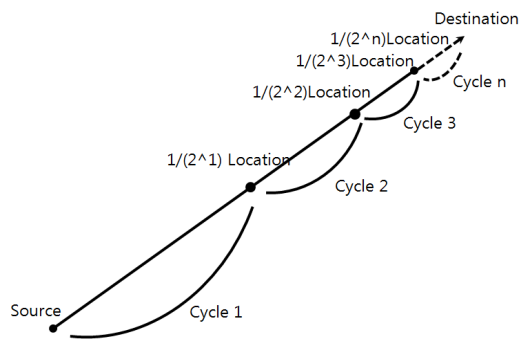


Fig.1. Concept of dynamic position perception technique (source: [27])

/제공 사실 확인자료 외의 개인 위치정보는 즉시 파기해야 한다[28]. 하지만 이러한 이유로 인해 국내 위치기반서비스 산업이 활성화 되지 못하고 있다는 지적이 제기되어 왔고, 이 연구[23]에서도 같은 지적을 하고 있다. 실제로 국내 관련법은 국외의 그것과 달리 개인의 프라이버시와 무관한 규제항목이 많이 존재하며, 이를 완화하였을 때 산업발전을 확대시킬 수 있다고 본다.

IV. 사물인터넷을 위한 물류관리시스템 제언

4.1 기존 물류 및 재고관리 시스템

현재 물류 및 재고관리 시스템에서 가장 많이 사용되는 인식 기술은 바코드 기술과 RFID 기술이다. 바코드 기술은 비용이 가장 저렴하여 다양한 물류 분야에서 사용되었다. 그러나 90년대 중반에 RFID 기술이 일부 응용분야에 나타나고, 물류 관리측면에서 바코드 기술의 문제점이 부각되면서, RFID 기술로 눈을 돌리기 시작하였다. 이 방식은 바코드 시스템의 경우 빛을 이용하여 판독하는 반면에, RFID 기술은 전파를 이용하여 각 태그의 정보를 가져온다. 전파를 이용하는 특성으로 인해 먼 거리에서도 태그를 읽는 것이 가능하며, 물체를 통과하여 정보를 읽는 것도 가능하다. 인식률도 기존의 바코드 보다 높으며, 데이터 저장 공간도 거의 천배 이상 차이가 난다. 다만 태그 비용이 기존의 바코드 보다 비싸다는 단점이 있으나, RFID 태그는 재활용이 가능하다는 장점이 있다. RFID는 태그의 동력 사용에 따라 Passive, Semi-passive, Active로 나누어지며 혹은 태그와 판독기간 통신에 사용하는 주파수(저/고/초고주파)에 따라서 LFID, HFID, UFID로 나누어진다.

그러나 기존의 물류시스템에서 사용하고 있는 바코드 시스템과 달리 RFID 시스템은 태그와 판독기가 동일한 주파수여야 정보를 얻을 수 있으며, RFID로 구성되어 있는 네트워크가 기존의 인터넷 네트워크와 달리 자율적인 분산 구조를 띄고 있어 기존의 네트워크 보안문제 보다 더 심각한 보안문제를 야기 할 수 있다. 또한 외부에 노출되어 있는 태그 정보 및 센서 노드의 위변조가 용이하다는 문제점을 가지고 있다.

또한 RFID 태그를 이용할 때 주위에 있는 물질이 무엇인가에 따라서 인식 여부에 차이를 보이고 있다. 김순석 등[29]은 10차에 걸친 RFID 태그의 물질 투과성 실험결과를 제시했는데, 일반적인 나무나 서적과 같은 비금속제 물질의 경우에는 태그가 정상적으로 인식하나, 철판이나 호일과 같은 금속제 물질이 있는 경우 태그 인식에 큰 장애요인이 된다.

4.2 시스템 제언 및 프레임워크

기존의 물류관리시스템에서 사용되고 있는 바코드 기술이나 RFID 기술의 문제점인 인식 장애 문제와 보안성 문제를 해결하기 위해 IPv6의 IP 주소를 고정 주소방식으로 할당하여 창고 내의 재고품을 관리하고 물류의 추적을 위해 네트워크 기반의 Cell 방식 위치기반서비스를 이용한 새로운 물류추적 및 재고관리 시스템을 제언하고자 한다. Fig.2.는 제언하고자 하는 시스템의 프레임워크를 나타낸 것이다.

