Vol.2010-MBL-52 No.9
2010/1/29

DLNA デバイスの操作履歴取得手法の検討

猿渡俊介[†1]　司　化[†1]　森川博之[†1]
ヨハン イェルム[†2]　小田稔周[†2]

DLNA デバイスの操作履歴から抽出可能な，ユーザがいつ，どのように，どのようなコンテンツを閲覧したかなどの情報は，新商品の開発やユーザの状況にあわせた推薦サービスなどに役立てることができる．本稿では，DLNA デバイス間の通信を ARP スプーフィングを用いてモニタリングすることで DLNA デバイスの操作履歴を取得するシステム「DLNA Probe」の設計について述べる．DLNA Probe を用いることで，既存の DLNA の枠組みを壊すことなく，ホームネットワークに DLNA Probe を接続するだけで DLNA デバイスの操作履歴を収集することができる．

Design of a System for Getting Operation History from DLNA Devices

Shunsuke Saruwatari,[†1] Si Hua,[†1]
Hiroyuki Morikawa,[†1] Johan Hjelm[†2]
and Toshikane Oda[†2]

We can extract user activity data, such as when and how the users enjoy contents, from operation history of DLNA devices. The activity data are useful for ethnography, context-aware recommendation services, and so on. In this paper, we show DLNA Probe, which is a system for getting operation history from DLNA devices by monitoring communication among the DLNA devices using ARP spoofing. In DLNA Probe, we do not need to change the DLNA specification, but only need to connect the DLNA Probe to a home network.

†1 東京大学 森川研究室 (Morikawa Laboratory, The University of Tokyo)
†2 日本エリクソン株式会社 (Ericsson Research Japan)

1. はじめに

われわれは生活をしながら無意識のうちに大量の情報を生み出している．情報技術の発展によってさまざまな情報が蓄積・解析可能となった現在，個人情報をどのように扱うかが今後のわれわれの生活を楽しく，充実したものにできるかどうかの鍵になる．もはや使い古された個人情報利用の例として，Amazon の推薦サービスが挙げられる．Amazon ではユーザの購入履歴などの個人情報を利用してユーザに対して本を推薦するサービスを提供している．Amazon に自分が購入した商品や閲覧した商品などがすべて監視されているという恐怖感を感じつつも，推薦された書籍をついついクリックし，最終的には購入した人も少なくは無いであろう．個人情報の利活用はインターネット上に構築された仮想空間でのユーザの行動情報（リンクのクリック等）の下では成功しつつあると言える．

このような仮想空間での成功を受けて，家庭内でユーザの行動情報を取得したり利用したりするための研究開発が活発化している[12)–15),19),21),24),28),29),32)]．しかしながら，これらの研究では現実的には設置が困難な量のセンサや，ユーザが特殊なデバイスを具備することを前提としており，実用化とは隔たりがある．例えば，MIT の Place Lab[12)] では，百以上のセンサが埋め込まれたテストベッドを構築し，ユーザが数日から数週間生活した際のデータを取得・蓄積して公開している．Place Lab はテストベッドであるから数百のセンサを設置できるのであり，実際の生活空間で同様のシステムを構築することは困難である．これらの研究のように最先端技術を駆使してアプリケーションエリアの可能性を模索する研究も重要であるが，それと同時に，これらの行動情報を利用したサービスをどのように実際の環境に展開していくかも検討する必要がある．

このような観点から，筆者らは家庭内でのユーザの行動情報を実用的な形で取得することを目指す．具体的には，既に多くの商品が発売されており，一般家庭にも展開されつつある DLNA デバイス[6)] の操作履歴を取得して行動情報を抽出する．DLNA デバイスの操作履歴を抽出できれば，ユーザがいつどのようなタイミングでどのようなコンテンツを閲覧したかなどが分かる．また，DLNA デバイスはインターネットを介したコンテンツ共有などインターネット上に築かれた仮想空間とわれわれが生活する実空間を接続するための鍵となる技術であるため[1),2),7),10),11),16)–18),20),23),26),27),30),31)]，推薦サービスなど行動情報の利活用への発展が容易である．

本稿では，DLNA デバイス間の通信を ARP スプーフィングを用いてモニタリングすることで DLNA デバイスの操作履歴を取得するシステム「DLNA Probe」の設計について述

べる．DLNA Probe は，既存の DLNA の枠組みを壊すことなく DLNA デバイス間の通信のみをモニタリングするので，実環境に簡単に導入することができ，また，ユーザが意識することなく行動情報を取得することが可能になる．DLNA Probe は，DLNA の SSDP[8]（Simple Service Discovery Protocol）と RAW ソケットを用いて DLNA デバイスを発見して IP アドレスと MAC アドレスを取得する．取得した IP アドレスと MAC アドレスを用いて ARP スプーフィングを行い，DLNA デバイス間の通信を全て DLNA Probe を経由するように各 DLNA デバイスの ARP テーブルを書き換える．そして，DLNA Probe を通過するパケットの中身を走査してユーザによる DLNA デバイスの操作情報を取得する．パケットの走査では，HTTP メッセージのリクエスト行の先頭に記述されている GET，POST，PUT のみを照合することで低オーバヘッドかつ低ストレージ容量で操作履歴を取得することができる．

本稿の構成は以下の通りである．まず，2. で，既存のユビキタスコンピューティングやユーザモデリングの分野で行われているユーザの行動情報を取得して利活用することを目指す研究を概観し，本研究で DLNA デバイスの操作履歴の取得に着目した理由を明らかにする．次に 3. で，本稿で提案する DLNA デバイスから操作履歴を取得するための技術である DLNA Probe の全体像と各機構の詳細について述べる．4. で DLNA Probe の初期的な評価を示し，最後に 5. でまとめとする．

