P2P architecture over IPv6 for personal internetworking

Chi-Yuan Chang, Fred Lin and Crota Chen

Department of Electrical Engineering,
National Dong Hwa University, Hualien, Taiwan
E-mail: andrew@mail.ndhu.edu.tw E-mail: gasloin@gmail.com
E-mail: m9323036@em93.ndhu.edu.tw

Han-Chieh Chao*

Department of Electronic Engineering,
National Ilan University, I-Lan, Taiwan
E-mail: hcc@mail.niu.edu.tw
*Corresponding author

Abstract: The purpose of this paper is to study the feasibility of Personal Internetwork (PIN) and find the approach to achieve the real cooperation of multiple personal devices and improve the usability of Hybrid and Pure P2P architecture within a personal scope. We proposed an IPv6 based Node Discovery Stack (NDS) to make the usage of Personal P2P application possible. This paper clarified the architecture of the PIN and shows how NDS could enhance the personal communication with co-working devices.

Keywords: PIN; NDS; P2P; IPv6.

Reference to this paper should be made as follows: Chang, C-Y., Lin, F., Chen, C. and Chao, H-C. (2006) 'P2P architecture over IPv6 for personal internetworking', *Int. J. Internet Protocol Technology*, Vol. 1, No. 4, pp.214–220.

Biographical notes: Chi-Yuan Chang is a PhD student in Electrical Engineering at the National Dong Hwa University, Hualien, Taiwan, ROC. His research interests include IPv6 based networks, wireless networks and network processors. He received his MS Degree from the Department of Computer Science and Information Engineering, National Chung Cheng University, Chia-Yi, Taiwan in 1994. He also works in the System Design Division, Computer and Information Technology Center, National Dong Hwa University, Hualien, Taiwan, ROC.

Fred Lin received his BS Degree from the Department of Electronic Engineering, National Dong Hwa University in July 2003. His research interests include network configuration, mobile IPv6 and P2P. He is pursuing his MS Degree with interests in network mobility at the Department of Electrical Engineering, National Dong Hwa University.

Crota Chen received his BS Degree from the Department of Electronic Engineering, National Dong Hwa University in July 2004. His research interests include IPv6, network processors, and embedded Linux. He is pursuing his MS Degree at the Department of Electrical Engineering, National Dong Hwa University.

Han-Chieh Chao is a Full Professor of Electronic Engineering at the National Ilan University, I-Lan, Taiwan, ROC. His research interests include high speed networks, wireless networks and IPv6 based networks and applications. He received his MS and PhD Degrees in Electrical Engineering from Purdue University in 1989 and 1993 respectively. He is also serving as an IPv6 Steering Committee member and Deputy Director of R&D division of the NICI Taiwan, and Cochair of the Technical Area for IPv6 Forum Taiwan. He is an IEEE senior member.

1 Introduction

Nowadays the trend of wide adoption of personal and residential online devices makes smallscale network configuration by endusers unavoidable and necessary (Yen et al., 2005). With the low price of broadband internet connections, many families can afford highspeed internet access and thus makes the peer to peer connection more practical and important.

To reduce configuration difficulty in applications and IP layers, rapid Application/IP layer configuration method for endusers is essential to popularise the use of all kinds of intelligent appliances or consumer electronic devices in our daily lives.

The personalscope internetwork for personal access is still far from convenient, efficient, and lacks the researchers' attention. While the enterprise internetwork systems, which can make employees access data from remote servers, store and share their experiences almost everywhere with appropriate network access ability. The cooperation of Online office/Net office optimises the usage of IT equipments and reduces companies' investment.

Most papers about personal networks are mainly focused on access technologies, such as Bluetooth, Wi-Fi (Farber, 2002), or are emphasised on physical configuration, such as plug and play (Ye et al., 2004). Although all of them make the network access more convenient, those works are not encouraged enough for customers to own more network enabled devices, which is the barrier in today's IT industry. In order to popularise the consumer electronic devices, finding ways to reduce configuration difficulty in application, network, and IP layer for end users is vital. For this circumstance, we defined a new term to describe the personal network devices: Personal InterNetwork (PIN) more clearly. PIN is the network which exchanges digital contents between individual IT units. Personal devices are not restricted to one place and all of them have variable degree of network access ability. To take security into consideration, Personal InterNetwork Group (PING) is restricted within those personal owned and controllable devices, such as home PC, smart mobile phone, net-music-player, intelligent appliances, home gateway…, etc. Associated devices such as desktop PC in office should connect to PIN through VPN or other methods to ensure the robust security of PIN.

