Logging Operation History of DLNA Devices using ARP Spoofing

Timothy Lawrence Sitorus[1], Shunsuke Saruwatari[1], Hua Si[1], Masateru Minami[1], Hiroyuki Morikawa[1], Johan Hjelm[2], Kenta Yasukawa[2], and Toshikane Oda[2]

[1] Research Center for Advanced Science and Technology, The University of Tokyo, Tokyo 153-8904, Japan,
{tsitora, saru, sihua, minami, mori}@mlab.t.u-tokyo.ac.jp
[2] Ericsson Research Japan, Koraku Mori Bldg. 1-4-14 Koraku, Bunkyo-ku, Tokyo 112-004 Japan,
{firstname.lastname}@ericsson.com

Abstract. The realization of context-aware and recommendation service can be provided by acquiring and collecting the operation history of home appliances. In this paper, in order to collect operation information from DLNA certified devices, we propose a method using ARP spoofing called DLNA spoofing. We show that this method is effective to collect all detailed information in a home network. Also, DLNA spoofing has the better way for our research than the method using DLNA event notification function called GENA (Generic Event Notification Architecture). In GENA, we can collect only some simple information, nevertheless we cannot collect detailed information. On the other hand, by using our technique, we can collect all the information without changing the DLNA standard.

1 Introduction

Many studies have investigated services made from recommender systems. The realization of such systems can be provided by acquiring and collecting the users' pattern history. In Amazon.com [1], the recommendation service is provided based on user's purchase history. In TSUTAYA [2], the similar items that others have selected at the same time are collected and recommended to users. The key for these technologies are user modeling. Started in the latter half of the 1980's from the research of information filtering system [4], the history of user modeling as the field of research in virtual space is quite long.

On the other hand, ubiquitous computing with the concept that computing infrastructure as a tool should be available everywhere, every time, and to everybody, plays the key role to bring computer to real space. Pioneered by the concept from Mark Weiser [5], the research of ubiquitous computing has been widely investigated. Because of the research on sensor network and context-aware computing, ubiquitous world is being realized gradually.

The present study focuses on user modeling in ubiquitous computing. We can apply applications such as context-aware service and recommender service in real space. For instance, in context-aware service, we apply an automatic download service according to the users' time activity such as downloading content in the morning for the users who are not at home at night. In the advertisement field, we can show the advertisement to particular users based on their behavior such as advertisement of soft drink for users who are addicted to TV.

In this paper, in order to realize user modeling in ubiquitous computing, we acquire and collect the operation history of home appliance using DLNA [7] certified devices. DLNA, which is a technology that has been standardized for sharing videos, photos, musics, any time, any where in the home network, can be also seen as the first step towards the realization of the ubiquitous computing technology that has been put in a practical use.

2 Acquisition of operation history in DLNA Devices

Because the aim of this research is user modeling, we need to collect the detailed information from DLNA certified devices. The accuracy of user modeling improves by the acquired detailed information. For instance, we can create more detailed user modeling by collecting the information such as "what kind of program is being watched". It will be better than just by collecting simple information such as "user is watching TV".

There is a function called GENA (Generic Event Notification Architecture) [6], that notifies the operation of home appliances. UPnP [3] uses it for notifying events among devices. DLNA that adapted UPnP as the base protocol, uses GENA for event notification. For instance, one of the DLNA certified device classes, the DMR (Digital Media Renderer) notifies the information such as play or stop as an event to all clients connected to it. Beside the DMR, there are devices classified as the DMP. Nevertheless, the DMP does not report events by GENA since it includes playback control function in itselfs. The DMP and the DMR are two device classes for media consumption, but most of DLNA media consuming devices in the current market are the DMP. Therefore, at present we cannot use GENA to acquire the information required for this research.

3 DLNA Spoofing

Based on the discussion in Section 2, we propose a method called DLNA spoofing, a method to acquire operation history in DLNA devices based on ARP spoofing. By using DLNA spoofing, we can acquire the communication between all DLNA certified devices and collect the operation history without interfere the DLNA standard. The acquired information is not only simple information such as "when it is being played" or "when it is being stopped", but also detailed information such as "what kind of content that is being watched".

