IEICE TRANS. INF. & SYST., VOL.E99–D, NO.3 MARCH 2016

PAPER

A New State-Based Connectivity Model for Peer-to-Peer Networks

Halil ARSLAN[†a)], ***Member and*** **Sinan TÜNCEL**[††], ***Nonmember***

SUMMARY The usage of peer-to-peer (P2P) networks that provide sharing of real-time environmental data by internet users is becoming more and more popular. As a result, it's necessary to identify the problems during P2P communication and to develop proper solutions. One of the major problems of P2P communication is that it's not possible to reach the clients behind devices that create private networks like network address translation (NAT) and firewalls from the public network. Among the solutions proposed for this problem, Interactive Connectivity Establishment (ICE) and Real Time Media Flow Protocol (RTMFP) are the methods most preferred in the literature. These methods seem more attractive than other NAT traversal mechanisms since they are independent from internet infrastructure and are also appropriate for dynamic structures. However, they do have some disadvantages. In this study, a new state-based end-to-end communication technique (SBN) for NAT traversal was designed and realized. The performance of the designed method was evaluated against three criteria, connectivity check delay, connection packet count and bandwidth, and compared with the ICE method. The results revealed that the suggested SBN method proved an average of 78% success in connectivity check delay, 69% in the number of packets used and 66% in the consumption of bandwidth over the ICE method.

key words: *peer-to-peer, NAT Traversal, ICE, RTMFP, SBN*

1. Introduction

P2P applications are utilizing internet bandwidth at an increasing rate every day. They are widely preferred in applications like file sharing, video conference, voice over internet protocol (VoIP), on-line gaming and Internet TV [5], and its usage has become more and more widespread [6]. In the traditional client-server approach, the server is, in architectural terms, in the center and is in charge of serving; on the other hand, clients are distributed and are consumers. Yet, for P2P networks, all the clients are both serving and consumers in a non-central structure. This approach remarkably stands out from the traditional client-server approach with its resource sharing and content distribution [1], [20].

Although data size in P2P networks increases dramatically, the desired bandwidth cannot be reached. That is why it has become crucial to clearly identify the peer-to-peer computer network infrastructure problems and application protocols and also to deal with these problems.

While providing P2P communication, devices that create private networks like NAT and Firewall prevent the direct connection between clients, which is one of the most fundamental problems. The studies in the literature that focus on this problem are named NAT/Firewall Traversal. Protocols/techniques proposed for the solution to this problem like STUN [4], TURN [7], PS-STUN [10], C-STUN [11] and newly developed traversal mechanisms [8]–[12] are incapable of solving the problem because of their disadvantages or insufficiencies.

In order to overcome problems that appear in protocols like STUN and TURN, Rosenberg defined the "Interactive Connectivity Establishment" (ICE) protocol [13]. The basic approach in this protocol is to use STUN and TURN protocols together and, thus, to provide peer-to-peer communication infrastructure in all NAT types. Tseng and others proposed a Context-Aware NAT (CAN) protocol to eliminate the connection set-up delay caused by STUN and TURN protocols, which are the basis of the ICE protocol [19]. In this study, agents working on peers gather network information of nodes and report them to the Session Initiation Protocol (SIP) server. The delay that occurs during the search for the most suitable way between the nodes to communicate was overcome by the control that was available thanks to the pre-known interface information. Nevertheless, that network information is pre-reported to the SIP server in every case, contributing additional loads of the model for all users.

Trickle-ICE, which was developed as an extension of the ICE protocol, is based on a step-by-step connection check between peers [27]. It aimed at increasing the signaling compared to classic ICE and making connection set-up faster. Both peers share their ICE membership incrementally via a current signal channel, and the ICE connection check continues until a successful candidate is found [28]. In this regard, Trickle-ICE increases signaling while peers are behind certain NAT types and, in this way, accelerates connection set-up, but cases observed in classic ICE still exist for all scenarios.