2 IPv6 and P2P

With a great number of network devices connecting to the internet, the problem of solving the address space shortage problem of IPv4 becomes more and more demanding. The next generation internet protocol, Internet Protocol version 6 (IPv6) (Deering and Hinden, 1998), that benefits from the IPv4 development experiences, has been accepted as a standard internet protocol. It provides sufficient IP addresses, address autoconfiguration, QoS, security and mobility to enable all kinds of devices connecting to the internet with public IP. With an autoconfiguration or DHCPv6 feature, nodes could retrieve IPv6 address automatically without tedious IP address setup procedure. The multicast and anycast supported by IPv6 also provide more internet transporting methods.

The higher and higher internet throughput and availability requirements make it difficult to satisfy current needs with traditional client-server architecture. Therefore, serverside technology evolves from a server to a server cluster and then to a P2P network.

The first generation P2P technology usually uses a massive broadcasting approach to send queries and retrieve information to/from the peers (Tetsuya et al., 2003; Conta and Deering, 1998). Many researches provide variable ways to reduce the network overhead, such as Oh-ishi (Tetsuya et al., 2003), which shows that multicast could reduce the P2P network load. Modern P2P technology reduces the overhead mainly by using resource location algorithms.

There are already many P2P applications such as instant messaging, file sharing, web archive, network file system, distributed location service and distributed computing. All of them are categorised as hybrid P2P architecture. A tracker (or socalled bootstrap node) is needed for resource exchanging. In contrast, pure P2P is the fully distributed P2P architecture which is thoroughly discussed by researchers. But due to resource allocation problems, there are no popular pure P2P models currently.

The rest of the paper is organised as follows: Section 3 presents the main consideration of PIN. To realise PIN, Section 4 introduces node discovery stack and personal P2P application architecture. Prototyping mechanism details are given in Section 5. Performance evaluation results are shown in Section 6. Finally, Section 7 follows with the concluding remarks.

3 PIN considerations

We start to describe PIN by addressing the core of all the PIN problems. Six considerations are defined to evaluate the PIN. Those are:

- difficulty of network settings for endusers
- difficulty of server settings for endusers
- how efficient is the data exchange between individual devices?
- are nodes acting as robustly as servers?
- how to claim nodes (how to find nodes)?
- bandwidth reservation and bandwidth judgement.

PIN is a fully configurable network and is also configuration sensitive. The first time adoption configuration and maintain process really affect the intention of further adopting new devices. Tedious configuration processes will prevent the adoption and the usage of new devices. In contrast, between PIN and Enterprise internetwork, the Enterprise internetwork has professionals to solve most of these problems.

To fit the trend of the future networking environment, we choose to develop our PIN over IPv6 in local network. With IPv6 we can ease the network configuration by its autoconfiguration (Thomson and Narten, 1998) feature and the global IPv6 address makes real peer to peer communications possible. To ease the server settings and use less effort to achieve PIN, we adapt P2P architecture to obtain the benefit of easy server configuration, directly maintain individual devices' join, leave, resource search and share procedures.

Even if we have the infrastructure of IPv6 network, endusers still do not have many choices to access their remote devices with the current network applications. For a nomadic network, the long and hardly recognised IPv6 address will be the psychological barrier for endusers. Interpreting the address to domain name through home gateway (Wu et al., 2004) is a good idea, but in some cases we do not want to route through the gateway to communicate with destination devices. The node discovery (to get the remote resources addresses) through DNS is common in internet, but not quite familiar for personal and home scale devices. The reason is that those personal devices are not typical always-on servers like most servers over internet. For example, the mobile node is a reliable DNS node, but it is also an unstable (mobility) IP node and cost expensive node.

