ETRI

전자통신동향분석 제26권 제5호 2011년 10월

미래인터넷 보안 기술동향

Trend on the Future Internet Security Technologies

소프트웨어 기술의 미래전망 특집

이상우 (S.W. Lee) 인프라보호연구팀 선임연구원
서동일 (D.I. Seo) 인프라보호연구팀 팀장
조현숙 (H.S. Cho) 지식정보보안연구부 부장

목 차

약 40년 전 설계된 현재의 인터넷은 보안 취약점, 사용자 이동성 지원 부족, 효율적인 콘텐츠 전달의 어려움 등 많은 문제점에 직면하고 있다. 특히, 스마트폰, 스마트TV 등과 같은 인터넷 접속 디바이스의 폭발적인 증가 및 대용량 비디오 트래픽으로 인한 트래픽 폭증 현상에 대한 대처 방안을 마련하는 것이 시급하다. 또한, 7.7 DDoS(Distributed Denial-of-Service), 3.4 DDoS 대란 등의 네트워크 침해 사태에 대한 근본적인 대처 방안을 마련하는 것 역시 매우 중요하다. 이러한 현재 인터넷의 문제점을 해결하기 위하여, 기존 인터넷과의 호환성을 고려하지 않고, 네트워크를 새로이 설계하고자 하는 "미래인터넷" 연구가 시작되었다. 본 고에서는 최근의 미래인터넷 연구 동향을 살펴보고, 특히 보안성을 해결하고자 하는 미래인터넷 보안 기술의 동향을 소개한다.

Ⅰ. 서론

오늘날 인터넷은 네트워크를 통한 정보의 자유로운 공유를 통해서 사람의 생활 형태에 많은 변화를 가져왔다. 그러나, 현재의 인터넷은 40여 년 전 정보의 공유를 위하여 설계된 망으로써, 이동성, 보안성, 서비스 품질 보장성 등의 원천적인 한계점을 가지고 있다. 특히, 스마트폰, 스마트TV 등과 같은 인터넷 접속 디바이스의 폭발적인 증가로 인한 트래픽 폭증 현상에 대한 대처 방안을 마련하는 것이 시급하다. 또한, 7.7 DDoS(Distributed Denial-of-Service), 3.4 DDoS 대란 등의 네트워크 침해 사태에 대한 근본적인 대처 방안을 마련하는 것 역시 매우 시급하다. 상기한 인터넷의 문제점을 해결하기 위한 연구 동향은 크게 두 가지로 구분할 수 있다. 하나는 현재의 인터넷 체계를 그대로 유지하면서, 점진적으로 문제점을 해결해 나가는 연구 방향이고, 또 다른 하나는 기존의 인터넷 체계와의 호환성을 고려하지 않고, 네트워크 구조 자체를 새로이 설계해 나가자는 연구 방향이다[1],[2],[3],[4].

본 고에서는 완전히 새로운 구조의 인터넷을 설계하는 연구(이러한 접근 방법을 clean-slate approach라고 한다)동향을 살펴 보고, 특히 보안성을 해결하고자 하는 미래인터넷 연구 동향을 분석한다.

미래인터넷의 주요 연구 분야는 아래의 4가지 분야로 요약할 수 있다[5].

• 콘텐츠 중심의 네트워크 구조 연구

오늘날 트래픽 폭증의 주된 원인 중의 하나는 대용량의 비디오 트래픽이 차지하고 있는 점유율이 높아지기 때문이다. 특히, 주목할 만한 사실은 동일한 콘텐츠의 전송이 빈번하게 일어난다는 점이다. 이러한 현상은 현재의 인터넷이 host-to-host 통신을 기초로 하여 설계되었다는 데 기인한다. 즉, 현재의 서버-클라이언트 네트워크 구조는 Narrow waist IP (Internet Protocol) 모델에 기초하여, 다양한 서비스와 애플리케이션을 지원하기에는 용이하였으나, 콘텐츠를 제공하는 서버의 위치에 무관하게 사용자가 원하는 콘텐츠를 전달받기에는 적합하지 않은 구조이다. 따라서, 기존의 호스트 중심의 IP 네트워크를 콘텐츠 전달 중심으로 변경하기 위한 다수의 연구가 진행 중이다. 이러한 콘텐츠 중심의 연구에서는 콘텐츠의 네이밍 및 확장성 그리고 전달되는 콘텐츠의 보안성 등이 해결해야 될 이슈이다.

