P2P 관련 국제 표준화 동향

고선기* 권혁찬** 나재훈***

P2P(Peer-to-Peer)는 서버의 도움없이 PC간 일대일 통신을 가능하게 하는 기술이며, 그 활용 분야는 매우 광범위하다. P2P의 궁극적인 목표인 유비쿼터스 정보화 사회를 성공적으로 구축하기 위해서는 앞으로 더욱 많은 노력들이 필요하며, 무엇보다도 표준화가 선행되어야 한다. 최근 IETF(Internet Engineering Task Force), ITU-T(ITU Telecommunication Standardization Sector) 등 표준화기구들에서 P2P 관련 표준화 활동이 점차적으로 증가되고 있는 추세이다. 본 고에서는 IETF, ITU-T, ASTAP(Asia-Pacific Telecommunity Standardization Program)에서의 P2P 관련 표준화 활동을 소개하고, 향후 표준화 진행 방향을 살펴본다. ▧

목 차

* ETRI P2P 보안연구팀/연구원
** ETRI P2P 보안연구팀/선임연구원
*** ETRI P2P 보안연구팀/팀장

I. 서 론

최근 현대인의 일상생활에 많은 변화를 가져오는 컴퓨터 관련 기술 중 하나가 P2P(Peer-to-Peer) 기술이다. P2P 기술은 이미 일상생활의 일부분이 되어버린 인스턴트 메신저, 인터넷 폰, 음악/동영상 파일 공유, 멀티미디어 서비스, 온라인 게임 등 수많은 분야에서 널리 사용되고 있으며, 가까운 미래에 모든 디지털 장치가 자유롭게 연결될 유비쿼터스 정보화 사회를 건설하는데 중요한 기술이기도 하다. P2P 기술은 우리에게 이러한 밝은 미래를 보여주는 반면, 취약한 보안성, 과다 트래픽 유발, 저작권 관련 법정 소송 등의 어두운 면을 드러내며 많은 우려를 낳기도 한다. 2005년 NGN2005에서 발표된 통계에 따르면, P2P가 인터넷에서 가장 많은 트래픽을 발생하는 서비스인 것으로 밝혀졌다[1]. 또한 국내외적으로 P2P로 인한 개인정보나 기밀 유출사고가 잦아지고 있고, P2P를 이용한 해킹의 위험성도 매우 높아지고 있다. 이러한 문제점들을 극복하면서 유비쿼터스 정보화 사회로의 발걸음을 가속화하기 위해서는 P2P 기술에 대한 학계와 업계의 더욱 많은 관심과 노력이 필요하며, 무엇보다도 P2P 관련 기술의 표준화가 먼저 선행되어야 한다. 본 고에서는 먼저 P2P 기술에 관한 간략한 소개와 함께, IETF, ITU-T와 같은 국제 표준화 기구들에서의 P2P 관련 표준화 동향, 그리고 앞으로의 표준화 진행 방향을 살펴보기로 한다.

II. P2P 기술 개요

1. Terminology

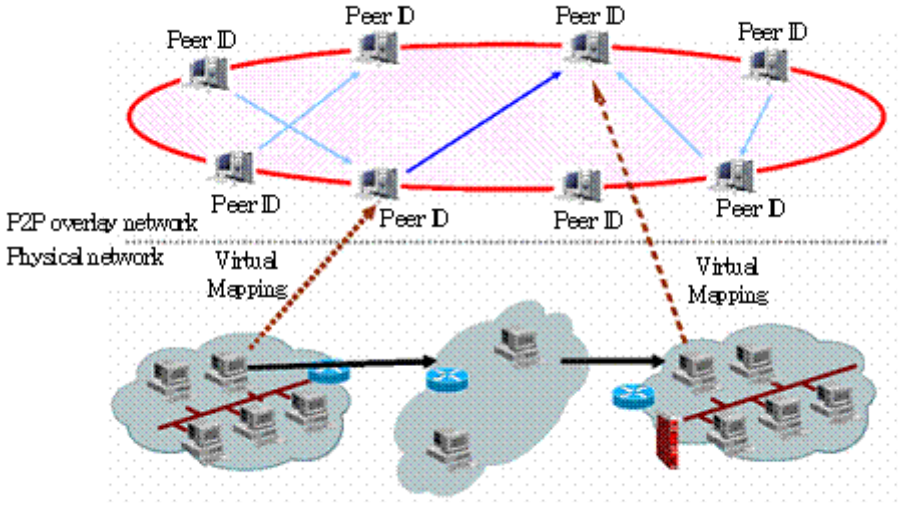
① 오버레이 네트워크(Overlay Network): 기존의 네트워크가 제공하지 않는 네트워크 서비스를 수행할 목적으로, 기존의 네트워크 위에서 설정된 노드들(nodes)과 논리적 링크들 (logical links)로 이루어진 가상 네트워크를 말한다. 따라서 오버레이 네트워크에서 이웃노드들은 물리적인 이웃 노드가 아니라 논리적인 이웃 노드이다.