4 Node discovery stack (NDS) and personal P2P application (PP2P)

In spite of using personal gateway or broker to handle multiple devices, the P2P approach using NDS over IPv6 is considered to achieve PIN. Figure 1 shows the NDS architecture. In our proposal, a new type of P2P software is introduced to serve the existing problems of communication between personal devices, which is called Personal P2P Applications (PP2P). Figure 2 shows the proposed PIN architecture. The PP2P applications should act as normal P2P applications while they are doing resources searching, data publishing, data transmission and data slicing. The differences of PP2P and normal P2P applications are the sharing target and sharing scope. Because the sharing target is focused on individual's devices, like PC to smart mobile phone, smart mobile phone to net-music-player, PP2P will lead to a totally different kind of sharing file behaviour, and cause no intellectual property issues because these electronic resources are exchanged between logical local networks which are under ownership. And as PIN is a fully configurable network, pure P2P mechanisms are adoptable.

Figure 1 Node discovery stack

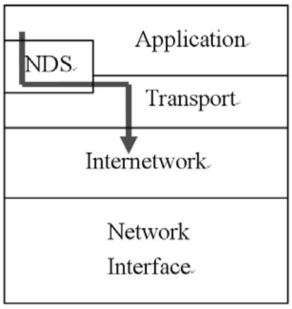
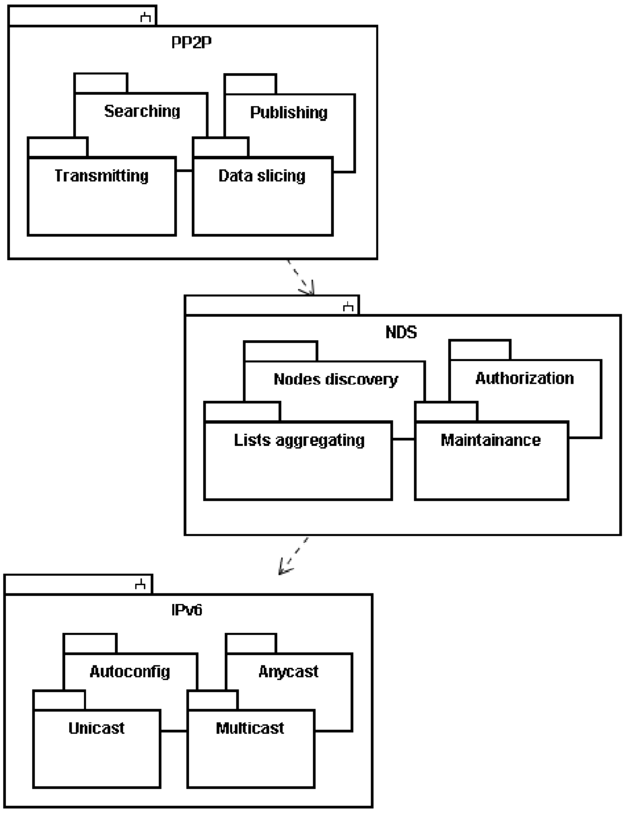


Figure 2 PIN architecture

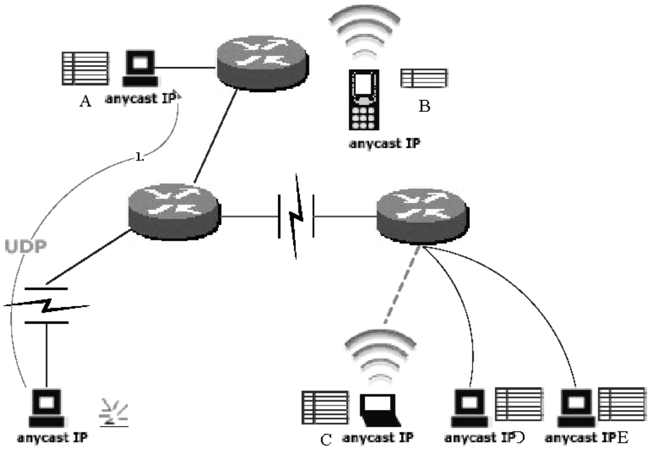


5 Node allocation mechanism

As shown in Figure 3, all of the computers and communication devices belong to an individual user, and all of them are connecting to the core router through wire or wireless connection. The user sends a NodeList Request message to the nearest Host A. While the user sets his personal anycast IP to a new device B, node B can acquire the nearest node A via Anycast options. NodeList Request message could contain loopback Node information for correspondent nodes (in this case, Node A), or transmit the Node information in the following secured procedure.