• 이동성 중심의 네트워크 구조 연구

오늘날 인터넷은 기존의 PC 기반에서의 컴퓨팅 환경에서 모바일 기반의 컴퓨팅 환경으로 급속히 패러다임이 변화하고 있다. 따라서, 이동성이 미래인터넷 연구에서의 중요한 이슈가 되고 있다. 즉, 셀룰러망, WiFi, 와이브로 등 다양한 네트워크 환경에서 사용자 단말의 이동성을 지원하기 위한 네트워크 구조의 요구사항이 증가하고 있는 실정이다. 이러한 이동성 중심의 연구에서는 이동성을 지원하면서도 효율적인 네트워크의 구성, 이동하는 사용자의 보안성 및 프라이버시 등이 해결해야 될 이슈이다.

• 클라우드 중심의 네트워크 구조 연구

데이터의 저장 및 컴퓨팅을 클라우드 중심 환경에서 수행하는 것이 새로운 인터넷 환경의 추세이다. 즉, 사용자는 클라우드에 접속할 수 있는 단말만 구비하고, 처리되는 데이터의 저장 및 컴퓨팅은 데이터 센터로 구성되는 클라우드에서 수행하게 된다. 따라서, 클라우드 중심 네트워크에서는 데이터 센터가 중요한 요소가 된다. 이러한 클라우드 중심의 연구에서는 사용자와 데이터 센터 간의 안전하고, 신뢰할 수 있으며, 또한 확장 가능한 네트워크 구조 설계 등이 해결

해야 될 이슈이다.

• 보안성 중심의 네트워크 구조 연구

오늘날 인터넷은 보안적인 측면이 설계 당시에 고려되지 않았다. 즉 현재의 IP 계층은 패킷의 전달 기능만 담당하고, 사용자 인증 및 전달되는 데이터의 무결성, 데이터의 보호를 위한 암호화 기능은 애플리케이션 영역에서 담당하도록 설계되었다. 따라서, 보안 기능을 네트워크 계층에서 원천적으로 수행하도록 설계하기 위한 다양한 연구가 진행 중이다. 특히 보안 이슈는 앞서 기술한 다양한 각도의 미래인터넷 연구, 즉 콘텐츠 중심, 이동성 중심, 클라우드 중심의 연구에서도 공통적으로 각 네트워크 구조 안에서 보안 기능을 제공할 수 있는 연구가 진행 중이다.

II. 미래인터넷 연구 동향

1. 국외의 연구 동향

본 절에서는 미국의 NSF(National Science Foundation)에서 추진 중인 연구 프로젝트를 소개한다. NSF에서는 FIA(Future Internet Architecture)라는 연구 프로젝트를 2010년 8월경에 시작하였다[6]. FIA 프로젝트는 <표 1>에 나타낸 바와 같이 연구 내용별로 4개의 세부 연구 프로젝트로 구성되어 있다[7],[8],[9],[10].

NDN(Named Data Networking) 프로젝트에서는 "Where"(호스트 또는 서버의 주소) 중심이 아닌, "What"(사용자가 원하는 콘텐츠) 중심으로 네트워크 구조 변화를 취하고 있다. 즉, 사용자가 특정 콘텐츠를 요청할 때, 해당 콘텐츠 서버에서 특정 콘텐츠를 제공하는 것이 아니라, 네트워크 상에서 해당 콘텐츠를 캐싱하고 있는 네트워크 노드가 사용자에 콘텐츠를 제공하는 방식으로 네트워크를 설계하고 있다. NDN 프로젝트에서는 라우팅의 규모성, 빠른 패킷 포워딩 메커니즘, 콘텐츠 보호 및 프라이버시에 관한 문제의 해결을 목표로 하고 있다.

〈표 1〉 NSF의 FIA 프로젝트

프로젝트	연구주제	주요 연구 기관
NDN	콘텐츠 중심	UCLA 외 9개 기관
Mobility-First	이동성 중심	Rutgers University 외 7개 기관
NEBULA	클라우드 중심	University of Pennsylvania 외 11개 기관
XIA	보안성 중심	Carnegie Mellon University 외 2개 기관