When the advantages and disadvantages of ICE, RTMFP [29] and CAN [19] protocols are taken into consideration, it becomes clear that there is a need for new studies that have low connectivity check delay and do not place extra loads on clients and are UDP/TCP supported.

In this study, a new state-based model to prevent disadvantages of ICE protocol that is widely used by P2P-based applications as NAT traversal was designed. The contributions of the proposed model in the literature are as follows:

Manuscript received June 5, 2015.
Manuscript revised October 20, 2015.
Manuscript publicized November 24, 2015.
[†]The author is with Sakarya University, Sakarya, Turkey.
[††]The author is with Department of Computer Engineering, Sakarya University, Sakarya, Turkey.
a) E-mail: halila@sakarya.edu.tr
DOI: 10.1587/transinf.2015EDP7220

1. An adaptive connection technique for P2P networks that works as state-based was developed.
2. As compared with state-of-the-art studies, end-to-end delay for applications that need NAT traversal was reduced.
3. Control packet count for connectivity was minimized, and in this way a more effective bandwidth usage was realized.
4. Proposed method is a real implementation, so it does not contain any abstractions as in simulated models.

The remaining sections of the study are organized as follows: Section 2 focuses on background required for NAT traversal studies. Section 3 includes a detailed description of the new model for the solution to the connectivity problem in P2P networks, mentioned above, and also its comparison with the current application. In Sect. 4, real-time applications of the designed model were carried out. The results of tests are presented in graphs. In the following section, advantages and disadvantages of the proposed model and studies that can be performed are included.

2. Background

2.1 Network Address Translation

Network Address Translation (NAT) is a standard that was developed by the Internet Engineering Task Force (IETF) in order to widen the address limit of 32-bit IPv4 and to create private networks. NAT is a network traversal that translates public network addresses to private network addresses and vice versa [2]. NATs are defined in four categories based on port translation (Table 1) [4]. For NAT traversal studies, it is crucial to know NAT types so as to produce alternative solutions for problems that crystallize.

One of the advantages of NAT is that it can create private networks and exceed the IPv4 address limits. Despite such advantages, it also has some weaknesses. For example, clients behind NAT cannot be accessed directly via public network addresses. This case is one of the main problems of P2P communication applications. There have been many studies undertaken to identify a solution to this problem. Approaches devised for solving the NAT traversal problem on P2P communication can be categorized into the following categories (indicated in subsequent headings).

Table 1 NAT types according to port translations.

Full Cone (FC)	For all requests, local IP addresses and ports are matched with the same public IP addresses and ports. Thus, access from public networks to local users is available.
Restricted Cone (RC)	All requests are matched like FC NAT. Access to this local IP address is only available from any port on the accessed public IP address. Requests from different public IP addresses cannot be mapped.
Port Restricted Cone (PRC)	Matching is like RC NAT. But, access to this local IP address is only available from the accessed public IP address and the port. When the public IP address to be accessed and the port are different from the accessed public IP address and the port, incoming requests cannot be mapped.
Symmetric (SYM)	Singular IP:port mapping is used for all sessions. When a different outbound request is produced on the same local IP and port, they are mapped with a new IP:port. A packet can be sent by only public IP address and port where requests are received.

2.2 NAT Traversal Approaches in P2P Communication

Manual port mapping: Private address of the user to be communicated with is matched with a suitable port number via NAT, and in this way, access from public network can be achieved. In this method, manual configuration is needed for access to private addresses. That is why it is not an applicable method for P2P applications.

Application layer gateway (ALG): It is considered an improved form of NAT. It is based on identifying the nodes between which communication will take place with the help of environmental data between communicating nodes. This method needs a media relay server in all NAT types. Besides the delay caused by this need, it also requires additional overheads for real-time communication and brings about security violations, which is why this method is not preferred [3].

Virtual private network, tunnel: Among the private networks to enable peer-to-peer communication, this method is one that uses a tunnel server. Because the tunnel server is necessary for all private networks to accept all incoming requests, and also because of high bandwidth usage and security requirements, this method is inefficient.