② P2P(Peer-to-Peer): 참여자들이 자신의 하드웨어 자원(resource)을 서로 공유하는 분산 네트워크 아키텍처의 일종이다 (예: 프로세싱 파워, 저장 용량, 네트워크 링크 용량, 프린터 등). 그리고 여기서 공유된 자원들은 그 P2P 네트워크에서 제공되는 서비스와 콘텐츠를 공급하는데 쓰인다(예: 파일 공유, 작업공간 공유 등). P2P 네트워크에서는 서버없이 모든 노드들이 서버와 클라이언트의 역할을 동시에 수행하며 직접적인 교환을 통해 디지털 자원을 함께 공유한다.

③ DHT(Distributed Hash Table): 분산 컴퓨팅을 위해 안전한 lookup 메커니즘을 제공할 목적으로, 분산된 위치에 Hash Table들을 저장하는 기술이다. 1990년대 중반에는 주로 LAN 에서 쓰였는데, 현재는 인터넷상의 Structured P2P 네트워크를 구성하는데 쓰인다.

2. P2P 오버레이 네트워크

P2P 기술은 기존의 Client-Server 개념과 달리 PC 들이 연결되어 자원을 공유하고 모든 참여자가 서버인 동시에 클라이언트의 역할을 수행하는 특징을 갖는다. (그림1)에서 보여지듯이, 물리적 네트워크상에 존재하는 피어(Peer)들이 P2P 서비스에 등록하면, 등록된 피어들 간의 가상 네트워크, 즉, P2P 오버레이 네트워크가 만들어진다. P2P 오버레이 네트워크상에서 피어들은 서버의 도움없이 다른 피어들과 직접 정보를 공유하고 교환할 수 있다. 이러한 P2P 컨셉은 단순히 컴퓨터와 컴퓨터가 연결됨을 의미할 뿐만 아니라, 인간과 인간이 직접 1:1로 연결됨을 의미한다. 이와 같은 사회문화적 특성으로 인하여, 현재 P2P 기술은 개인을 중시하고 개방화를 지향하는 21세기 인터넷 사이버 공간에서 새로운 문화 창조의 주도적인 역할을 하고 있다.



(그림 1) P2P 오버레이 네트워크

3. P2P 네트워크의 종류

P2P 네트워크는 크게 두 가지로 나뉜다. 하나는 서버에 먼저 접속해야만 다른 피어와 접속이 가능한 중앙집중형 (Centralized) P2P 방식이고, 다른 하나는 서버의 도움없이 피어들이 서로 IP주소 등의 정보를 공유함으로써 피어간 직접 연결이 가능한 분산형(Distributed) P2P 방식이다. 중앙집중형 P2P방식도 일단 서버의 도움으로 접속과 검색이 이루어진 후에는, 분산형 P2P 방식과 마찬가지로 피어들끼리 직접 통신하여 자료를 공유한다. 또한 P2P 네트워크는 노드간 연결 구조 방식에 따라 분류될 수 있는데, 노드간의 임의적인 연결에 의해 구성되는 비구조적(Unstructured) 방식, 그리고 정의된 방식에 따라 체계적이고 규칙적으로 형성되는 구조적(Structured) 방식으로 나누어진다. 기존의 P2P 네트워크들을 구조적/비구조적 방식에 따른 분류 방법으로 나누어 보면 아래와 같다[23].

가. Unstructured 방식

① Flooding: Gnutella(초기), Kazaa(초기), BitTorrent

② Random Walk: Gnutella(현재), Kazaa(현재), LMS

나) Structured 방식은 Routing 또는 Topology에 따라 아래와 같이 분류할 수 있다.

A. Routing

① 2nd Generation Multi-Hop: Chord, Pastry, CAN, Tapestry, Kademlia

② One Hop: Epichord
③ Variable Hop: Accordian
B. Topology
① Flat: Chord, Pastry, CAN, Tapestry, Kademlia, Epichord, Accordian
② Super Node: JXTA
③ Hierarchical & Multi-Ring: TOPLUS

또한 P2P는 서비스 목적에 따라 Instant Messaging, File Sharing, Distributed Computing 등으로 나눌 수 있다.