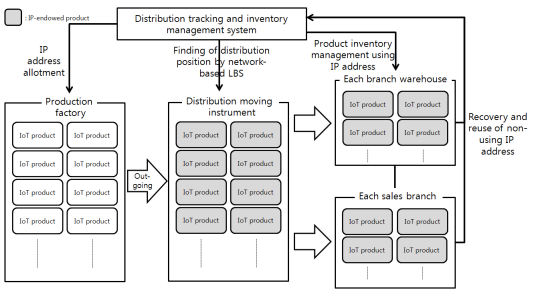


Fig.2. Framework for distribution tracking and inventory management system

4.2.1 IPv6의 IP주소 고정할당 부여 및 관리

IPv6의 주소 개수는 현재 사용되고 있는 IPv4의 IP주소 개수를 훨씬 상회하며 무량대수라고 말할 정도의 수이다. 이에 따라 IoT와 관련된 제품에 각 IP주소를 고정적으로 할당하여, 제품을 생산하는 회사에서 효율적, 일괄적으로 관리할 수 있도록 한다. IPv6의 최대 강점 중 하나인 Stateless IP주소 할당방식을 사용하지 않는 이유는 IP의 고정화로 인한 사용자의 익명성 문제는 일반적으로 '제품' 그 자체의 익명성과 무관하며, 오히려 IP주소의 자동할당방식(Stateless 또는 Stateful)을 사용하게 되었을 경우 외부에서 침입 할 수 있는 보안문제가 고정할당방식 보다 더 취약할 수 있기 때문이다. 또한, 기존의 IPv4에서 고정할당 방식을 사용하지 못한 것은 일반 사용자의 익명성도 있었지만, 전세계 사용

자 대비 IP주소 수가 현저히 부족했기 때문이다.

생산 완료 후 IP주소를 부여 받은 IoT 제품은 창고에 적재되어 출고가 된다. 생산된 창고에서 각 지점의 창고로 이동되는 경우나 혹은 소비자에게 팔린 상품의 경우에 지정된 장소와 제품 사이의 거리를 계산하여 일정 거리 이상을 벗어나게 되면, 이동통신망을 기반으로 하는 Cell방식의 위치기반서비스를 이용하여 도착지점까지 현재 제품이 이동하고 있는 위치를 추적하게 된다.

4.2.2 네트워크 기반의 Cell방식 위치기반서비스

네트워크 기반의 Cell방식 위치기반서비스는 이동통신망의 네트워크를 이용하기 때문에 역시 IP 주소를 사용하게 된다. GPS방식의 위치기반서비스도 이용하는 것이 가능하나, 물품 추적을 위해 IoT 제품 자체에 GPS 수신기를 설치하게 되면 GPS 칩에 관한 비용이 들며, GPS방식은 고층 건물이 많은 도심지역이나 실내와 같은 음영지역이 많은 장소에서는 제 기능을 발휘할 수 없기 때문이기도 하다. 물론 Cell방식 위치기반서비스는 GPS방식에 비해 위치에 대한 오차가 발생하기는 하지만, 애초에 트럭 등의 물류를 담당하는 이동수단에는 GPS장치가 이미 설치되어 있으며, 이동 중인 IoT 제품의 위치를 판단하기를 원할 때 이 장치를 이용할 수 있는 여지는 충분히 있다고 할 수 있다. 또한 생산된 IoT 제품의 목적지는 재고를 관리할 수 있는 창고 즉, 실내라는 점을 고려할 때, Cell방식 위치기반서비스가 더 적합하다고 할 수 있다.

Mobile IPv6와 연동되는 것과 관련, 노드의 이동성을 제공하여 향상된 서비스를 제공해 주지만 노드는 이동시 마다 홈 주소와 외부 네트워크에서의 주소를 바인딩하기 위한 메시지를 홈 에이전트에게 보내야 되는 점이 있다. 노드를 이동하는 메시지로 인하여, 노드 자체의 처리와 네트워크상에서 증가할 수 있는 트래픽을 유발할 수 있는 문제점을 가지고 있다. 특히 핸드오버 시에 이동하는 관리 시그널 메시지에 패킷 전송 지연에 따른 추가 비용이 발생하게 되는 상황이 발생 할 수 있기 때문에, 이를 줄이기 위한 방법으로 Hierarchical Mobile IPv6와 Paging Hierarchical Mobile IPv6를 고려해 볼 수 있다.