Universal plug and play (UPnP): It was developed by the UPnP forum to connect various network devices to P2P networks. A network device with UPnP support automatically maps the private network address and public network address with an appropriate port and makes NAT traversal possible [15]. Although configuration is not necessary for the last user, which is a significant advantage, it is not supported by many NAT manufacturers.

Real-time media flow protocol: Real Time Media Flow Protocol (RTMFP) [16], [18] makes use of UDP hole punching technique identical to the STUN protocol. Supporting only UDP-based direct connections, this protocol focuses on principles such as low delay time, data prioritization and P2P data distribution without a media distributor server. As a NAT traversal method, it attempts to achieve UDP connection by changing End Point Discriminator (EPD) data via forwarder servers. This protocol does not support P2P communication for users behind NAT/Firewall where direct connection is not possible and UDP packets are avoided. In this case, the use of Transmission Control Protocol (TCP) based Real Time Messaging Protocol (RTMP) is recommended [17]. However, because of its TCP-oriented structure that is based on client-server architecture and requires high bandwidth, RTMP does not seem like an ideal solution for real-time applications dependent on P2P communication.

Interactive connectivity establishment (ICE): ICE protocol [13] created a framework for NAT traversal protocols that uses User Datagram Protocol (UDP) hole punching technique like Simple Traversal of UDP through NATs (STUN) and Traversal Using Relay NAT (TURN). In this approach, when a direct connection is not possible, TURN servers are employed. In other cases, proper public-private network address mapping is done through STUN server and a direct connection is built. This protocol is based on the principle that the client controls all network interfaces to find the most suitable connection path, which brings about disadvantages such as high connection test time and overuse of control packets.

2.3 Extensible Messaging and Presence Protocol (XMPP)

Besides being defined as a packet to carry data between different communication points, Extensible Messaging and Presence Protocol (XMPP), like all communication protocols, is an open communication infrastructure protocol, using the XML (Extensible Markup Language) format for real-time communication. This protocol, which has been recognized as a standard by many applications, is an instant messaging service that can create a federated network [14]. XMPP standards were defined with RFC 3920 and RFC 3921 published by IETF.

The XMPP protocol, in a standard manner, uses the ICE-UDP-based NAT Traversal technique named jingle and defined in XEP-0176 and XEP-0215 extensions. All steps for P2P communication are carried out in accordance with the ICE protocol.

3. Proposed Model

P2P communication steps for two clients behind NAT have been described in numerous studies. Basic improvements on this point are about NAT traversal steps using minimum delay and minimal bandwidth. In the widely used ICE technique, the main reason for delay is that connectivity for candidates determined from all current interfaces is tried one by one (Fig. 1).

This study includes a proposal of a new state-based model to decrease connection time, number of packets used and bandwidth usage, which are the weaknesses of RTMFP and ICE protocols.

The algorithm of the proposed model is exhibited in Fig. 2. According to this algorithm, nodes that want to establish P2P communication firstly attempt to communicate directly depending on whether they are local or public to each other. If establishment of communication via specified public or local interfaces is successful, P2P media flow is initiated. Otherwise, nodes are checked for suitable UDP couples via the Cumulus Server [21]. If connection via these specified interfaces can be established, the specified IP and port data is defined as a Real-time Transport Protocol (RTP) Socket. The proposed model was used the Cumulus server in point of avoids extra RTTs, repeated NAT traversal effort.