① Instant Messaging: MSN Messenger, ICQ, JPPP
② File Sharing: Gnutella, Napster, eDonkey, 소리바다
③ Distributed Computing: SETI, Groove(Virtual Office), KOREA@Home

III. P2P 관련 국제 표준화 동향 개요

P2P 관련 표준화 활동은 IETF(Internet Engineering Task Force)와 ITU-T(ITU Telecom-uiation Standardization Sector)와 같은 국제 표준화 기구들과 Sun Microsystems와 같은 기업들을 중심으로 이루어지고 있다. 본 장에서 그 활동에 관한 대략적인 개요를 설명하고, 이어지는 제IV, V, VI장에서 각각 IETF, ITU-T, ASTAP 에서의 P2P 관련 표준화 동향을 구체적으로 살펴보기로 한다.

먼저, IETF 에서는 작업그룹 xmpp가 2004년까지 총 4건의 RFC를 등록함으로써 IM (Instant Messaging) 분야의 표준화 작업을 완료한 상태이다. 그리고 2006년 3월에는 P2P기반 SIP네트워크의 표준화를 위한 작업그룹 p2psip가 새로이 제안될 것으로 예상되고 있는데, 그에 대한 사전 준비작업으로 sipping, sip 등 기존의 SIP 관련 작업그룹들에서 8건의 드래프트가 제출된 상태이므로 이들의 향후 움직임을 주시할 필요가 있다. 또한 2003년에 조직된 연구그룹(Research Group: RG) p2prg에서는 P2P 표준화 작업의 기초를 제공하기 위한 연구를 진행하고 있다.

한편 Sun Microsystems은 현재 Project JXTA을 통하여 공개 P2P 프로토콜 프레임워크를 개발하고 있는데, 어떠한 운영체제, 시스템에서도 운용될 수 있는 P2P 네트워크를 위한 프로토콜 표준을 제공하는 것을 목표로 하고 있다. Sun은 2002년, IETF내에 P2P 작업그룹을 조직하여 JXTA를 표준으로 추진하려고 시도하였으나 실패하였다. 그러나 JXTA는 현재도 누구나 참여할 수 있는 공개된 환경 하에서 꾸준히 연구개발이 진행중에 있다.

ITU-T에서는 많은 공공 및 민간 단체들이 ITU-T 내에서 표준 개발을 위하여 상호 협력해 오고 있다. 2005년 10월, 스위스 제네바에서 있었던 Study Group 17 회의에서 Question 9/17에 P2P 네트워크 보안 프레임워크, 익명 인증 아키텍처 등에 관한 기고서 3건이 제출되었고, 한국과 일본이 P2P 관련 프로젝트를 각각 하나씩 맡기로 결정되었다. 최근 중국도 2건의 관련 기고서를 제출하며 프로젝트에 참여할 의지를 보이고 있다. 2006년 4월 제주도에서 열리는 SG. 17 회의에서 이 프로젝트들에 관련한 후속 활동이 예상된다.

IV. IETF 표준화 동향

IETF는 공식적인 멤버쉽 없이 자발적으로 참여하는 순수한 자원자들로 이루어진 표준화 기구이며, 공개적으로 인터넷 표준을 개발하고 홍보하는 일을 한다. IETF는 많은 작업그룹(Working Group: WG)들로 조직되어 있는데, 각각의 작업그룹은 특정한 주제를 다루며, 작업그룹은 주어진 주제에 대한 작업이 끝나면 함께 종결된다. 아래에서 작업그룹 xmpp, p2psip, 그리고 연구그룹 p2prg의 활동에 관하여 좀 더 자세히 알아보도록 한다.

1. IETF Working Group – xmpp

WG xmpp는 IM의 표준을 제정하기 위한 작업그룹으로서, 이를 위해 security 기능이 추가된 xmpp 프로토콜의 표준화 작업을 진행하였다. 또한 채널 암호화를 위해 SASL(Simple Authentication and Security Layer)과 TLS(Transport Layer Security)/SSL(Secure Sockets Layer)을 사용하도록 규격을 정의하였으며, 개체 암호화를 위해 OpenPGP를 사용하도록 규격을 정의하였다. WG xmpp는 표준화 작업을 완료한 뒤 2004년 10월 종결되었다. WG xmpp에 의해 등록된 RFC는 모두 4건으로 아래와 같다.

① Extensible Messaging and Presence Protocol(XMPP): Core[2]
이 문서는 Extensible Messaging and Presence Protocol(XMPP)의 핵심 기능들을 정의하고 있다. XMPP는 두 네트워크 단말간에 구조적인 정보를 교환하기 위하여 실시간으로 Extensible Markup Language(XML) element들을 streaming하기 위한 프로토콜이다. XMPP은 XML 데이터를 교환하기 위한 일반화되고 확장 가능한 프레임워크를 제공하는 반면,

그것은 RFC 2779의 요구조건을 충족하는 instant messaging 과 presence applications을 구축하기 위한 목적으로 사용된다.