MobilityFirst 프로젝트는 사용자 또는 사용자 단말의 이동성을 고려한 네트워크 구조 설계에 관한 것이다. 현재의 인터넷은 가용성과 유연성 측면에서 우리의 생활을 크게 변화시킬 정도로 큰 변혁을 이루어 왔다. 그러나, 현재의 인터넷은 고정된 위치의 호스트 간의 통신을 고려하여 설계되었기 때문에, 사용자 또는 사용자 단말의 이동성을 끊김 없이(seamless) 지원하는 데는 한계가 있다. MobilityFirst 프로젝트 그룹에서는 통신 채널을 설정하는 데 있어서, 사용자 단말이 이동되는 것을 예외적인 사항으로 규정하지 않고, 근본적으로 단말이 이동되는 것을 고려하여 네트워크 구조를 설계한다. 사용자의 이동으로 인하여 통신 채널의 연결이 단절되었을 때도 데이터의 전송을 보장하는 DTN(Delay-Tolerant Network)를 기초로 하여 네트워크를 설계한다. 이러한 구조는 context-aware 서비스 또는 location-aware 서비스를 보장하는 것을 목표로 한다. MobilityFirst 프로젝트는 사용자 단말의 이동성 지원과 네트워크의 확장성 및 가용성 측면에서의 균형(trade-off), 그리고 이동 단말 간의 효율적인 통신 구조 설계를 목표로 하고 있다. 또한, 장기적으로 V2V(Vehicle-to-Vehicle) 및 V2I(Vehicle-to-Infrastructure) 통신을 이용한 차량 통신환경을 구축하는 것도 연구목표에 포함된다.

NEBULA의 사전적 의미는 성운을 뜻한다. 즉, 프로젝트의 이름에서 짐작할 있듯이, NEBULA는 클라우드 중심의 미래인터넷 구조 연구를 수행하는 프로젝트이다. NEBULA 프로젝트에서는 신뢰 가능하며, 고속의 연결성을 지원하는 데이터 센터의 구축, 데이터 센터와 코어 라우터 간의 병렬 경로 구축, 인증 메커니즘에 기초한 통신 채널 구축 등의 설계 목표를 가지고 네트워크 구조 연구를 진행 중이다.

XIA(eXpressive Internet Architecture) 프로젝트에서는 다양한 통신 개체(예를 들어, 호스트, 서비스, 콘텐츠 등)를 지정하고, 이들 간의 신뢰 통신을 제공하는 네트워크 구조에 대한 연구가 진행 중이다. 보안성은 앞 절에서 기술했듯이 다양한 미래인터넷 연구의 필수적인 요구사항이지만, XIA 프로젝트는 네트워크 계층 내부에서 본질적으로 제공하는 보안성(built-in security)을 목표로 하여 네트워크 구조 연구를 진행 중이다. 즉, 통신 개체들 간의 인증 및 전달되는 콘텐츠의 무결성을 네트워크 계층에서 본질적으로 제공하기 위한 네트워크 구조를 제안한다. XIA의 보다 상세한 분석은 다음 절에 기술한다.

EU에서도 미래인터넷에 대한 많은 연구가 진행 중이다. EU의 대규모 연구 프로그램인 FP7(Framework Program 7)의 ICT Challenge 1에서 미래인터넷 관련 연구가 진행되고 있다. FIA(Future Internet Assembly)는 미래인터넷 관련한 프로젝트의 협력 기구로서, FP7의 150여 개의 프로젝트를 수행 중에 있다[11]. 이 프로젝트들은 미래의 네트워크, 클라우드 컴퓨팅, 서비스의 인터넷(Internet of Services) 및 소프트웨어 엔지니어링, 신뢰 정보 통신, 네트워크형 미디어 및 검색 시스템, 미래인터넷 연구 및 실험 등의 다양한 주제를 다루고 있다. 특히, 신뢰 정보 통신 기술 분야의 목표는 통신, 컴퓨팅, 스토리지 등 다양한 인프라의 신뢰성을 제고하고, 보안성, 신뢰성, 프라이버시를 보장하는 새로운 네트워크 구조를 개발하며, 다양한 네트워크 및 시스템에 적용할 수 있는 안전한 인터페이스 및 위기상황을 자율적으로 모니터링 할 수 있는 플랫폼 및 시스템 개발이다.

2. 국내의 연구 동향

국내에서는 2006년부터 미래인터넷포럼 등을 중심으로 미래인터넷 연구가 시작되었다[12]. 미래인터넷포럼은 미래인터넷 연구에 관심 있는 학계, 연구소, 산업체의 자발적인 연구 그룹으로서, 포럼 산하에는 세부 연구 주제에 따라 Architecture, Wireless, Service, Testbed, Security 워킹 그룹이 결성되어 연구를 진행하고 있다. 또한, ETRI, 서울대, KAIST 등의 기관에서 네트워크 가상화 지원 및 프로그래머블 플랫폼 개발, 미래인터넷에서 이동환경 및 네트워크 다양성 지원 구조 연구, 이름 주소 기반 네트워킹 기술 연구, 이동통신 네트워크 응용을 위한 DTN 기술 개발 등이 진행 중이다. 한편, FN2020 포럼은 미래 한국의 IT 인프라 비전과 전략을 제시하고 새로운 성장 동력을 모색하기 위해 지난 해 설립되었다[13]. FN2020 포럼에서는 스마트 네트워크 구축을 최우선 과제로 연구 전략을 수립하고 있다.