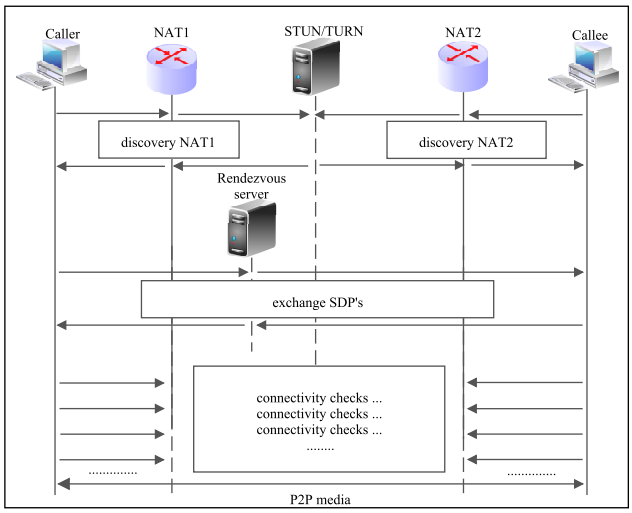

Fig. 1 ICE network flow model

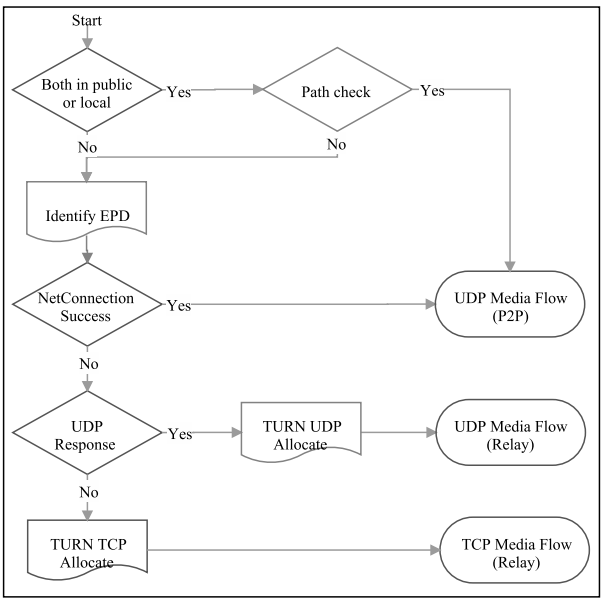

Fig. 2 SBN algorithm.

In case P2P connection cannot be established between nodes, UDP relay interfaces are defined via TURN server and RTP data flow is continued through the UDP Relay Server. For hosts without UDP response, TCP relay interfaces are defined and data flow continues as TCP.

The data flow diagram that explains the difference between ICE and the proposed SBN model is shown in Fig. 3. This figure also demonstrates formation of P2P communication requests and the steps involved in the initiation of media flow between two clients. These steps were designed according to the caller's creation of a request to start P2P communication with the callee.

Steps followed;

1. Caller opens an UDP socket via an empty port on 4096 and sends a P2P communication request (XMPP IQ

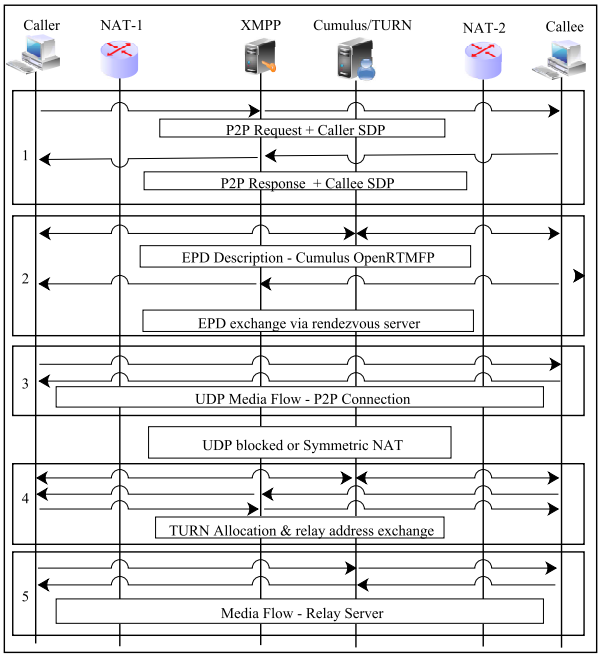

Fig. 3 SBN network flow model.