4.2.3 물류추적 및 재고관리 시스템 보안 및 IP주소 회수

이 제언에서 시스템의 보안은 물리적 보안, 외부 IP의 유입 문제, 관리자 보안을 생각할 수 있다. 여기에서 제언할 부분은 두 번째 부분을 집중적으로 하고자한다. 물리적인 보안 문제로 보관되어 있는 사물인터넷 제품을 누군가가 악의적인 의도로 훔쳐갈 수 있으며 혹은 시스템 자체를 망가뜨릴 수 있다. 그러나 이러한 보안 문제는 외부 경비를 강화하는 방법 외에는 다른 여지가 거의 없다.

두 번째 외부 IP 유입 문제의 경우 Fig.3.와 같이 IPv6를 사용하는 네트워크상에서 IoT 제품을 관리하기 때문에 이 부분의 보안이 중요하다. 의도하지 않은 외부 IP의 유입을 허용하게 되면, 지속적으로 패킷을 주고받아야 되는 네트워크의 특성을 역으로 이용하여 패킷 위변조를 하는 해킹이 발생할 수 있다. 이것은 시스템 자체의 오류 및 다수의 재고를 관리하는데 많은 문제를 가질 수 있기 때문에 반드시 고려해야 되는 요소이다. 앞서 선행연구에서 살펴보았듯, 외부 IP에 관한 호스트 정보의 자체적인 은닉/변조 부분까지 고려한 연구사례는 없었다. 이러한 외부 IP의 유입을 막기 위해 통합시스템 내에 접속을 허용할 수 있는 IP를 지정하고, 그 외의 IP주소는 막을 수 있어야 한다. 앞에서 주소 할당 방식을 제언 하였을 때, IP 주소의 자동설정 방식이 아닌 처음부터 고정할당 방식을 제언하였다. 이 때 이 고정할당 방식으로 받은 IP는 이미 IP주소 관리 기관에서 할당받은 IP주소를 이용하여 할당하기 때문에, 오히려 시스템에 접근할 수 있는 IP주소를 지정하는 것이 훨씬 간편해진다. 고정 IP의 보안성은 유동 IP 보다 우수하여 보안이 요구되는 정보를 관리하는 회사에서는 이미 많이 사용되고 있다.

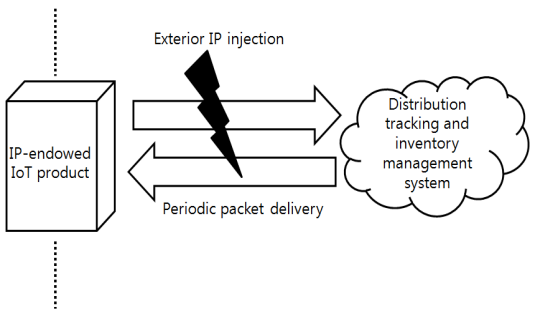


Fig.3. Exterior IP injection of distribution tracking and inventory management system

IPv6의 IP주소가 무한정 많다고 하나 시간이 갈수록 IoT 제품도 역시 무한정 늘어난다고 볼 수 있으며, IP 관리기관 역시 한번에 IP주소를 할당하는 것이 아니라 서서히 할당하기 때문에 필요한 경우 IP주소를 회수해야 한다. IP주소를 회수하기 위한 방법은 우선 상품이 소비자에게 전달된 경우를 생각해야 된다. 소비자가 IoT 제품을 구매하여 사용하는 동안에는 전력공급이 원활하게 이루어지기 때문에 IP 패킷이 끊기는 일이 발생하지 않는다. 게다가 그 제품이 냉장고나 TV와 같은 항시 전력이 들어가는 경우에는 끊기는 일이 일어나기 어렵다. 그러나 이러한 제품들도 더 이상 사용되지 않고 중고제품이나 혹은 폐기제품화 될 수 있는데, 이때 전력이 공급되지 않기 때문에 IP 패킷이 끊어지게 되고 이것을 시스템 상에서 확인하게 되면 IP 주소를 회수해야 된다. 또한, 시스템에 전력이 필요하고 항시 필요한 제품일수록 전력 끊김에 민감하기 때문에, 대략 1주일 동안 해당 IP패킷이 끊어지게 되면 다시 회수하는 방향으로 제언하고자 한다.