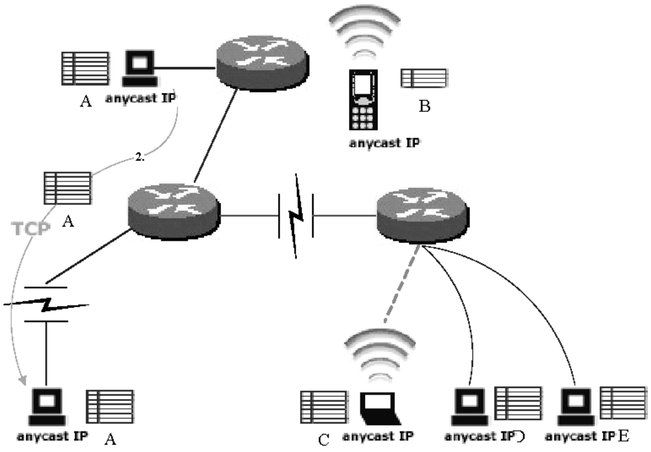
For the features of time and space locality in PIN, we use the gauge of adoptable scale for several types of anycast (Zhang and Hu, 2003) including IP layer anycast (Metz, 2002; Doi et al., 2004), Global IP layer anycast (Katabi and Wroclawski, 2000), application layer anycast (Zegura et al., 2000), and DNS.

Figure 3 Node request



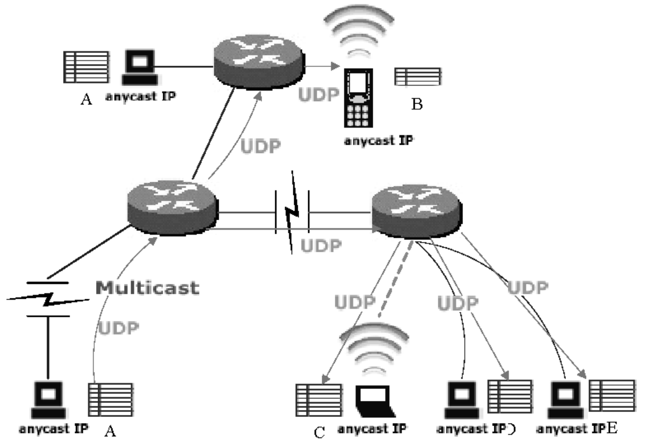
As shown in Figure 4, after proper authorisation procedures are done and the node is authorised, node A would send back the NodeList Acknowledgement message that brings the 'Node Maintain List' (this is information regarding global-link address and bandwidth etc., about all nodes in the PIN Group) to the node that requested the list.

Figure 4 Node response



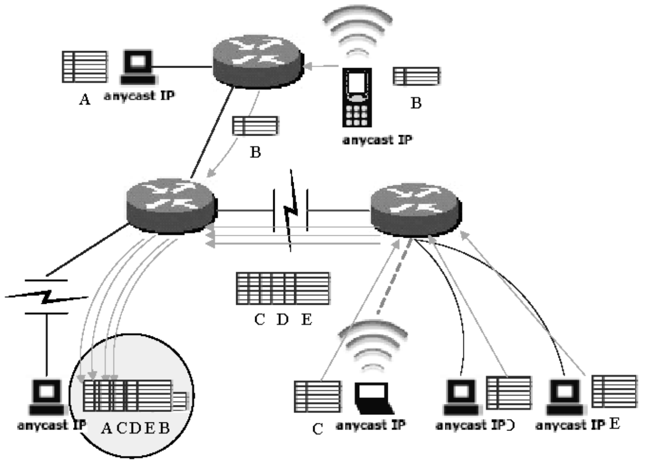
As shown in Figure 5, when a node requests for Node Maintain List to receive the list, it would add all node IPs into the Group. Then it would send a Unicast/Multicast Validate Request message to make sure that the nodes on the list are available. The advantage of using Multicast is not clear in hybrid P2P mode. But in pure P2P mode, multicast can reduce the requirement of bandwidth. Furthermore, it can reduce the cost when sending requests to several other nodes on the list (some ISPs used to bill their customers according to the data bits which they had sent).