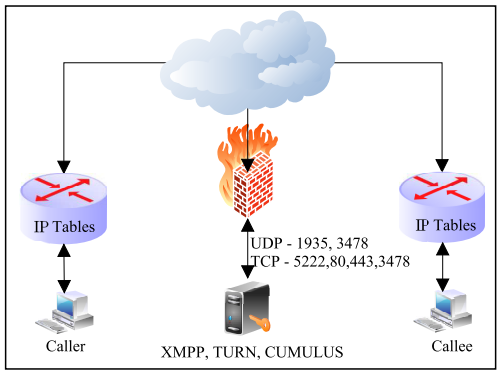

Fig. 4 Model of real-world scenario

Table 2 ICE-SBN test configuration.

System	Tools
Client platforms	Win 7, i7 3.4Ghz and 8GB RAM
Rendezvous server	Win 2008, Xeon 3.1GHz, 4GB RAM
TURN/Cumulus	Ubuntu 13.04, Xeon 3.1GHz, 4GB RAM
Development	Java 1.7, Action Script 3
Bandwidth	8 Gbps ADSL Internet
NAT box	4 different NAT, Linux Ubuntu 13.04 defined with iptables (PPPoE connection), dual ethernet.

packet) with specific SDP (Session Description Protocol), which contains local IP:port. The rendezvous server [23], [24] adds a specific SDP packet including caller's public IP and local IP:port information and callee's public IP to received communication request and delivers this to the callee. If this request is accepted by the callee (by opening an UDP socket similar to the caller's UDP socket), the rendezvous server sends a response packet containing specific SDP content to the caller and callee. Connection controls of clients are performed through the content specified in a private SDP packet. If communication can be achieved via specified candidates, the process is completed. In this case, SBN has started P2P communication between nodes according to clients being on local or public networks.

2. The callee and caller identify EPD data via the Cumulus (UDP port 1935) Server and generate their Near IDs. Generated Near IDs are exchanged as Far IDs between the callee and caller on the XMPP server.
3. If connection through this produced potential communication channel is possible, P2P media flow is continued between the caller and callee.
4. In step 3, in case P2P communication cannot be established, clients specify Relay connection interfaces via the TURN server. SDP information produced by them is exchanged via the XMPP server and connectivity check processes are only inspected through relay address candidates.
5. At this stage, the Relay TCP/UDP socket is ready for clients to establish P2P communication. Application and test results of the proposed model are presented in the following section.

4. Performance Evaluation of Proposed Model

In order to evaluate performance analyses of the proposed model, the real-world application in Fig. 4 was performed.

In the P2P communication model described in this study, XMPP was used as the rendezvous server between clients so as to create a full end-to-end model. Located in the very center of the application, the rendezvous server has functions like starting a session, authorization, presenting user lists, managing status changes and instant messaging, without a need for high bandwidth. Besides these, the primary function of the rendezvous server is to manage session description parameters needed for P2P communication among clients.

In the scenario here, public-private network ip/port translation of clients was managed with IP Tables (ADSL modems in bridge mode). Different NAT types were modeled via IP Tables and current NAT devices were tried on network topology. According to the scenario, the rendezvous server with XMPP infrastructure serves via TCP-5222, 80, 443 port. The caller, behind NAT-1, wants to have a P2P connection video chat request with the callee, which is behind NAT-2. The TURN server [26] in the model listens to UDP-3478, TCP-80, 443 while the Cumulus server serves via the UDP-1935 port.

Configuration details of the scenario used here are summarized in Table 2. In this scenario, SBN and Jitsi version 2.2.4603 [25], an open-source code VoIP software that uses ICE protocol as the NAT Traversal technique, were run separately. Data flow was supervised via the caller with Wireshark Network Analyzer software version 1.8.4 [22].

A sample application was run on the network topol-

Table 3 ICE-SBN connection states.