DLNA spoofing can be described as follows. For an example, we take three devices that are connected to a home network, which are a TV that is certified

as DMP (Digital Media Player), a video recorder that is certified as DMS (Digital Media Server) and a DLNA snooper which is a home gateway that has a function to collect the information of operation history. IP and MAC addresses of the three devices are, `192.168.0.1` and `00:00:00:00:00:11` for the DLNA snooper, `192.168.0.2` and `00:00:00:00:00:22` for the DMP, `192.168.0.3` and `00:00:00:00:00:33` for the DMS. First, the DLNA snooper discovers the DMP and the DMS using one of DLNA function, SSDP (Simple Service Discovery Protocol). At the same time, the DLNA snooper can obtain the IP and MAC addresses of the clients. Then, using those IP and MAC addresses, we can send the ARP request periodically to the DMR and the DMS to change the ARP table. For instance, we send the ARP request to the DMP with IP source of the DMP `192.168.0.3`, MAC source of the home gateway `00:00:00:00:00:11` and IP destination of the DMP `192.168.0.2`, MAC destination of the DMP `00:00:00:00:00:22`. By doing this, all the data sent from the DMP to the DMS will transit the DLNA snooper. So, this method can change the routes of the communication between the DLNA devices and make all the data transited to the DLNA snooper.

4 Preliminary Evaluation

Table 1 shows the impact on the throughput between the DLNA devices when DLNA spoofing is used. It shows the throughput according to different numbers of flow in the same home network. Concretely, we used 6 devices and measured the throughput using `netperf` through a switch with the capacity of 100Mbps. Without using the DLNA spoofing, there is no impact on the throughput even when the flow increases. By using the DLNA spoofing, the network performance decreases gradually according to the number of flow. Considering that the traffic on service in DLNA such as video and picture is below 10 Mbps, the reduction of throughput according to number of flow is acceptable. However, it will be a problem if more than 6 devices are played at the same time in the same home network.

Table 1. The throughput between the DLNA devices

	1 flow	2 flow	3 flow
without DLNA spoofing (Mbps)	94.14	94.14	94.14
with DLNA spoofing (Mbps)	87.3	37.43	27.81

Then, we use ping command 1000 times between two terminals to calculate RTT (Round Trip Time). Without using the DLNA spoofing, the average of RTT is 0.559 ms and the standard deviation is 0.157 ms. By using the DLNA spoofing, the average of RTT is 0.669 ms and the standard deviation is 0.528 ms. Also, the calculation of the delay for 100 times out of 1000 times is shown in Fig.1. We can see that the delay increases when the DLNA spoofing is applied.

However, we can say that the impact of the DLNA spoofing is small because we can assume that in DLNA, when considering the delay factor, the most sensitive is voice communication and the maximum of acceptable delay is about 10 ms.

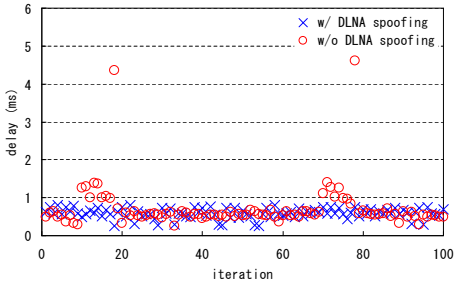

Fig. 1. RTT for 100 times out of 1000 times trial

5 Summary

In this paper, we proposed the DLNA spoofing as the method for logging operation history of the DLNA devices. The DLNA spoofing acquires all the information without changing the DLNA standard. In this paper, we showed the preliminary evaluation of the traffic between the devices when DLNA spoofing is used. At present, we are analyzing the method on user modeling using operation history based on DLNA spoofing.

6 Acknowledgment

This work is supported by Ministry of Internal Affairs and Communications, Japan (Ubiquitous Service Platform).

References

1. http://amazon.com
2. http://www.tsutaya.co.jp
3. http://www.upnp.org
4. Thomas W. Malone, Kenneth R. Grant, Kum-yew Lai, Ramana Rao, and David Rosenblitt: Semi-structured are Surprisingly Useful for Computer-Supported Coodination, Proc. of CSCW 86, pp. 102-114(1986)
5. M. Weiser: The Computer for the Twenty-First Century, Scientific American, pp. 94-101, 1991
6. J. Cohen, and S. Aggarwal: General Event Notification Architecture Base. Internet Draft(1999)
7. Digital Living Network Alliance, http://www.dlna.org/