② Extensible Messaging and Presence Protocol(XMPP): Instant Messaging and Presence[3]
이 문서는 XMPP의 핵심 기능들의 애플리케이션들과 익스텐션들을 기술하고 있다. XMPP는 기본적인 IM과 RFC 2779에 정의된 presence functionality를 제공한다.

③ Mapping the Extensible Messaging and Presence Protocol(XMPP) to Common Presence and Instant Messaging(CPIM)[4]
이 문서는 XMPP와 Common Presence간 매핑과 Instant Messaging(CPIM) 규격을 기술하고 있다.

④ End-to-End Signing and Object Encryption for the Extensible Messaging and Presence Protocol(XMPP) [5]
이 문서는 XMPP를 위한 end-to-end signing과 object encryption을 정의한다.

2. IRTF Research Group: p2prg

연구그룹 p2prg(Peer-to-Peer Research Group)는, IRTF(Internet Research Task Force)의 12개의 연구그룹(RG)들 중 하나로, 2003년 말에 시작되었으며, 작업그룹(WG)에 비해 상대적으로 긴 기간 동안 안정적으로 연구를 수행한다. p2prg의 설립 목적은, 연구자들에게 근본적인 P2P관련 이슈들을 폭넓게 연구할 수 있도록 포럼을 열고, 연구결과를 IETF에 제출함으로써, P2P 프로토콜 표준화 작업을 담당할 미래의 작업그룹들에게 도움이 될만한 기반을 제공하는 것이다.

p2prg의 공동 의장 중 한 명인 Bill Yeager는 Sun Microsystems의 Sunlabs 연구원으로, 2000년부터 지금까지 Open P2P Protocol 프레임워크를 개발하는 Project JXTA를 이끌고 있다. 여기서 잠시 JXTA에 관하여 알아보면, JXTA라는 이름은 '나란히 놓여있다'라는 영어단어, Juxtapose에서 유래되었으며, 여기서는 P2P 기술이 Client-Server/Web-based computing 옆에 '나란히 놓여있다'라는 의미를 가진다. JXTA는 공개 P2P 프로토콜 세트로서, 네트워크상의 모든 장치(휴대폰, PDA, PC, Server 등)들이 피어로서 상호 통신할 수 있는 프로토콜 표준을 제공하는 것을 목적으로 한다. JXTA 프로젝트의 목표는 크게 세가지로 축약된다. 첫째, Interoperability. 즉, 서로 다른 이(異)기종 P2P 서비스의 피어간에 상호운용이 가능한 환경을 제공하는 것을 말한다. 둘째, Platform independence. 즉, 개발 언어, 통신 프로토콜, 시스템 플랫폼에 독립적인 환경을 제공하는 것을 말한다. 마지막으로 셋째, Ubiquity. 네트워크에 접속 가능한 모든 디바이스상에 구현 가능한 환경을 제공하는 것을 의미한다.

이렇게 매우 거대한 비전이 담긴 JXTA는 B. Yeager에 의해 2002년 IETF에 드래프트로 제출되었으나, 전반적인 연구가 미비하다는 이유로, 최초의 본격적인 P2P Working Group 발족을 이끌어내는 데는 실패하였다. 그 결과, 2003년 말, 대체수단으로서 연구그룹인 p2prg가 조직되었고, B. Yeager의 주도 하에 P2P에 대한 전반적이고 근본적인 연구가 진행중이다.

p2prg 아래에는 더욱 세분화된 연구를 위한 Subgroup들이 존재한다. 현재까지 Applications, Discovery and Resource Location Protocols, Metadata, Mobility, Overlay, Security, Peer-to-Peer over IPv6, Peer-to-Peer Content, Resource and Service Discovery 등의 여러 Subgroup들이 조직되었는데, 지금은 대부분 활동이 드문 편이다. 2006년 3월 현재, 연구가 활발한 서브그룹은 CORE(Peer-to-Peer Content, Resource and Service Discovery)이다. 아래 문서는 CORE 서브그룹에서 나온 최근 문서들 중 하나이다.

Tools for Peer-to-Peer Network Simulation[6]

극도로 커져버린 P2P 오버레이 네트워크의 스케일로 인하여, 최근 복잡성이 주요 이슈가 되어가고 있다. 연결된 노드가 수백만 개에 다다르면, 오버레이 네트워크를 정확히 시뮬레이션 할 수 있는 플랫폼이 중요해진다. 패킷 레벨의 네트워크 모델링부터 완전히 오버레이 네트워크에 집중하는 것에 이르기까지, 많은 무료 네트워크 시뮬레이터가 존재한다. 이 문서는 실험에서 얻어진 시뮬레이트 된 노드들의 최대 수, 모델링 된 P2P 오버레이 아키텍처들, 선택된 개발 언어들을 기술함으로써, 이 시뮬레이터들에 대한 개요를 제공해준다.

