DLNA Protocol Analysis Tool for Smart Device Interoperability Test

Yong-Suk Park, Se-Ho Park , Kyung-Taek Lee, Myung-Hyun Yoon
Communications & Media R&D Division
Korea Electronics Technology Institute
Seoul, Korea

Abstract—**The propagation of smart devices and the rapid expansion of wireless mobile networks have increased the need for ubiquitous device connectivity and contents access. DLNA is currently being used as the de facto standard for connectivity of consumer devices in the digital home. The guidelines provided by DLNA are intended to facilitate device and contents discovery, management, sharing and distribution. In this paper, the design and implementation of a DLNA protocol analysis tool is presented for interoperability analysis among smart devices. The tool monitors the home network and performs analysis of the underlying protocols used by DLNA. The tool can be used for diagnostics and troubleshooting, enabling the developer to test DLNA functionality of Smart device**

Keywords— DLNA, protocol analysis, interoperability analysis, content sharing, home network

I. Introduction

Diverse smart devices such as smartphones, tablets, and smart TVs have emerged over the past few years and have gained increasing popularity. The dissemination of such smart devices has increased the use and exchange of multimedia contents, leading to the need for easy media sharing and seamless contents access. The seamless display of multimedia contents among various devices is known as "N-screen" service. Many different technologies can be used for N-screen services. Many commercial service providers offer cloud web server based services to enable N-screen. A popular choice in the home networking environment is Digital Living Network Alliance (DLNA) technology.

In the home network, DLNA is one of the most widely used ways of multimedia sharing. Most of the networked multimedia consumer electronic devices in the market implements DLNA in one form or the other. DLNA enables you to stream media content between devices connected to the same home network, using either wired or wireless connection, without having to store the content on both devices [1]

In this paper, the design and implementation of a DLNA protocol analysis tool for smart device interoperability test is presented. The tool monitors the home network, detects DLNA devices connected in the network, and performs analysis of the underlying protocols used. The tool can be used to test and analysis DLNA functions between devices or problems in the network. The user can diagnose and troubleshoot existing or potential problems in DLNA operation.

II. DLNA Analysis Tool

In order to provide the user with useful information about the devices connected in the home network, the type of media formats supported, as well as analysis on errors and misoperation, the following design of the analysis tool is proposed, illustrated in Fig. 1.

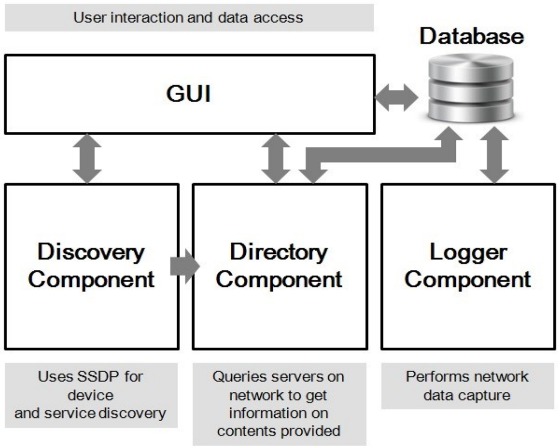

User interaction and data access
Database
GUI
Discovery Component
Directory Component
Logger Component
Uses SSDP for device and service discovery
Queries servers on network to get information on contents provided
Performs network data capture

Fig. 1. High-level block diagram of the analysis tool

The basic experimental environment is illustrated in Fig. 1. A wireless access point router manages connection of wireless DLNA devices. It also dynamically assigns local IP address to all DLNA devices on the network through its DHCP (Dynamic Host Configuration Protocol) server. A dummy hub is connected to the wireless access point router via a single Ethernet cable. All wired DLNA devices are connected to the dummy hub, including the DLNA analysis tool. A dummy hub is used in order to facilitate network packet capture. Most network devices today operate in switching mode, which means that unicast traffic will be forwarded only to its associated or connected port. This increases network performance, but capturing of all traffic

This work was supported by the IT R&D program of MSIP/IITP. [10039196, Smart Platform Development for Integrating Worldwide Radio Technology to Smart Devices]

978-1-4799-8342-1/15/$31.00 ©2015 IEEE

data within the network is not possible. The use of a dummy hub creates a shared media network allowing all traffic data to be received on all its ports. Therefore, the DLNA analysis tool with its network adapter operating in promiscuous mode will be able to see and capture all packets in the network.