	(Callee) FC	RC	PRC	SYM
FC	P2P	P2P	P2P	P2P
RC	P2P	P2P	P2P	P2P
PRC	P2P	P2P	P2P	RELAY
SYM	P2P	P2P	RELAY	RELAY

ogy described in Fig. 4, and the network was observed for parameters like connection status of clients behind different NAT types, their connection delay times, number of packets used and bandwidth usage. For verification, connection models behind different NAT types used for ICE and SBN and also the connection type are shown in Table 3. Both models demonstrate the same behavior behind all NAT types. If both ICE and SBN, Caller and Callee are SYM-SYM or PRC-SYM, relay connections can be established via the TURN server. In the other 13 cases, P2P connection is possible.

In evaluations, a P2P communication request was produced in four different NAT types for the SBN and ICE technique. Results of these requests were observed against three criteria such as connectivity delay at the start of RTP media flow, bandwidth usage and number of packets used. The experiments were symmetrically performed for four NAT types thus, 16 different scenarios were realized. All scenarios were repeated 10 times and the parameters such as bandwidth, connectivity delay check and packet count were calculated.

4.1 Connectivity Delay

According to evaluations, peer-to-peer communication between clients on different private networks can be efficiently initiated within the ICE platform in 4–5 seconds [19]. However, it is observable that delay in a real application environment is much higher.

Connection delay times of the proposed SBN model and ICE for 16 different scenarios exhibited in Table 3 are displayed in Fig. 5. Figures in the graph are significant since they reveal whether the main objective of this study has been met or not. It shows that the proposed SBN method has an advantage of averaging 78% over ICE in terms of connectivity delay in all scenarios since ICE try to connect for all potential cases while SBN chooses the appropriate link interface according to Caller and Callee.

In cases when the relay server is used, the reason for the discrepancy between ICE and the proposed model in terms of connection delay time is that among all specified candidates, only relay candidates are included in the connectivity check.

4.2 Control Packet Count

The low control packet numbers in connections are important in terms of effective usage of bandwidth. It is also known that the previously mentioned Trickle-ICE increases packet usage number more than classic ICE.

The numbers of control packets produced by ICE and the proposed SBN method for connectivity are displayed in Fig. 6. As can be seen in Fig. 6, while, for example, the Caller and Callee use FC NAT type and ICE is preferred as the connection model, and the packet count is 85, whereas when SBN is preferred, it is 13. The same discrepancy is observable across different NAT types.

It appears that the SBN method has an advantage of 69% over ICE in packet count in P2P connection set-up. This advantage will contribute greatly to efficient usage of network resources.

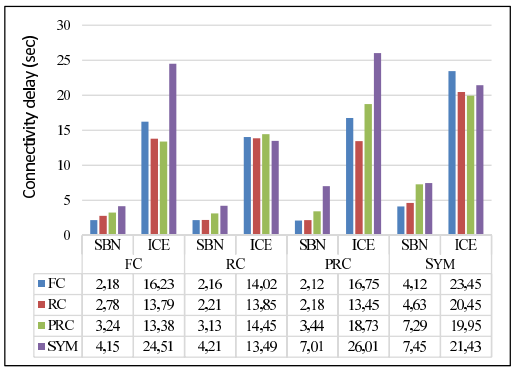

Fig. 5 ICE and SBN connectivity delay time comparison.

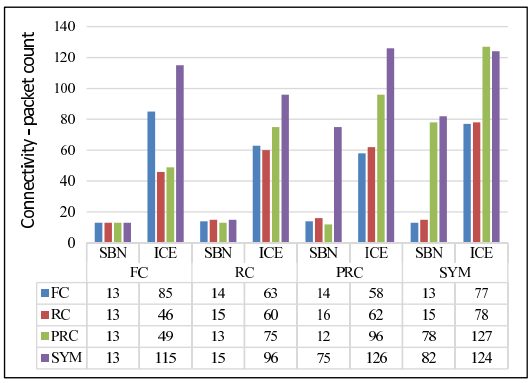

Fig. 6 Comparison of ICE and SBN packet counts.