Ⅲ. 미래인터넷 보안 기술 분석

앞서 기술했듯이, XIA는 보안성을 최우선 해결 목표로 선정하고 이를 위하여 연구되고 있는 프로젝트이다. 본 절에서는 XIA 프로젝트에서 제시하는 요구사항, 서비스 시나리오, 주소 체계 등을 살펴보고, XIA의 선행 연구인 AIP(Accountable Internet Protocol)의 내용을 분석한다[14],[15].

1. XIA

XIA에서의 목표는 다양한 형태의 통신 개체를 지원하고, 네트워크 계층 내부에서 본질적으로 보안성을 제공하면서, 현재 인터넷의 장점인 Narrow waist 모델을 따르는 네트워크 구조를 설계하는 데 있다. 이러한 목표를 달성하기 위하여 Principal이라는 용어를 정의한다. Principal은 다양한 통신 개체를 의미한다. 예를 들어, 호스트, 서비스, 콘텐츠 등을 들 수 있다. 즉, 기존의 호스트 간의 통신이 아니라, 패킷을 전송할 때, 어떤 서비스를 위하여 패킷을 전송하는 지, 어떤 콘텐츠를 받기 위하여 패킷을 전송하는 지를 명시적으로 표현하도록 하기 위하여, Principal을 정의하고 이들 간의 통신을 지원한다.

XIA에서 제시하는 요구사항은 다음과 같다.

- 사용자 및 애플리케이션은 통신하고자 하는 의도를 명확히 표현해야 한다.

즉, 사용자 또는 애플리케이션이 패킷을 전송할 때, 어떤 서비스를 위하여 패킷을 전송하는 지, 어떤 콘텐츠를 받기 위하여 패킷을 전송하는 지를 명시적으로 표현할 수 있어야 한다는 것이다. 이렇게 함으로써, 현재 인터넷에서는 IP 계층에서 단순한 패킷 포워딩만 수행하는 것과 달리, 네트워크 계층에서 패킷이 전송되는 의도에 따라 패킷의 캐싱, 콘텐츠 중심의 라우팅 등의 네트워크 최적화가 가능하다.

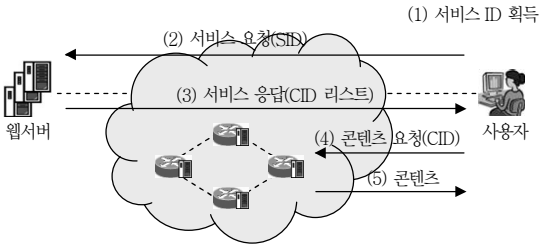
- Principal 형태는 진화 가능해야 한다.

즉, 새로운 형태의 Principal을 추가하는 것이 가능해야 하고, 또한, 추가하는 작업이 쉽게, 그리고 점진적으로 이루어질 수 있어야 한다.

- Principal ID는 내재적으로 안전해야 한다.

임의의 Principal은 올바른 Principal과 통신하고 있음을 검증할 수 있어야 한다. 이것은 Principal의 형태에 따라 다를 수 있다. 호스트 간의 통신에서는 송수신 호스트가 서로를 인증할 수 있어야 하며, 콘텐츠 전달에 있어서는 콘텐츠의 무결성을 검증할 수 있어야 한다.

사용자가 웹페이지를 수신하는 서비스 시나리오를 (그림 1)에 나타내었다. 그 절차는 다음과 같다.



(그림 1) 서비스 시나리오

(1) 사용자의 웹 브라우저가 웹 검색, 북마크, 또는 DNS(Domain Name Service) 서비스 등을 이용하여 해당 사이트(예: site.com)의 서비스 ID를 획득한다. 여기서, 서비스 ID는 서비스를 제공하는 홈페이지의 공개키의 해시 값으로 구성된다.

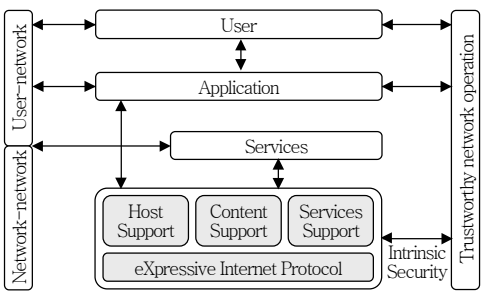
(2) 사용자의 웹 브라우저는 앞서 찾은 서비스 ID를 목적지 주소로 가지는 서비스 요청(request) 패킷을 서비스 제공자에게 전송한다. 여기서, 주목할 점은 서비스 제공자의 호스트 ID가 아니라, 서비스 ID를 목적지 주소로 사용한다는 점이다. 이렇게 함으로써, 네트워크에서는 해당 서비스를 제공하는 보다 가까운 서비스 호스트에게 패킷을 전송할 수 있게 된다.