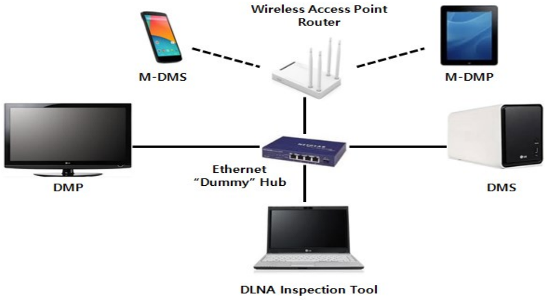


Fig. 2. Test environment setup

III. Implementation Results

The DLNA protocol analysis tool was implemented on a PC running Windows operating system. Fig. 3 shows a snapshot of the initial implementation of the DLNA analysis tool.

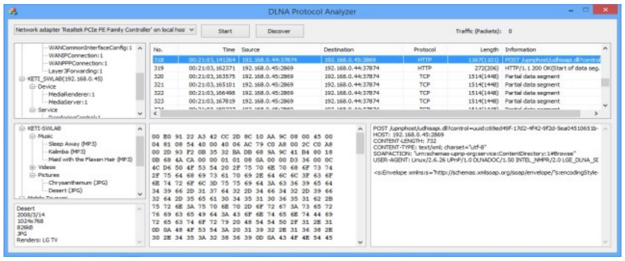
To perform analysis of DLNA data by capturing network traffic, WinPcap was used [8]. WinPcap provides a Windows OS based network interface API (Application Program Interface). Network packets are captured from the network adapter set to operate in promiscuous mode. The captured data is saved to a database. SQLite was used as the database for its simplicity of use. In addition, unlike other client-server databases, SQLite can be embedded into the program and become an integral part of it. Information on the data captured can be retrieved from the database for further analysis.

The right-top window of the GUI displays IP traffic captured. In order to reduce computation and processing burden, the IP stream is filtered and only packets that are relevant to DLNA are captured. If a particular data is selected, the captured data is retrieved from the database, and its hexadecimal data and payload information are displayed in the windows below.

The three windows on the left side show DLNA device information in the network. The top window displays device and service information for each DLNA device discovered. This information is obtained by analyzing SSDP relevant traffic data. The middle window shows all media files discovered. Content Directory information is processed to extract information on media formats supported and media files currently available in the network. The last window displays additional information about a device, service, or content selected. For media files, it also provides information about compatible devices.

This initial implementation is able to detect devices and list the available multimedia contents, as well as identify compatibility in media formats. Currently, the GUI lists the devices and provided contents, and shows the details about media formats. The GUI also shows all DLNA relevant data traffic, so analysis on network or protocol relevant problems can be performed by tracing the data captured. Since manual data tracing of captured data can be a tedious task, we intend to enhance the tool and include protocol flow graphs in order to automate and facilitate analysis of traffic flow.

In addition, the use of Address Resolution Protocol (ARP) spoofing may be necessary for more detailed analysis as described in [9]. ARP spoofing is a technique where fake ("spoofed") ARP messages are sent onto a Local Area Network. The aim is to associate the analysis tool's MAC address with the IP addresses of other DLNA devices, causing any traffic meant for those IP address to be sent to the analysis tool instead. ARP spoofing is an effective method to collect all detailed information in a home network, since all traffic will be sent to the analysis tool before reaching their actual destinations.