3. IETF Working Group: p2psip

2005년 11월, 캐나다 Vancouver 에서 제64차 IETF 총회가 막을 내리던 날, P2P에 관련한 Ad-Hoc Meeting이 열렸다. 이 회의의 안건은 SIP(Session Initiation Protocol) 네트워크에서 중앙 서버들의 필요성을 최소화 또는 제거하고, 분산된 자원의 발견을 허용하도록 하기 위하여, P2P의 분산적 특성을 SIP 네트워크에 도입하는 문제였다. 이 회의를 계기로 David Bryan의 주도 하에 현재 p2psip(Peer-to-Peer Session Initiation Protocol) 작업그룹이 준비중에 있으며 2006년 3월 제65차 IETF 총회에서 제안될 것으로 예상되고 있다.

이 작업그룹의 목적은 세션 설치/관리가 중앙서버보다는 단말들의 집합체에 의하여 완전히 또는 부분적으로 처리되는 설정에서의 SIP 세션 이용을 위한 메커니즘과 가이드라인을 개발하는 것이며, 이것은 서비스 공급자의 프록시들에 의존하는 재래식 SIP 접근의 대안이 될 수 있다. SIP에 P2P 기술을 도입하려는 주된 이유는 P2P의 확장성과 서버 유지비용의 절감이다.

수 백만 개 피어들의 등록과 위치정보를 관리해야 하는 SIP 서버들의 역할을 P2P가 대신하도록 하려는 것이다. p2psip 작업그룹을 위한 사전 작업으로 여러 건의 드래프트가 제출되었는데 아래에 간략히 정리해본다.

① Use Cases for Peer-to-Peer Session Initiation Protocol[7]
이 문서는 P2P기반 SIP의 사용 케이스들을 식별, 분류하고 있으며, 전적으로 실시간 IP 통신에 관한 케이스들에 집중하고 있다.

② Requirements for SIP-based Peer-to-Peer Internet Telephony[8]
이 문서는 DHT를 이용한 SIP 등록과 자원 발견을 위한 P2P기반 접근의 동기와 요구사항을 대략적으로 설명하며, 그러한 시스템을 위한 아키텍처 설계를 제안한다. 이 설계는 SIP과의 완전한 역호환성을 제공하고, 기존의 클라이언트들의 재사용을 허용하며, P2P 노드들이 재래식 SIP 엔티티들과 통신할 수 있도록 해주는 동시에, 중앙 서버의 필요성을 없애준다.

③ A P2P Approach to SIP Registration[9]
이 문서는 DHT 테이블을 이용한 SIP 등록과 자원발견을 위한 P2P 기반 접근의 요구사항과 동기를 개괄적으로 기술하며, 그 시스템을 위한 아키텍처 설계를 제안하고 있다.

④ SIP, P2P and Internet Communications[10]
이 문서는 SIP 의 P2P와 비P2P 능력을 분석하여, P2P 프로토콜이 IETF에서 Registrar/ Proxy/Redirect 서버와 Location 서비스 간에 사용되는 프로토콜로서 표준화되어야 한다는 점을 제안하고 있다. 이 프로토콜은 Registrar의 오퍼레이터가 P2P 네트워크를 이용하여 등록 상태를 얼마나 많이 로컬에 저장하는가, 그리고 얼마나 많이 분산형 Location 서버에 분산할 수 있는가를 결정할 수 있게 해준다. 또한 이 문서는 기존의 SIP 와 P2P 연구들을 조사하고 있다.

⑤ Industrial-Strength P2P SIP[11]
만약 SIP와 P2P에 기반한 인터넷 telephony 네트워크가 기존의 중앙집중식 telephony 서비스처럼 실행 가능하려면, P2P SIP 기술은 기존 기술들의 모든 기능들을 제공해야만 한다. 이 문서는 P2P SIP가 지원할 만한 기능들을 기술하고 있으며, 그에 따른 프로토콜 suite를 위한 구조를 제안하고 있다.

⑥ An Architecture for Peer-to-Peer Session Initiation Protocol [12]
이 문서는 P2P SIP 시스템을 위한 아키텍처를 기술하고 있다. 이 시스템에서는 P2P 오버레이 레이어가 SIP을 위한 검색과 분산적 리소스 배치 서비스를 제공한다.