(3) site.com 서비스는 요청 패킷을 전송한 호스트 ID를 목적지 주소로 지정하여 응답 패킷을 전송한다. 이 때, 웹페이지를 구성하는 콘텐츠들의 콘텐츠 ID를 함께 전송한다. 이 때, 전송되는 응답 패킷은 site.com이 서명한 메시지로서, 사용자는 이 서명을 검증함으로써 정당한 서비스로부터의 응답임을 검증할 수 있다.

(4) 사용자의 웹 브라우저는 서비스 제공자로부터 제공받은 콘텐츠 ID를 목적지 주소로 지정하여 요청 패킷을 전송한다.

(5) 사용자는 요청한 콘텐츠를 제공받는다. 이 때, 콘텐츠 제공자에 상관 없이, 가까운 위치의 콘텐츠 제공자 또는 네트워크에 캐싱되어 있는 콘텐츠를 제공받는다. 사용자의 웹 브라우저는 수신된 콘텐츠의 해시 값과 콘텐츠 ID가 일치하는지를 확인하여, 콘텐츠의 무결성을 검증한다. 이 때, 네트워크에 캐싱되어 있지 않은 콘텐츠의 경우에는 site.com의 서비스 ID를 이용하여 해당 서비스를 제공하는 콘텐츠 제공자에게 콘텐츠 제공 요청을 하게 된다.

XIA의 데이터 처리 계층을 (그림 2)에 나타내었다. 데이터 처리 계층은 크게 두 부분으로 구성된다. 하나는 XIP(eXpressive Internet Protocol) 계층이고, 또 다른 하나는 Principal 맞춤형 지원 계층이다. XIP는 모든 Principal들에게 적용되는 공통적인 주소 체계와 헤더 포맷 및 포워딩 프로세싱을 정의하는 프로토콜 계층이다. Principal 맞춤형 지원 계층은 각각의 Principal 형태에 최적화된 포워딩 프로세싱을 정의하는 계층이다. 예를 들어, 호스트 형태의 Principal의 경우에는 전통적인 인터넷 라우팅 및 포워딩 메커니즘을 이용할 수 있다. 콘텐츠 형태의 Principal의 경우에는 호스트 중심의 라우팅을 하기 전에 로컬



(그림 2) XIA 데이터 처리 계층

캐시를 체크하는 메커니즘이 추가될 수 있다.

XIA에서 Principal 형태를 구분하는 식별자를 XID라고 정의한다. XID 중에서 호스트는 HID(Host Identifier), 서비스는 SID(Service Identifier), 콘텐츠는 CID(Contents Identifier), 관리 도메인은 AD(Autonomous Domain)로 정의한다. HID, SID, 및 AD는 각각의 Principal의 공개키의 해시 값이고, CID는 콘텐츠 자체의 해시 값이다. 여기서, 해시 값을 생성할 때는 암호학적 해시 알고리즘인 SHA-1, RIPEMD-160 등을 사용한다. XID는 AIP의 자가 보증형(self-certifying) ID를 도입한 것이다. 여기서, 자가 보증 식별자의 의미는 제3자의 개입 없이 자신의 정당성을 상대방에게 증명할 수 있는 ID를 의미한다. 즉, 오브젝트의 이름 자체를 해당 오브젝트의 공개키 또는 공개키의 해시를 사용하는 것이다. (그림 3)은 ID의 구조를 나타낸 것이다. (그림 3)에서 각 필드의 의미는 다음과 같다.

Crypto vers (8)	Public key hash (144)	Interface (8)