DLNA Protocol Analyzer
Network adapter 'Realtek PCIe FE Family Controller' on local hos
Start
Discover
Traffic (Packets): 0

```
WANCommonInterfaceConfig:1
WANIPConnection:1
WANPPPConnection:1
Layer3Forwarding:1
KETI_SWLAB(192.168.0.45)
  Device
    MediaRenderer:1
    MediaServer:1
  Service
```

No.	Time	Source	Destination	Protocol	Length	Information
318	00:21:03,141264	192.168.0.44:37874	192.168.0.45:2869	HTTP	1167(1101)	POST /upnphost/udhisapi.dll?control
319	00:21:03,162371	192.168.0.45:2869	192.168.0.44:37874	HTTP	272(206)	HTTP/1.1 200 OK(Start of data seg.
320	00:21:03,163575	192.168.0.45:2869	192.168.0.44:37874	TCP	1514(1448)	Partial data segment
321	00:21:03,165101	192.168.0.45:2869	192.168.0.44:37874	TCP	1514(1448)	Partial data segment
322	00:21:03,166498	192.168.0.45:2869	192.168.0.44:37874	TCP	1514(1448)	Partial data segment
323	00:21:03,167819	192.168.0.45:2869	192.168.0.44:37874	TCP	1514(1448)	Partial data segment

```
KETI-SWLAB
  Music
    Sleep Away (MP3)
    Kalimba (MP3)
    Maid with the Flaxen Hair (MP3)
  Videos
  Pictures
    Chrysanthemum (JPG)
    Desert (JPG)
```

```
Desert
2008/3/14
1024x768
826kB
JPG
Renders: LG TV
```

```
00 E0 91 22 A3 42 CC 2D 8C 10 AA 9C 08 00 45 00
04 81 08 54 40 00 40 06 AC 79 C0 A8 00 2C C0 A8
00 2D 93 F2 0B 35 32 BA DB 68 9A 9C 41 B4 80 18
0B 68 4A CA 00 00 01 01 08 0A 00 00 D3 36 00 0C
4C D6 50 4F 53 54 20 2F 75 70 6E 70 68 6F 73 74
2F 75 64 68 69 73 61 70 69 2E 64 6C 6C 3F 63 6F
6E 74 72 6F 6C 3D 75 75 69 64 3A 63 36 39 65 64
34 39 66 2D 31 37 64 32 2D 34 66 34 32 2D 39 66
32 64 2D 35 65 61 30 34 35 31 30 36 35 31 62 2B
75 72 6E 3A 75 70 6E 70 2D 6F 72 67 3A 73 65 72
76 69 63 65 49 64 3A 43 6F 6E 74 65 6E 74 44 69
72 65 63 74 6F 72 79 20 48 54 54 50 2F 31 2E 31
0D 0A 48 4F 53 54 3A 20 31 39 32 2E 31 36 38 2E
30 2E 34 35 3A 32 38 36 39 0D 0A 43 4F 4E 54 45
```

```
POST /upnphost/udhisapi.dll?control=uuid:c69ed49f-17d2-4f42-9f2d-5ea0451065 1b-
HOST: 192.168.0.45:2869
CONTENT-LENGTH: 732
CONTENT-TYPE: text/xml; charset="utf-8"
SOAPACTION: "urn:schemas-upnp-org:service:ContentDirectory:1#Browse"
USER-AGENT: Linux/2.6.26 UPnP/1.0 DLNADOC/1.50 INTEL_NMPR/2.0 LGE_DLNA_SE

<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"s:encodingStyle-
```

Fig. 3. Implementation of the DLNA analysis tool

IV. Conclusion

In this paper, the design and implementation of a DLNA protocol analysis tool is presented in order to test and analyze DLNA functions between devices and problems in the network. The tool monitors the network, captures DLNA relevant traffic, and performs analysis of the protocols used by DLNA. The tool discovers and identifies DLNA devices on the network and creates a topology of services and media contents provided.

Based on the media type classification information provided by the tool, the user is able to test device interoperability. Since the tool also captures all IP traffic relevant to DLNA, networking or protocol problems can also be identified.

References

[1] DLNA, "DLNA for HD Video Streaming in Home Networking Environments", DLNA Whitepaper, May 2011.

[2] F. Risso and L. Degioanni, "An Architecture for High Performance Network Analysis", in Proc. of the 6th IEEE Symposium on Computers and Communications (ISCC 2001), pp. 686-693, July 2001.

[3] S. Saruwatari, J. Hjelm, T. Oda, and H. Morikawa, "A System for Logging Operation Histories of DLNA Devices by Combining ARP Spoofing and SSDP", IEEE International Conference on Consumer Electronics (ICCE), pp. 233-234, January 2011