Figure 5 Send multicast request to group, or send request to each nodes



As shown in Figure 6, all of the nodes that are alive in the list reply to the request node with their 'Node Maintain List'. While the Validate Request is received, nodes will compare the Record in their Node Information List. If all node records are the same, the node will return a Validate Acknowledgement message with Null payload. The Request node must compare all of these 'Node Maintain Lists', delete the repetition node, and connect the nodes that were never reached, until a well maintained PIN Group List is done. The Maintain procedure should repeat periodically to make sure that the Node information List is correct. After receiving a Validate Acknowledgement, the request node will calculate the SRTT (Smoothed Round Trip Time Estimate) and schedule the next Maintain time to Current time plus random value scaled in Interval parameter.

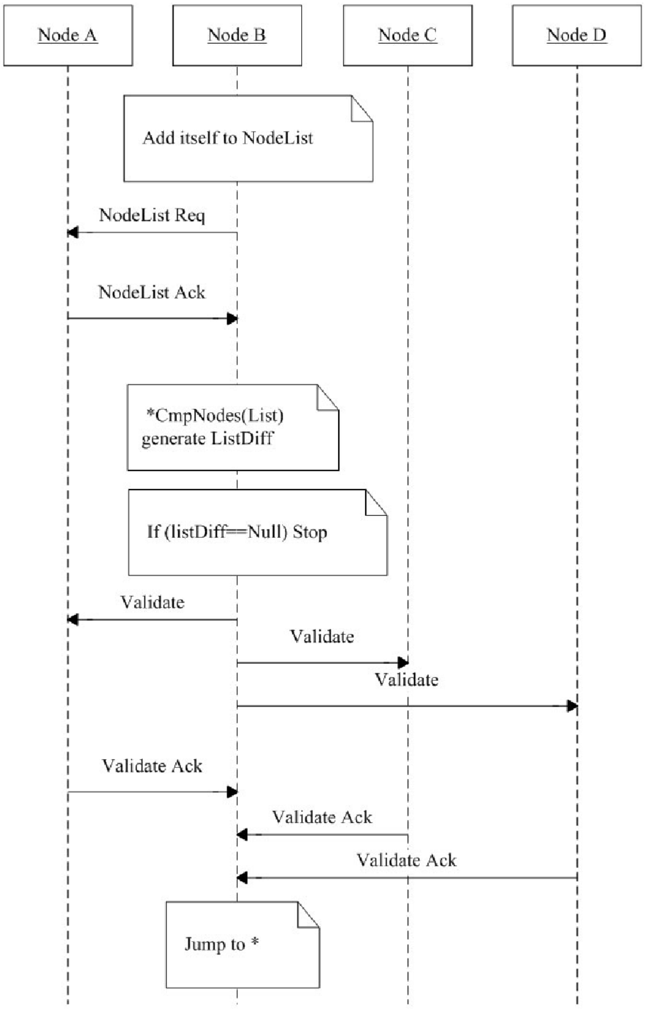
Figure 6 Node aggregation



The NDS procedure is shown in Figure 7. The full procedure has been illustrated at above sentences.

A more distributed environment will lead to much more management difficulty. Instead of using Rank value, Density value and Distance value to evaluate the Cluster-Based network (Lloyd, 2004), the setting time and bandwidth cost are also considered in PIN. To prioritise the links for selection, we give each link a weight according to its SRTT, BBW (Bottleneck Bandwidth) and the user customised NAC (Network Access Cost). Figure 8 shows the abstract Node Discovery Stack plotted within UML Class Diagram. ListHandler and NDStack are the main NDS panels to control the whole stack. NodeRecords are the main structure of each node's information, which is maintained by NodeMaintainer class. NodeList and ListDiff are extra message headers to encapsulate NodeRecords. Besides the procedures mentioned above, while the current node's network state is changed or the Maintain Interval is exceeded, the Maintain procedure is continued.