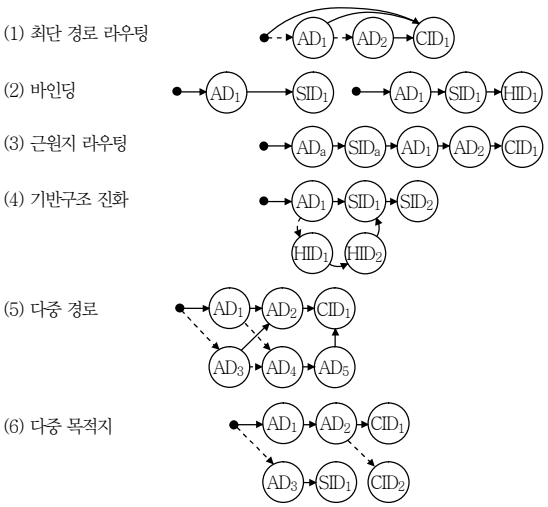
(그림 3) ID 구조

- Crypto vers: 서명 알고리즘과 해시 알고리즘의 종류를 정의
- Public key hash: 특정 Principal의 공개키의 해시 값
- Interface: 해당 ID를 갖는 Principal이 네트워크에 접속하는 인터페이스를 구분하기 위한 인덱스. 예를 들어, 하나의 호스트가 유선 및 무선 이더넷에 동시에 접속했을 경우, 이들의 인터페이스를 구분하기 위함임.

XID는 Principal의 형태를 구분하고, 각각의 Principal에 적합한 통신 메커니즘을 적용하기 위하여, 유일한 값을 가져야 한다. 따라서, XID는 충돌을 회피하는 방법으로 생성되어야 하고, 자가 보증형 특성을

만족하기 위하여, 이상적으로는 중앙 집중 기관의 도움 없이 생성되어야 한다. 따라서, XID를 생성할 때, Principal의 공개키의 암호학적 해시 값을 이용하여 생성하게 된다.

XIA에서는 XID를 연접시켜서 주소를 구성한다. XIA에서의 주소 체계 및 라우팅 방법의 예는 (그림 4)와 같다. 가장 좌측의 검은 점이 시작 노드를 의미하고, 가장 우측이 최종 목적지를 의미한다. 노드로부터 출발하는 경로가 여러 개인 경우, 윗부분에 표시된 노드가 우선 순위가 높다.



(그림 4) 주소 형태 예제

(1) 최단 경로 라우팅: 목적지의 주소가 최종 의도, 즉 CID_1 및 CID_1에 이르는 경로를 표현하는 경우이다. 그림에서 표현했듯이 모든 노드는 최종 목적지 CID_1를 향하는 경로를 가지게 된다. 구체적인 예로, 최단 경로 라우팅은 콘텐츠 캐싱 라우터로 하여금 CID 쿼리에 대한 응답을 원래의 목적지로 포워딩하는 것이 아니라 직접적으로 응답을 전송할 수 있게 한다.

(2) 바인딩: 특정 근원지와 목적지가 고정되어야 하는 통신의 경우, 예를 들어, 기존의 HTTP 통신을 그대로 서비스 하는 경우의 주소 체계 예제이다. 첫 번째 패킷은 SID를 서비스하는 어떤 호스트에도 전송될 수 있다. 하지만, 그 뒤에 연속되는 TCP 패킷들은 반드시 첫 번째 패킷이 전달되었던 호스트로 전송되어야 한다.

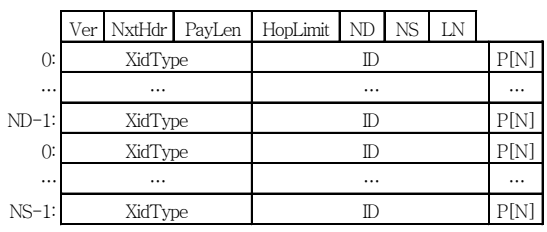
(3) 근원지 라우팅: XID가 연접되는 주소 체계는 근원지에서 라우팅 경로를 설정하는 근원지 라우팅으로도 데이터가 전달될 수 있다.

(4) 기반구조 진화: 이것은 기존의 인터넷 프로토콜을 사용한 기존 시스템과의 호환성을 제공한다. 예를 들어, AD_1의 SID_1으로 전송되어야 하는 패킷이 있을 때, AD_1에서 SID_1으로의 라우팅 경로가 지원되지 않을 경우, 기존의 호스트 간 통신 상에서의 경로(HID_1, HID_2)를 이용한 패킷 전달이 가능하다.

(5) 다중 경로: 이것은 다중 경로를 통하여 목적지로 패킷 전달이 가능한 것을 의미한다. 다중 경로 라우팅은 WiFi 및 이동통신망을 이용하는 스마트폰에서의 데이터 전송 시 발생할 수 있다.

(6) 다중 목적지: XIA의 주소 지정 방법으로 다중 목적지에 대한 라우팅이 가능하다.