⑦ The Effect of NATs on P2P SIP Overlay Architecture[13]
이 문서는 NAT가 P2P SIP 시스템에서 가능한 오버레이 아키텍처에 주는 제약들을 언급하고 있으며, 'symmetric interest'라고 알려진 속성을 가지는 구조적 partial-mesh 오버레이 네트워크가 가장 적당한 네트워크라고 결론짓고 있다.

⑧ Problem Statement for SIP-signalled Peer-to-Peer Communication across Middleboxes[14]
미들박스, 특히 방화벽과 네트워크 어드레스 트랜슬레이터는 오늘날 인터넷 인프라스트럭처의 필수적인 요소인데, 클라이언트-서버 애플리케이션들을 지원하기 위하여 설계되지만 자주 장애가 되곤 한다. 이 문서는 SIP 기반 P2P의 미들박스 관련 이슈들을 다룬다.

V. ITU-T 표준화 동향

ITU-T(ITU Telecommunication Standardization Sector) 내에는 각각 특정 분야의 표준 개발을 담당하는 SG(Study Group)가 13개 존재하며, 각 SG 아래에는 더욱 세분화된 분야를 맡고 있는 Q(Question)들이 있다. 그 중에서 SG 17 은 보안, 개발언어, Telecommunication 소프트웨어 분야의 표준을 담당하고 있으며, 그 아래에 보안 통신 서비스 분야를 담당하는 Question이 Q. 9/17이다.

2005년 SG 17 회의는 10월, 스위스 제네바에서 개최되었는데, 이 회의에서 한국과 일본은 총 3건의 P2P 관련 기고서를 Question 9/17에 제출하였고, P2P 보안 분야의 프로젝트를 각각 1개씩 수행하기로 결정하였다. 이 프로젝트들 중 하나인 X.p2p-1은 요구사항(위협 분석 등)에 관한 것으로 일본측에서 맡고 있고, 다른 하나인 X.p2p-2은 P2P 보안을 위한 세부 기술에 관한 것으로 한국측에서 담당하고 있다. 또한 2006년 초, 중국도 이 프로젝트들에 관심을 보이며 P2P 네트워크를 위한 Trust 모델과 보안 아키텍처에 관한 2건의 기고서를 제출한 상태이다. 이상 언급된 5건의 기고서의 내용은 아래와 같다.

① Proposal for studying anonymous authentication architecture in community communication[15]
BBS(bulletin board system), SNS(social networking site), P2P, Blog(with trackback), Wiki, Instant Messaging과 같은 커뮤니티를 제공하는 통신 서비스들의 대부분은 유저들의 편의를 위하여 익명성(Anonymity)을 보장해주고 있다. 그러나 이러한 익명성은 해당 커뮤니티의 보안성을 약화시킬 수 있다. 이 문서에서 저자는, 익명성이 허용되는 커뮤니티에게 참가자들의 인증정보를 제공해주는 익명 인증 아키텍처에 관한 연구를 시작할 것을 제안하고 있다.

차후에는 인증정보의 내용, 네트워크 측으로부터의 인증정보 메커니즘 제공, 네트워크간 인증정보 메커니즘 교환, 멀티플 네트워크들을 사용하는 유저들을 위한 지원 메커니즘 등이 계속 다루어질 예정이다.

② Proposal on the new study item about secure communication using TTP services[16]

TTP(trusted third party)가 애플리케이션을 대신하여 보안 기능을 수행하는 애플리케이션들 간에 안전한 통신이 이루어지기 위해서는 TTP와 애플리케이션은 서로 밀접하게 협력해야 한다. 이미 ITU-T 권고안 X.842에서 TTP가 제공하는 주요 보안 서비스를 정의하기는 했지만, 어느 TTP 서비스를 사용할 것인지, 애플리케이션이 안전한 통신을 수행할 때 TTP서비스를 사용하는 방법에 대하여 명확한 설명이 없다. 이 문서의 저자는 이에 대한 연구를 시작할 것을 제안하고 있다.

③ Proposal for studying P2P Network Security[17]

이 문서에서 저자는 Q.9/17 워크 아이템의 일부로서 P2P 네트워크 보안을 연구하도록 강력히 촉구하고 있으며, P2P 네트워크 보안 프레임워크 구축을 제안하고 있다. 현재 P2P가 저작물 불법 공유에 자주 관여하고 있긴 하지만, 그 기술 자체는 많은 장점을 가지고 있으며, 유비쿼터스 네트워크를 향하여 빠르게 진화중이라고 볼 수 있다. 이 문서는 P2P가 단기간 존재하는 기술이 아니고, 앞으로도 사용자들이 지속적으로 필요로 하는 기술임을 강조하고 있다.