Figure 7 NDS procedure



The source mobility (Ernst et al., 2000) should be taken into consideration as well. To guarantee service continuity, a renew sequence based node allocation mechanism is used. As shown in Figure 9, while the node receives a new list, it extracts the node list to several node records, and then the CompareNode procedure uses the records to compare the Mac address of each node. NDS records the node's MAC address because it is the most stable identifier for each kind of node. The right branch shows whether the Mac address of Node Record matches, the CompareNode procedure is continued to compare the Renew Sequence parameter, which denotes the Maintain times (numbers) since the node is activated. Then it will append the new Record to 'ListDiff' record, which will be sent out through the NodeDeliver module. The left branch shows whether the Mac is not on this NDS's node list. NDS will add these node records to the node list. Then the Individuality Judgement (IJ) is activated. To make a balance between retrieving full node list and preserving bandwidth cost, Individuality Judgement denotes a decision procedure that will judge the proper next step based on node characters unveiled from RTT, BBW, NAC parameters. For a tightly integrated model, where PP2P and NDS are combined together, application information such as resource replica status could be taken into Individuality Judgement consideration, too.

Figure 8 Node discovery stack

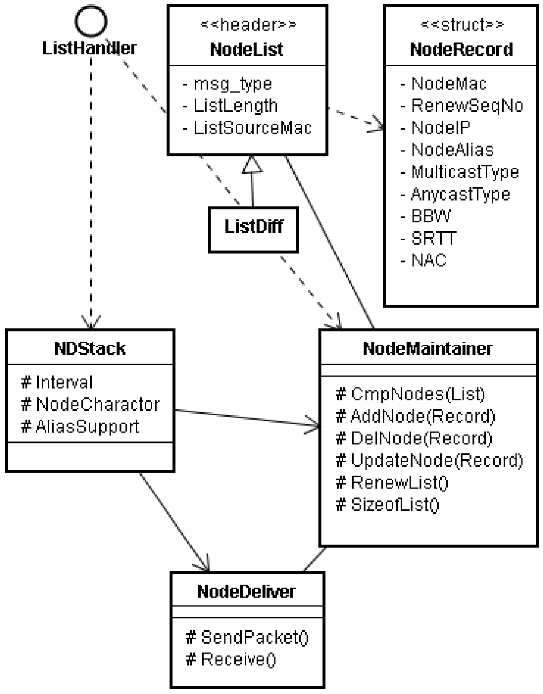
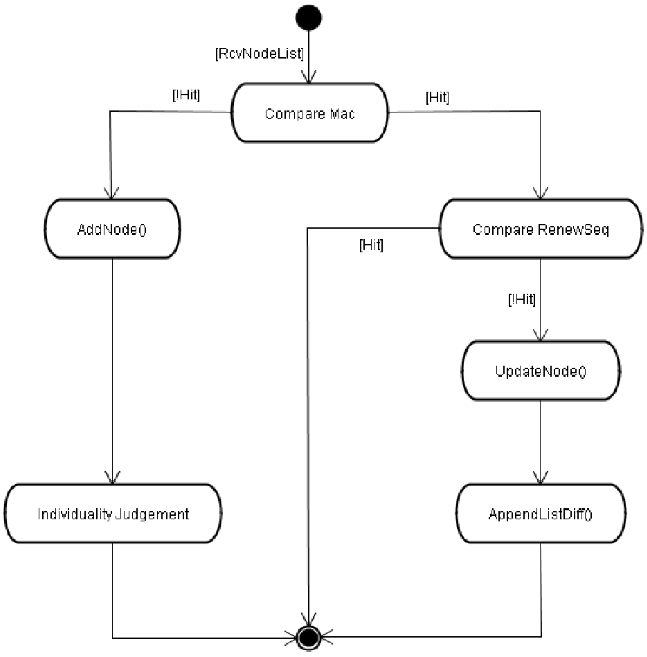


Figure 9 Compare node records



The device distribution bias will influence PIN in different device distribution schemes. For the best locality devices with the shortest logical distance (passing through less hops), we can imagine that this PING will have limited mobility. For the scheme with more mobility, the PING's location is harder to predict.