XIA에서의 패킷 헤더 포맷은 (그림 5)와 같다. 그림에서 XidType은 Principal 형태를 지정하기 위하여 4바이트를 할당하고 있다. ID는 HID, SID 및 CID 등과 같은 XID를 의미하고, 20바이트로 구성된다. ND는 목적지 주소의 크기를 의미하고, NS는 근원지 주소의 크기를 의미한다. XIA 주소 체계에서 각각의 노드는 다음 홉으로 패킷을 전송하기 위한 4개의 출



(그림 5) 패킷 헤더 포맷

력 경로를 가진다. 이것을 구분하기 위하여 4개의 1 바이트로 구성되는 P[N]이 사용된다.

2. AIP

현재의 IP 계층은 위조된 근원지로부터 전송되는 악성 패킷을 차단할 수 없다는 보안 취약성을 가지고 있다. 이러한 문제를 해결하기 위하여 AIP는 IP 계층에 책임성(accountability)을 부여하자는 목적의 프로토콜이다. 즉, IP 계층에서 패킷의 단순 전송만 하는 것이 아니라, 패킷의 근원지 주소와 실제 패킷이 유입된 경로가 일치하는 지를 확인하는 기능을 수행하고자 하는 것이다.

AIP에서는 호스트의 ID를 EID로 표기하고, 관리 도메인 상의 라우터를 AD로 표현한다. XIA에서 사용하는 주소 체계의 근간이 되는 AIP의 주소 체계는 자가 보증형 ID를 연접시키는 방식으로 구성된다. AIP에서는 라우터에서 유입되는 패킷의 근원지를 검증하여, 검증된 패킷만 다음 홉으로 포워딩 함으로써, 근원지가 위조된 패킷의 유통을 원천적으로 차단하는 프로토콜을 제시한다.

패킷의 근원지를 검증하는 절차는 크게 두 과정으로 구성된다. 하나는 사용자의 네트워크 접속 지점에 존재하는 라우터(첫 번째 라우터)에서의 EID 검증 과정과 또 다른 과정은 네트워크 상에 존재하는 라우터에서의 AD 검증 과정이다. 즉, 첫 번째 라우터에서는 호스트의 주소가 위조되었는 지를 검사하게 되고, 네트워크 상의 라우터에서는 이전 홉이 위조되었는 지를 검사하게 된다.

첫 번째 라우터에서의 EID 검증 절차는 다음과 같다.

(1) 수신된 패킷의 근원지 주소가 검증된 패킷 저장용 캐시에 존재하는가를 검증한다.

(2) 그렇다면, 패킷을 다음 홉으로 포워딩한다.

(3) 그렇지 않다면, 수신된 패킷을 버리고, 근원지 검증 프로토콜을 수행한다.

(4) 근원지 검증 프로토콜 수행 결과가 정상이면 해당 근원지 주소를 캐시에 저장하고, 패킷 송신자는 이전에 보낸 패킷을 첫 번째 라우터에게 재전송한다.

상기한 근원지 검증 프로토콜은 다음과 같다.

(1) 첫 번째 라우터가 해당 패킷의 근원지로 검증 패킷 V를 전송한다. V는 해당 패킷의 근원지 및 목적지 주소, 해당 패킷에 대한 해시 값 H<P>와 패킷이 도착한 인터페이스 값 iface로 구성되고, 이 값들을 연접한 값을 첫 번째 라우터만이 알고 있는 비밀 값인 rs를 키로 사용하여 HMAC(Hash-based Message Authentication Code)한 결과이다.

(2) V를 수신한 패킷 송신자는 EID와 연관된 개인키를 이용하여 V에 대한 서명 값을 생성하고, 이것을 첫 번째 라우터에게 전달한다.

(3) 서명 값을 수신한 첫 번째 라우터는 패킷 송신자의 서명을 검증한다.

네트워크 상의 라우터에서의 AD 검증 과정은 다음과 같다. AD_B로부터 AD_A로 패킷이 전달되었을 때, AD_A는 다음과 같은 절차를 수행하게 된다.

(1) AD_A가 AD_B로부터 수신한 패킷의 근원지에 대한 신뢰가 있다면, AD_A는 수신한 패킷을 포워딩한다.

(2) 만약 AD_A가 AD_B를 신뢰할 수 없다면, uRPF(Unicast Reverse Path Forwarding) 프로토콜을 수행하여 패킷이 수신된 인터페이스와 패킷의 근원지 주소가 일치하는 지를 검증한다. 그 검증 결과가 정상이면, AD_A는 패킷을 포워딩한다.

(3)앞 단계의 검증 결과가 비정상이면, 패킷을 버리고, EID 검증 과정에서의 패킷 V를 근원지에게 전송하고, 근원지 검증 프로토콜을 수행한다.

(4)근원지 검증 프로토콜 수행 결과가 정상이면 해당 근원지 주소를 검증된 패킷 저장용 캐시에 저장한다.