④ A set-based P2P security trust model[18]

이 문서는 P2P 네트워크를 위한 새로운 보안 trust 모델을 연구하도록 제안하고, 노드들간의 Trust 등급을 어떻게 계산해야 하는지를 설명하고 있다.

⑤ A security architecture of operable secure P2P service[19]

이 문서는 teleco 환경에서 P2P 서비스 모델을 연구하기를 제안하고 있다. 여기서 제안된 안전하고 사용가능한 P2P 서비스 아키텍처는 P2P 기술의 장점을 활용하기 위해서, P2P 서비스의 분산적 사용을 지원하는 동시에, 사용자의 서비스 접근 인증에는 중앙집중식 관리 모델을 사용한다.

VI. ASTAP 표준화 동향

2005년 10월 호주 멜버른에서 제10차 ASTAP(Asia-Pacific Telecommunity Standardization Program) 포럼이 열렸다. 이 포럼의 주 목적은, 태국에서 열렸던 제9차 포럼 이후 ASTAP Expert Group들의 진행 상황을 검토하고, 2006년 ITU Plenipotentiary Conference를 위한 APT 지역 예비 프로세스의 통신 표준화 자료를 개발하며, IP Telephony and NGN Workshop에서 제안된 발의들을 검토하는 것이었다. 이 포럼에서 P2P 네트워크 보안에 관련한 기고서가 총 3건 발표되었는데, 그 기고서들을 아래에서 간략히 살펴본다.

① Proposal for studying P2P Network Security[20]

이 문서는 P2P 네트워크 보안을 IS WG을 위한 워킹 아이템의 일부로서 연구하는 것이 필수적이며, 지금이 그 연구를 시작하기에 적기라는 점을 권고하고 있다.

② Security for P2P Overlay Network based on DHT[21]

이 문서는 DHT 기반 P2P 네트워크에서의 주요 보안 위협 6가지를 거론하고 있다. 분산형 P2P 모델은 중앙 서버가 없다. 따라서 파일들의 위치 정보가 노드간에 분산되어 있다. DHT(Distributed Hash Table) 기반 scheme은 structured 분산형 P2P 네트워크를 구축하고, 효율적인 파일 검색 서비스를 제공하는데 사용될 수 있다. 많은 P2P 애플리케이션들이 DHT 기반 오버레이 네트워크상에서 설치되어 오고 있으나, 이 애플리케이션들은 현실의 P2P서비스에 적용될 수 없다. 왜냐하면 DHT 기반 P2P 는 매우 유용하지만, 충분한 보안성을 제공할 수 없기 때문이다. 이 문서에서는, DHT 기반 P2P 네트워크에서의 주요 보안 위협들인 Node ID related attack, Attacks on message routing, DoS(Denial of Service), Attacks on forged routing, Storage and retrieval attack, Rapid join and leave attack 들이 언급되고 있다.

③ Analysis of P2P Traffic Detection Mechanism [22]

이 문서는 현존하는 P2P 트래픽 탐지 메커니즘을 분석하고 있다. 최근 P2P 사용량이 급증함에 따라 P2P 트래픽도 급격히 증가하고 있다. 이 증가된 트래픽은 대역폭을 소비하고, 네트워크 통신을 방해한다. P2P 트래픽은 컴퓨터 바이러스나 악성 코드들의 출입구를 제공할지도 모른다. P2P트래픽을 탐지하기 위한 많은 실험과 연구들이 있었음에도, P2P 프로토콜을 위한 표준 규격이 없기 때문에, 뛰어난 P2P 트래픽 탐지 방법을 찾는 것이 매우 힘들다. 이 문서는 잘 알려진 포트들을 사용하는 방법, 특별한 Signature들을 비교하는 방법, Heuristic 방법들을 비교 분석하고 있다.

VII. 결 론

이제까지 주요 국제표준화 기구들에서의 P2P 관련 표준화 동향을 대략적으로 살펴보았다. 지금 이 시간에도 P2P 기술이 놀라운 속도로 급속히 확산되고 있음에도 불구하고, P2P 관련 표준화 활동은 다소 미약한 상황이다. 인터넷 표준화의 주축인 IETF에서 연구그룹(RG) 차원으로 꾸준한 연구활동이 진행되고 있긴 하지만, 실질적으로 IM 분야를 제외하면 P2P 표준은 거의 제정되어 있지 않은 실정이다. 그러나 앞에 언급된 작업그룹 p2psip의 준비 움직임에서 볼 수 있듯이, 향후 P2P 기술과 기존 기술을 결합시키려는 시도가 점점 활발해질 것으로 예상되고 있으며, 그에 따라 P2P 기술의 확산은 점점 속력을 더해 갈 것이다. 이러한 기술의 확산은 결국 국제 표준화의 필요성을 증대시키게 될 것임이 자명하므로, 앞으로 P2P 관련 분야의 표준화를 위하여 기존의 IETF내 작업그룹들과 ITU-T내 스터디그룹들 간의 더욱 활발한 정보교류와 협력이 요구된다.