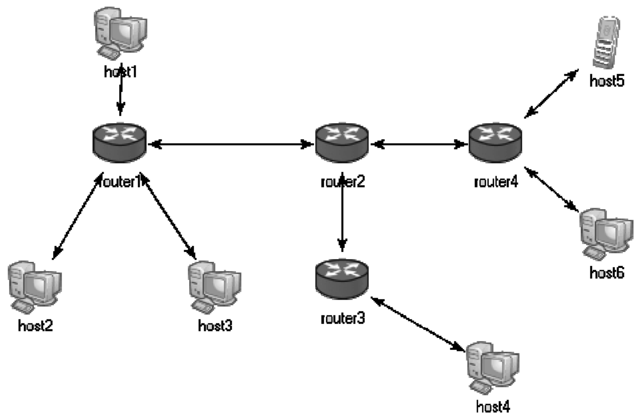
To take security into consideration, we have considered several approaches to enhance the security of NDS. To avoid the revelation of personal nodes information, in the NDS maintain procedure we could reduce the actual node list transmission frequency by sending to other nodes with the Node Record Hash instead. When other nodes received the hash record, it could be used to compare it with its existing record. If the hash is not the same, then the node activates an actual Node Record request by the hash records' index numbers. The exactly security cooperation model should be fully considered in future work.

6 Evaluation

We use OMNeT++ and IPv6SuiteWithINET (http://www.omnetpp.org/) module to implement our proposal. OMNeT++ is a component based, modular simulation environment based on C++. IPv6WithINET is an open source simulation model for OMNeT++, which integrates IPv6 and IP modules for simulation (Bless and Doll, 2004).

As shown in Figure 10, this network consists of four routers and six nodes (hosts), the top right node is a mobile device. We evaluate the system throughput for unicast and multicast datagrams. In the simulation, we could navigate the system's throughput with multicast which is better than using unicast, because multicast datagrams are duplicated by the router only if there is a group member in the subnet. Therefore, there is no redundant or unnecessary data packet.

Figure 10 Simulation topology



The nodes run a Node Discovery Stack which maintains the nodes list between the nodes. As the complete node list is not more important than a replica number (which denotes the available pieces of the resource file) in P2P, a brand new node could use fewer steps to aggregate most of Nodes in PIN.

As shown in Figure 11, based on the overall P2P file transmission, NDS causes less and less percentage of loading overhead but achieves better visibility of personal owned nodes, and makes personal internetwork possible.

Figure 11 Load percentage of NDS based on file transmission

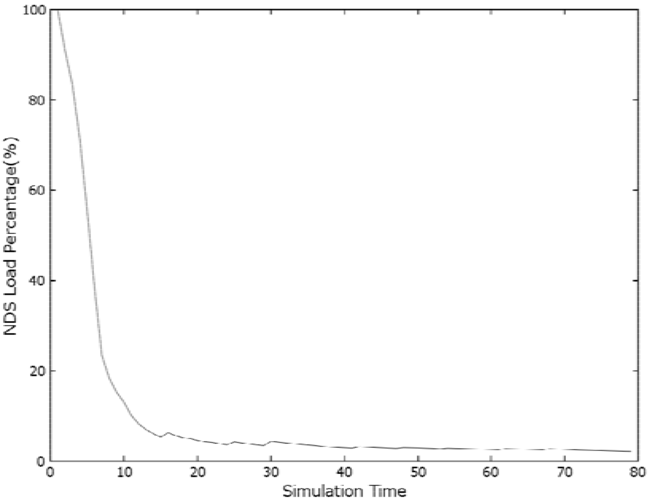
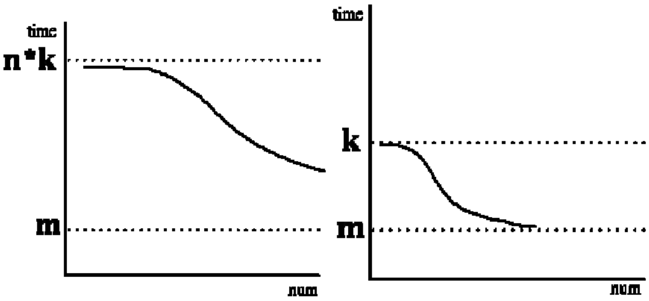


Figure 12 presents a decreased adaptation gap with lower setting time and bandwidth cost. The curve emulates what a user will experience: lesser average configuration time after several practices. The symbol m denotes minimum setting time that an experienced user would spend, k denotes the adoption configuration time for one device, n denotes the amount of devices within the PIN, num denotes the experience to do the configuration setting.