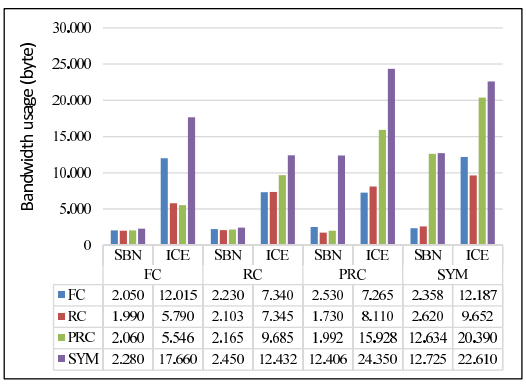

Fig. 7 Comparison of ICE and SBN bandwidth usage.

4.3 Bandwidth Usage

As a result of the decrease in number of packets used for connection set-up, bandwidth usage also decreases. Figure 7 displays bandwidth usage by ICE and SBN techniques. There is an approximate decrease of 66% in bandwidth usage, which is a significant advantage of the proposed model.

5. Conclusion

This study focuses on the communication problem of clients behind NAT, which is a serious problem for P2P applications. We have proposed and implemented a novel state-based and end-to-end communication technique (SBN) for NAT traversal problem. SBN overcomes the disadvantages of ICE protocol, which is widely used in P2P-based applications as NAT traversal, by helping the user to choose the most appropriate link interface according to Caller and Callee. Performance evaluation of SBN was realized according to the connectivity check delay, connection packet count and bandwidth parameters in a private network created by NATs and Firewalls. Compared with ICE, SBN can provide lesser connectivity check delay up to 7 times, lesser number of packets up to 10 times and lesser bandwidth consumption up to 8 times. As a result, SBN outperforms ICE, which is widely used in P2P application, in terms of various performance criteria. In the future works, we plan to adapt new-generation technologies such as WebRTC [30] in SBN.

Acknowledgments

This study is supported following organizations: The Scientific and Technological Research Council of Turkey (BIDEB-2211 and Project number TEYDEB-7110304) and Research Fund of the Sakarya University (Project Number: BAPK-2012-50-02-051).