V. 결 론

IoT 확산에 맞추어 새로운 IP 체계인 IPv6로의 전환이 빨라지게 될 가능성이 높다. 특히 IPv6는 기존에 존재하던 IPv4보다 더 많은 장점과 성장 잠재력을 가지고 있다. 국내외 관련 기관에서도 보다 빠르게 전환을 하기 위한 노력을 하고 있으며, 여러 연구에서도 그 잠재력을 충분히 입증하고 있다. 그러나 물류관리 측면에서 보았을 때는 바코드 방식과 RFID를 이용한 관리시스템이 대부분의 물류관리시스템을 차지하고 있다. 이러한 방식들이 지금까지 계속 유지되고 있으나, 앞으로 IoT가 더욱 활성화 되어 관련 제품을 사용하는 사람들이 많아질수록 이러한 물류관리시스템은 도태될 것으로 예상된다.

본 논문은 기존의 바코드 방식이나 RFID 방식이 아닌 IoT 제품에 꼭 필요한 요소 중 하나인 IP 주소를 이용하여 IoT 제품을 관리할 수 있는 물류추적 및 재고관리 시스템을 제언했다. IPv6의 IP주소 수는 무한정에 가깝기 때문에 생산된 각 제품 당 하나의 이름을 부여하듯 고정적으로 IP 주소를 할당할 수 있다. 이러한 이유로 제품이 어디에 위치하고 있든지 네트워크 기반의 위치기반서비스를 이용하여 제품의 위치를 비교적 정확하게 파악할 수 있다. 그리고 이 기능과 제품회사의 ERP를 연결하여 제품의 이동현황이나 재고현황 및 사용현황을 도식화하여 나타낼 수 있는 가능성도 있다. 또한 유동적인 IP를 사용하는 것이 아니기 때문에 지정된 IP 주소를 제외한 모든 IP를 차단함으로써, 물류추적 및 재고관리 시스템의 안정성 및 보안성을 확보할 수 있을 것이다.

한편 일부 전문가들은 아무리 IPv6가 거의 무한대의 주소를 제공한다고는 하지만 예전의 IPv4 주소 사용량이 폭발적으로 증가한 점을 지적하여, IoT가 무한정 늘어나면서 IPv6 주소도 언젠가는 고갈될 수 있다고 예상한다. 그러나 IoT도 역시 하나의 물건이기 때문에 폐기될 수 있으며, 본 논문에서 제시한 것과 같이 IP주소를 효율적으로 회수할 수 있는 방안에 따라 IP주소의 사용량은 Fig.4.처럼 될 것으로 기대된다.

Fig.4.의 왼쪽 그래프는 IP주소의 회수를 고려하지 않았을 경우 IoT 수에 따른 IP주소 수 증가를 보여주는 그래프이다. 각 IoT 제품마다 하나의 IP주소를 부여받기 때문에 제품의 수가 늘어날수록 IP주소의 수도 동일한 숫자만큼 늘어난다는 의미이다. 아무리 IPv6의 주소 개수가 기존의 IPv4보다 세제곱만큼 많다고 하더라도 그 수량은 한정되어 있으며, IoT 제품이 일반화 되고 보급화가 진행될수록 IP주소의 부족 현상을 한 번 더 경험할 수도 있다. 그러나 본 논문에서 제언한 새로운 물류관리시스템 내에 존재하고 있는 IP주소를 제어하고 효율적으로 관리할 수 있는 시스템을 구현하게 되면, Fig.4.의 오른쪽 그래프처럼 변할 수 있다. IoT 제품이 향후 보편화 되더라도 지속적으로 발전하는 기술 변화에 맞추어, 뒤떨어지는 옛 제품이 존재하게 되고 그러한 제품들은 품목에서 사라지게 될 것이다. 이와 같이 더 이상 사용하지 않는 IP 부여 IoT 제품의 IP주소를 회수하게 되면, Fig.4.의 오른쪽 그래프처럼 일정량의 IP주소 증가 이후에는 증가폭이 서서히 줄어들면서 평형상태에 도달할 수 있으리라 예상된다. 즉, 일정한 IP주소 수의 증가 이후에는 IoT 제품이 증