Ⅳ. 결론

본 고에서는 미래인터넷의 국내외 동향을 분석하고, 특히, 미래인터넷 보안 기술 관련한 대표적인 연구 내용을 분석하였다. 미래인터넷의 정보보호 요구사항은 3가지로 요약할 수 있다. 첫째, 보안 기능은 추가적인 기능이 아니라, 네트워크 내부에서 원천적으로 제공되어야 한다. 둘째, 악성 패킷이 유통되지 않는 네트워크를 구성하기 위하여, 패킷 전달 계층에서의 신뢰성이 보장되어야 한다. 셋째, 네트워크 침해사고 발생 시 공격자를 추적할 수 있어야 한다.

혁신적인 네트워크를 설계하고자 하는 미래인터넷 연구는 현재 인터넷의 문제점을 해결하기 위하여 특화된 목적을 해결하고자 하는 다양한 연구가 진행중이다. 예를 들어, 콘텐츠 전달 중심망을 설계하여 트래픽 폭증에 대처하기 위한 연구, 사용자의 이동성을 네트워크 계층에서 원천적으로 해결하고자 하는 연구 등을 들 수 있다. 여기서, 우리는 다양한 미래인터넷 연구들이 모두 해결하고자 하는 각기 다른 첫 번째 목표 외에 공통적으로 보안성을 설계 요구 사항에 반영하고 있다는 것을 주목할 필요가 있다. 즉, 미래인터넷 연구에서 있어서, 보안성이라는 문제는 어떠한 네트워크 구조가 되더라도 해결해야 하는 가장 중요한 요구사항이라는 점이다. 따라서, 다양한 설계 목표를 만족하는 연구와 더불어, 보안성의 중요성을 인식하고 이에 대한 연구가 진행되어야 할 것이다.

● 용 어 해 설 ●

미래인터넷(Future Internet): 현재 인터넷의 문제를 극복하기 위해 현재의 인터넷과의 호환성을 고려하지 않고, 혁신적인 구조로 설계되는 미래의 인터넷

자기보증형 식별자(self-certifying ID): 제3자의 개입 없이 자신의 정당성을 상대방에게 증명할 수 있는 식별자

Principal: XIA에서 다양한 통신 개체를 의미함(예: 호스트, 서비스, 콘텐츠 등).

약어 정리

AD	Autonomous Domain
AIP	Accountable Internet Protocol
CID	Contents Identifier
DDoS	Distributed Denial-of-Service
DNS	Domain Name Service
DTN	Delay-Tolerant Network
EID	Endpoint ID
FIA(미)	Future Internet Architecture
FIA(EU)	Future Internet Assembly
FP7	Framework Program 7
HID	Host Identifier
HMAC	Hash-based Message Authentication Code
IP	Internet Protocol
NDN	Named Data Networking
NSF	National Science Foundation
SID	Service Identifier
uRPF	Unicast Reverse Path Forwarding
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
XIA	eXpressive Internet Architecture
XIP	eXpressive Internet Protocol

참 고 문 헌

[1] 서동일, 장종수, 조현숙, “미래인터넷 정보보호 요구사항,” 한국인터넷정보학회, 제10권 제4호, 2009. 12.

[2] 변성혁, “미래인터넷 아키텍처 연구 동향,” 전자통신동향분석, 제24권 제3호, 2009. 6.

[3] 김영화, “미래인터넷의 네트워크 가상화 기술 동향,” 전자통신동향분석, 제25권 제1호, 2010. 2.
[4] 김대영, “미래인터넷 개념 및 현황,” 한국통신학회지, 제27권 제10호, 2010. 10.
[5] J. Pan et al., “A Survey of the Research on Future Internet Architecture,” *IEEE Commun. Mag.*, July 2011.
[6] NSF, Future Internet Architecture Project. http://www.nets-fia.net
[7] Named Data Networking Project. http://www.named-data.net
[8] MobilityFirst Future Internet Architecture Project. http://mobilityfirst.winlab.rutgers.edu
[9] NEBULA Project. http://nebula.cis.upenn.edu
[10] eXpressive Internet Architecture Project. http://www.cs.cmu.edu/~xia
[11] Future Internet Assembly. http://www.future-internet.eu
[12] 미래인터넷 포럼. http://fif.kr
[13] FN2020 포럼. http://www.fn2020.or.kr
[14] A. Anand et al., “XIA: An Architecture for an Evolvable and Trustworthy Internet,” Technical Report CMU-CS-11-100, Feb. 2011.
[15] D. Anderson et al., “Accountable Internet Protocol (AIP),” *Proc. ACM SIGCOMM*, Aug. 2008.