The left one in Figure 12 shows that if a user applies more number of devices, the configuration time will be increased with amount n. While the original nodes' configuration setting time would be bounded within n*k and m. The right one in Figure 12 shows that the Node Discovery Stack is used and the configuration setting time could be decreased and bounded within k and m.

Figure 12 Configuration setting time



7 Conclusion and future work

The PIN architecture is suitable for Hybrid or fully distributed P2P architecture. To facilitate PP2P applications design, parallel replica access of resources and files could be adopted in an efficient small files transmission. Better P2P information sharing systems have also been supported, such as IP mapping for the distributed hashing table (DHT) technique. This paper proposed PP2P and NDS to form the basis of PIN. The digital contents type of PIN is not like the traditional P2P resource type. In PIN, the new kind of PP2P application, decentralised vision control (Kao, 2003) for modified documents is needed.

Acknowledgement

This work is a partial result of project no NSC 94-2218-E-259-004 conducted by National Dong Hwa University under the sponsorship of the National Science Council, Taiwan, ROC.

References

Bless, R. and Doll, M. (2004) 'Integration of the FreeBSD TCP/IP-stack into the discrete event simulator OMNet++', *The 2004 Winter Simulation Conference*, 5–8 December, Washington DC, USA.

Conta, A. and Deering, S. (1998) *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*, RFC2463, IETF, December.

Deering, S. and Hinden, R. (1998) *Internet Protocol, Version 6 (IPv6) Specification*, IETF RFC 2460, December.

Doi, S., Ata, S., Kitamura, H. and Murata, M. (2004) 'IPv6 anycast for simple and effective service-oriented communications', *IEEE Communications Magazine*, Vol. 42, No. 5, May, pp.163–171.

Ernst, T., Castelluccia, C. and Lach, H.Y. (2000) 'Extending mobile-IPv6 with multicast to support mobile networks in IPv6', *Proc. IEEE ECUMN '00*, October, Colmar, pp.114–121.

Farber, D.J. (2002) 'Predicting the unpredictable: future directions in internetworking and their implications', *IEEE Communications Magazine*, Vol. 40, No. 7, July, pp.67–71.

Kao, C-L. (2003) *SVN*, http://svk.elixus.org/.

Katabi, D. and Wroclawski, J. (2000) 'A framework for scalable global IP-anycast (GIA)', *Proc. of the Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication*, Stockholm, Sweden, pp.3–15.

Lloyd, E.L. (2004) 'CLTC: a cluster-based topology control framework for ad hoc networks', *IEEE Transactions on Mobile Computing*, Vol. 3, No. 1, January–February, pp.18–32.

Metz, C. (2002) 'IP anycast point-to-(any) point communication', *IEEE Internet Computing*, Vol. 6, No. 2, March–April, pp.94–98.

Tetsuya, O-i., Sakai, K., Kikuma, K. and Kurokawa, A. (2003) 'Study of the relationship between peer-to-peer systems and IP multicasting', *IEEE Communications Magazine*, Vol. 41, No. 1, January, pp.80–84.

Thomson, S. and Narten, T. (1998) *IPv6 Stateless Address Autoconfiguration*, RFC 2462, December.

Wu, T.Y., Hsu, C-C. and Chao, H-C. (2004) 'IPv6 home network domain name auto-configuration for intelligent appliances', *IEEE Transactions on Consumer Electronics*, Vol. 50, No. 2, May, pp.491–497.

Ye, Z., Ji, Y. and Yan, S. (2004) 'Home automation network supporting plug-and-play', *IEEE Transactions on Consumer Electronics*, Vol. 50, No. 1, February, pp.173–179.

Yen, Y-S., Lin, F. and Chao, H-C. (2005) 'Integrated residential gateway: easy IA management with P2P community using RFID', *IEEE Transactions on Consumer Electronics*, Vol. 51, No. 3, August, pp.824–830.

Zegura, E.W., Ammar, M.H., Zongming, F. and Bhattacharjee, S. (2000) 'Application-layer anycasting: a server selection architecture and use in a replicated web service', *IEEE/ACM Transactions on Networking*, Vol. 8, No. 4, August, pp.455–466.

Zhang, R. and Hu, Y.C. (2003) 'Anycast in locality-aware peer-to-peer systems', *Proceedings of International Workshop on Networked Group Communications (NGC)*, September, Munich, Germany, pp.34–46.