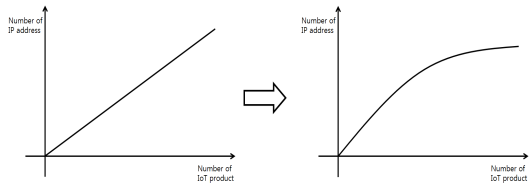


Fig.4. Estimation of IP address usage by number of IoT product

가하여도 그만큼 IP주소 수가 증가하지 않는다는 의미이다.

마지막으로, 본 논문에서 고려한 사항은 완성제품에 IP주소를 부여하는 부분부터 소비자에게 판매되기 직전까지의 물류관리를 상정하였기 때문에, 소비자가 사용할 경우의 IP주소 여부는 고려하지 않았다. 또한, IoT 제품이라고 하는 범위가 사물 간 통신할 수 있는 모든 제품 보다는 '대부분 실내에서 사용되는 IoT 제품'을 상정하여 관리시스템을 제언하였다. 그렇다고 하더라도 IP주소를 이용한 물류추적 및 재고관리 시스템은 기존의 물류관리시스템 연구자들에게 새로운 관점을 제시할 수 있을 것이며, IP주소의 새로운 가능성을 보여줄 수 있을 것으로 기대된다. 다만, 이 제언은 선험적이고 탐색적 성격을 가지고 있어서, 본 제안사항을 정교화하고 검증하는 추가 연구가 필요하다.

References

[1] M. Weiser, "The Computer for the 21st Century," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 3, no. 3, pp. 3-11, July 1999.

[2] Gartner, "2012 Gartner's Hype Cycle for Emerging Technologies," Aug. 2012.

[3] MarketandMarket, accessed at http://www.marketsandmarkets.com/

[4] DataNet, "IPv4 allotment, actually termination, " Apr. 14th, 2011.

[5] ITU, "ITU Internet Reports 2005, Internet of Things," Nov. 2005.

[6] IERC (European Research Cluster on the Internet of Things), accessed at http://www.internet-of-things-research.eu/

[7] Korea Communications Commission, "The fundamental plan of machine to machine basis construction," Oct. 2009.

[8] Tae-shik Shon and Jong-bin Ko, "Security trends of IoT (Internet of Things) in Cloud Computing," *Journal of the Korea Institute of Information Security and Cryptology*, 22(1), pp. 20-30, Feb. 2012.

[9] "M2M service requirements standardization," TTAK. KO-06.0301, TTA, ICT Standardization Committee, June 2012.

[10] Ho-won Kim and Dong-kyue Kim, "IoT technology and security," *Journal of the Korea Institute of Information Security and Cryptology*, 22(1), pp. 7-13, Feb. 2012.

[11] Ministry of Science, ICT and Future Planning, "IoT primary plan," May 2014.

[12] Chol-shik Pyo, "IoT technology trends," *The Journal of Korean Institute of Electromagnetic Engineering and Science*, 25(4), pp. 49-58, July 2014.

[13] "IoT technology and convergence service workshop," The Institute of Electronics and Information Engineers: M2M/IoT study society and IoT Forum, Jeju University, June 2014.

[14] Dong-il Lee, "Integrated IP address management system based on IP agents," Master Thesis, Ulsan University, Dec. 2013.

[15] S. Deering and R. Hinden, "Internet Protocol Version 6 (IPv6) Specification," RFC 2460, Dec. 1998.

[16] A. Conta, S. Deering, and M. Gupta, Ed.,"Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6(IPv6) Specification," RFC 4443, Mar. 2006.

[17] T. Narten, E. Nordmark, W. Simpson, and H. Soliman, "Neighbor Discovery for IP Version 6(IPv6)," RFC 4861, Sep. 2007.