References

[1] A. Oram, Peer to Peer: Harnessing the Power of Disruptive Technologies, 1st ed. O'Reilly & Associates, Inc, 2001.
[2] K. Egevang and P. Francis, "The IP Network Address Translator (NAT)," RFC:1631, May 1994.
[3] H. Sinnreich and A.B. Johnston, Internet Communications Using SIP: Delivering VoIP and Multimedia Services with Session Initiation Protocol, 2nd ed. Wiley Publishing, 2006.
[4] J. Rosenberg, J. Weinberger, C. Huitema, and R. Mahy, "STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)," RFC: 3489, March 2003.
[5] C. Labovitz, S. Iekel-Johnson, D. McPherson, J. Oberheide, and F. Jahanian, "Internet Inter-Domain Traffic," SIGCOMM'10, pp.75–86, 2010.
[6] B. Harzog, "Net Neutrality and the Cloud. Cloud Computing," http://www.virtualizationpractice.com/net-neutrality-and-the-cloud-8794/, 2014.
[7] R. Mahy, P. Matthews, and J. Rosenberg, "Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)," RFC: 5766, April 2010.
[8] Y.-C. Chen and W.-K. Jia, "Challenge and solutions of NAT traversal for ubiquitous and pervasive applications on the Internet," The Journal of Systems and Software, vol.82, no.10, pp.1620–1626, 2009.
[9] C. Topal and C. Akinlar, "Secure seamless peer-to-peer (P2P) UDP communication using IPv4 LSRR option and IPv4+4 addresses," Computers and Electrical Engineering, vol.35, no.1, pp.115–125, 2009.
[10] Y. Wang, Z. Lu, and J. Gu, "Research on Symmetric NAT Traversal in P2P Applications," ICCGI'06, p.59, 2006.
[11] Z. Zhang, X. Wen, and W. Zheng, "A NAT Traversal Mechanism for Peer-to-Peer Networks," International Symposium on Intelligent Ubiquitous Computing and Education, pp.129–132, 2009.
[12] A. Mueller, N. Evans, C. Grothoff, and S. Kamkar, "Autonomous NAT Traversal," Tenth International Conference on Peer-to-Peer Computing, IEEE P2P'10, pp.1–4, 2010.
[13] J. Rosenberg, "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols," RFC: 5245, April 2010.
[14] J. Moffitt, Professional XMPP Programming with JavaScript and jQuery, Wiley Publishing, 2010.
[15] "UPnP forum," http://www.upnp.org, 2014.
[16] A. Sathiaseelan and G. Fairhurst, "TCP-Friendly Rate Control (TFRC) for bursty media flows," Computer Communications, vol.34, no.15, pp.1836–1847, 2011.
[17] K.J. Ma, R. Bartoš, and S. Bhatia, "Survey of schemes for Internet-based video delivery," Journal of Network and Computer Applications, vol.34, no.5, pp.1572–1586, 2011.
[18] L. Xue, F. Wen, C. Fan, J. Wang, and X. Wang, "Group Audio Application with Flash Multicast Streaming Based on RTMFP," The 2nd International Conference on Computer Application and System Modeling, pp.41–44, 2012.
[19] C.-C. Tseng, C.-L. Lin, L.-H. Yen, J.-Y. Liu, and C.-Y. Ho, "Can: A context-aware NAT traversal scheme," Journal of Network and Computer Applications, vol.36, no.4, pp.1164–1173, 2013.
[20] L. Rodero-Merino, A.F. Anta, L. López, and V. Cholvi, "Self-managed topologies in P2P networks," Computer Networks, vol.53, no.10, pp.1722–1736, 2009.
[21] "Cumulus: Open source RTMFP server." https://github.com/OpenRTMFP/Cumulus, 2014.
[22] "Wireshark: Network protocol analyzer." http://www.wireshark.org, 2014.
[23] "Openfire is a real time collaboration server." http://www.igniterealtime.org/projects/openfire/, 2014.
[24] "Smack is an Open Source XMPP client library." http://www.igniterealtime.org/projects/smack/, 2014.
[25] "A Java implementation of the ICE protocol - ice4j." http://code.google.com/p/ice4j/, 2014.
[26] "TurnServer: Open-source TURN server implementation." http://turnserver.sourceforge.net/, 2014.
[27] E. Ivov, E. Rescorla, and J. Uberti, "Trickle ICE: Incremental Provisioning of Candidates for the Interactive Connectivity Establishment (ICE) Protocol," http://tools.ietf.org/pdf/draft-ietf-mmusic-trickle-ice-02.pdf, Jan. 2015.
[28] I. Grigorik, "High-Performance Browser Networking, In: WebRTC," 1st ed. O'Reilly Media Inc, pp.309–362, 2013.
[29] M. Thornburgh, "Adobe's Secure Real-Time Media Flow Protocol," RFC: 7016, Nov. 2013.
[30] "WebRTC site." http://www.webrtc.org, 2015.

Halil Arslan was born in Sivas, Turkey, on December 10, 1982. He received B.S. and M.S. degree in electronic and computer education from Sakarya University, Turkey in 2004 and 2008 respectively. From March 2004 to February 2009, he was at the Computer Research and Application Center from the Sakarya University, Turkey. He is currently pursuing his Ph.D. degree at electronic and computer education from Sakarya University, Turkey. His research interests are peer-to-peer and real-time communication.

Sinan Tüncel received B.S. and M.S. degree in 1999 and 2002 from Sakarya University of Electronic and Computer Education, Turkey and Ph.D. degree in electrical and electronics engineering from Sakarya University, Turkey in 2010. His major research interests are modelling and simulation, communication protocol.