<참 고 문 헌>

[1] 권혁찬, 나재훈, 정교일, "DHT(Distributed Hash Table) 기반 P2P 오버레이 네트워크 보안 위협 분석," 정보보호학회지 제15권 제6호, Dec., 2005.

[2] P. Saint-Andre, Extensible Messaging and Presence Protocol(XMPP): Core, RFC 3920, Oct., 2004.

[3] P. Saint-Andre, Extensible Messaging and Presence Protocol(XMPP): Instant Messaging and Presence, RFC 3921, Oct., 2004.

[4] P. Saint-Andre, Mapping the Extensible Messaging and Presence Protocol(XMPP) to Common Presence and Instant Messaging(CPIM), RFC 3922, Oct., 2004.

[5] P. Saint-Andre, End-to-End Signing and Object Encryption for the Extensible Messaging and Presence Protocol(XMPP), RFC 3923, Oct., 2004.

[6] Alan Brown & Mario Kolberg, Tools for Peer-to-Peer Network Simulation, draft-irtf-p2prg-core-simulators-00, IETF, Jan., 2006.

[7] David A. Bryan, Eunsoo Shim and Bruce B. Lowekamp, Use Cases for Peer-to-Peer Session Initiation Protocol (P2P SIP), draft-bryan-sipping-p2p-usecases-00, IETF, Nov., 2005.

[8] S. Baset, H. Schulzrinne, E. Shim and K. Dhara, Requirements for SIP-based Peer-to-Peer Internet Telephony, draft-baset-sipping-p2preq-00, IETF, Oct., 2005.

[9] David A. Bryan and Cullen Jennings, A P2P Approach to SIP Registration, draft-bryan-sipping-p2p-01, IETF, Mar., 2006.

[10] Alan Johnston, SIP, P2P and Internet Communications, draft-johnston-sipping-p2p-ipcom-01, IETF, Mar., 2005.

[11] P. Matthews and B. Poustchi, Industrial-Strength P2P SIP, draft-matthews-sipping-p2p-industrial-strength-00, IETF, Feb., 2005.

[12] E. Shim, S. Narayanan, G. Daley, An Architecture for Peer-to-Peer Session Initiation Protocol, draft-shim-sipping-p2p-arch-00.txt, Feb., 2006.

[13] E. Shim, S. Narayanan, G. Daley, The Effect of NATs on P2P SIP Overlay Architecture, draft-matthews-p2psip-nats-and-overlays-00, Feb., 2006.

[14] J. Quittek, M. Stiemerling, T. Dietz, S. Niccolini, Problem Statement for SIP-signalled Peer-to-Peer Communication across Middleboxes, draft-quittek-p2p-sip-middlebox-00.txt, Feb., 2006.

[15] Yutaka Miyake, Proposal for studying anonymous authentication architecture in community communication, D.74, ITU-T, Oct., 2005.

[16] Yutaka Miyake, Proposal on the new study item about secure communication using TTP services, D.75, ITU-T, Oct., 2005.

[17] Jae Hoon Nah, Hyeok Chan Kwon and Jong Soo Jang, Proposal for studying P2P Network Security, D78, ITU-T, Oct., 2005.

[18] Jiwei Wei, Jing Liu, A set-based P2P security trust model, D132, ITU-T, Jan., 2006.

[19] Hongwei Luo, Jiwei Wei, A security architecture of operable secure P2P service, D133, ITU-T, Jan., 2006.

[20] Jae Hoon Nah, Jae Young Song, Hyeok Chan Kwon and Jong Soo Jang, Proposal for studying P2P Network Security, ASTAP, Oct., 2005.

[21] Jae Young Song, Hyeok Chan Kwon, Jae Hoon Nah and Jong Soo Jang, Security for P2P Overlay Network based on DHT, ASTAP, Oct., 2005.

[22] Jae Young Song, Gae Il An, Jae Hoon Nah and Jong Soo Jang, Analysis of P2P Traffic Detection Mechanism, ASTAP, Oct., 2005.

[23] John Buford, Keith Ross, P2P Overlay Design Overview, IETF P2P-SIP ad hoc, Dec., 2005.

---

* 본 내용은 필자의 주관적인 의견이며 TTA의 공식적인 입장이 아님을 밝힙니다