[18] Ji-soo Oh, Ho-yeon Kim, Heon-jeong Lim, and Tae-myoung Jeong, "A Study on Privacy Issue for IPv6 Stateless Address Autoconfiguration," *The 35th Conference of the KIPS*, May 2011.

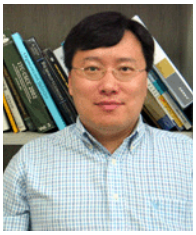
[19] Seong-goo Kang, Jae-kwang Kim, Kwang-sun Ko, and Young-ik Eom, "A Response Mechanism for Denying DoS Attacks abusing IPv6 Address Auto-configuration," *Proceedings I of The Korean Institute of Information Scientists and*

Engineers, 31(2), pp. 493-495, Oct. 2004.
〔20〕 Youn-ky Chung and Hae-eun Moon, "An Agent System for Searching of Host Computer and Blocking Network Access in IPv6 Environment," *Journal of Korea Multimedia Society*, 14(1), pp. 144-152, Jan. 2011.
〔21〕 CISCO, "CISCO Visual Networking Index: Global Mobile Data Traffic Forecast Update 2013-2018," Feb. 2014.
〔22〕 Kee-hun Sung, "IPv6 focus Internet of Things technology trends," Korea Internet & Security Agency, Aug. 2014.
〔23〕 Sun-mi Nam, Min-su Park, Kyung-shin Kim, and Seung-joo Kim, "A Study on the Regulations and Market of Location Based Service(LBS)," *Journal of Internet Computing and Services*, 15(4), pp. 141-152, Aug. 2014.
〔24〕 Hee-chan Lee, Joon-heong Lee, Zin-won Park, and Myung-kyun Kim, "Design and Implementation of IP address management system," *Proceedings I of The Korean Institute of Information Scientists and Engineers*, 32(2), pp. 232-234, Nov. 2005.
〔25〕 Sun-young Han, Sang-wook Bae, Min-soon Kim, So-ra Son, and Shim-in Sun, "Design and Implementation of the IPv6 Address Management Server for IPv6 Host Access Control," *Journal of Computing Science and Engineering*, 41(1), pp. 13-21, Mar. 2014.
〔26〕 Kyoung-jun Lee and Jeong-ho Jun, "IoT and business opportunity: smart things like omnipotent rice cooker adding recipe, bring about function revolution," *Donga Business Review*, 159, Aug. 2014.
〔27〕 Chang-hun Jung and Chul-jin Kim, "A Dynamic Location Recognition Technique for Location-based Service," *Journal of the Korea Academia-Industrial cooperation Society*, 15(7), pp. 4562-4572, July 2014.
〔28〕 Korea Communications and Commission, "The law of location information protection, use, and so forth (abbreviation: Location information law)," 〔Law number: 12840, revised and enacted in 2014/10/15〕
〔29〕 Soon-seok Kim and Yeoung-hun Kim, "Stock Management of Products and Location Tracking System Using RFID Technology," *Journal of Security Engineering*, 5(5), pp. 381-392, Oct. 2008.

〈저자소개〉

이 정 민 (Jeong-min Lee) 학생회원
2013년 2월: 창원대학교 정보통신공학과 졸업
2015년 2월: 한양대학교 정보시스템학과 석사
〈관심분야〉 정보보호, Bigdata, IoT

안 종 창 (Jong-chang Ahn) 정회원
1994년 2월: 고려대학교 경제학과 졸업
2002년 8월: 세종대학교 인터넷소프트웨어학과 석사
2007년 8월: 한양대학교 정보기술경영학과 박사
2010년 9월~현재: 한양대학교 정보시스템학과 조교수
〈관심분야〉 정보보호, 지식경영, 정보시스템 감사



이 욱 (Ook Lee) 정회원
1987년 2월: 서울대학교 계산통계학과 졸업
1989년 6월: Northwestern대학교 전산학과 석사
1997년 1월: Claremont대학교 경영정보학과 박사
2002년 3월~현재: 한양대학교 정보시스템학과 교수
〈관심분야〉 정보보호, IT 행태/철학/응용