2. 関 連 研 究

本研究では，実空間でユーザの行動情報を取得する技術を実用的な形で実現することを目指す．そのためには，実環境に簡単に展開できること，ユーザが意識することなく活動情報を取得できることの 2 つの要件を満たす必要がある．

2.1 行動情報取得技術

現在，ユビキタスコンピューティングやユーザモデリングの研究コミュニティを中心に，実空間でのユーザの行動情報を蓄積して新しいサービスや知識を生み出すことを目指して多くの研究がなされている[12)–15),19),21),24),28),29),32)]．実空間上で取得された情報はコンテクストアウェアサービス，推薦サービス，エスノグラフィなどさまざまな分野へ応用できる．たとえば，MIT の Place Lab では，百以上のセンサを生活空間を模した環境に埋め込み，ユーザが実験的にその環境で生活した際の情報を取得・公開している[12)]．Place Lab で取得された情報は，家庭内の電力消費を削減するコンテクストアウェアサービスの研究などで利用されている[22)]．Zancanaro らの研究[29)] では，美術館で得たユーザの移動履歴を用いてユーザの行動パターンを教師無し学習で分類した結果，エスノグラフィで得られた分類と同様の分類が可能であることが示されている．

ところが，現状の研究コミュニティで検討されているユーザの行動情報を取得する手法は，特殊な機器，装置，環境を前提としている点が問題になる．たとえば，Place Lab では Living Laboratory と呼ばれる生活空間を緻密に再現した模擬環境に対して高密度にセンサを埋め込む[12)]．Place Lab で用いられているセンサは Maxim 社の TINI ネットワークマイクロコントローラを用いることによって空間に埋め込みやすい工夫がなされているが，百以上ものセンサを実際に人が生活している実環境にそのまま埋め込むことは現実的ではない．特殊なデバイスをユーザに持たせて行動情報を取得した研究として，Zancanaro らの研究[29)] が挙げられる．Zancanaro らの研究[29)] では美術館を歩き回るユーザにハンドヘルドデバイスを持たせることを前提としている．確かにユーザに特殊なデバイスを持たせることができればユーザの行動情報を詳細に取得できるが，デバイスを持つことでユーザの行動が変化する可能性や，ユーザが常にデバイスを具備しなければならないというコストを無視できない．

2.2 DLNA デバイスの操作履歴の取得

テストベッドの域を出ることができない現状の行動情報取得技術に対し，筆者らは実環境で DLNA デバイスの操作履歴を取得する技術の実現を目指す．DLNA は家庭内でのメディア機器，PC，モバイル機器の相互接続を実現するための業界標準であり，UPnP[25)] を基盤にガイドラインを作成している[6)]．既に多くの企業がテレビ，ブルーレイディスクレコーダ，デジカメなどの DLNA デバイスを販売しており，徐々に一般家庭内にも普及し始めている．DLNA デバイスの操作履歴を取得することができればユーザの行動情報を抽出してさまざまな応用が期待できる．たとえば，操作履歴を取得した結果としてユーザが夜間に音楽を聴きながらショートコンテンツを楽しむ「ながらユーザ」であることが抽出できた場合，ながら作業でも楽しむことができるようなショートコンテンツをお勧めする推薦サービスを提供することができる．エスノグラフィ的な観点では，DLNA デバイスをどのようにユーザが利用するかが観察できれば新商品の開発のヒントを得ることも可能であろう．

また，DLNA は単にホームネットワーク内のデバイス同士の連携を促進する技術ではない．DLNA デバイスをはじめとした情報家電は，インターネット上に築かれた仮想空間とわれわれが生活する実空間をシームレスに接続する架け橋の役割を担う．そのため，DLNA デバイスを介してユーザの活動情報を取得することができれば，これまでウェブサービスを中心に培われたユーザモデリング技術との連携も容易となる．実際に，YouTube の動画を DLNA デ

バイスで閲覧可能とする製品，DLNA と SNS を連携させて友達や家族とコンテンツを共有するサービス[23]，サードパーティに DLNA 内のコンテンツを提供するための技術[1]，IPTV や IMS と融合するための技術[3),7)]，モバイルデバイスや外部のホームネットワークからインターネットを介して DLNA デバイスにアクセスするための技術[2),10),11),16)–18),20),26),27),31)]などの研究開発がされている．

DLNA デバイスの操作履歴を取得する方法として，DLNA デバイス自身が直接操作情報を広告する手法が考えられる．DLNA の基盤となっている UPnP[25] はイベントを通知する GENA[4] と呼ばれる仕組みを持っているため，GENA でユーザの操作情報を通知することができれば操作履歴を取得することができる．たとえば，DLNA の DMR（Degital Media Renderer）では複数の DMC（Digital Media Controller）による操作の同期のために GENA を用いて操作履歴を通知する仕組みを提供している．しかしながら，現状では DLNA では DMR における再生イベントなどのごく一部のイベントしか通知しない．仮に将来的に操作履歴を全て通知することを DLNA の標準に組み込むとしても，まずは操作履歴を取得することが有用であることを実証する必要がある．

3. DLNA Probe

2. での議論に鑑み，本研究では DLNA デバイス間の通信をモニタリングする機器「DLNA Probe」を用いて操作履歴の取得を行う．ホームネットワークが全てリピータハブを用いて構築されていればイーサネットのプロミスキャスモードを用いて全てのトラフィックをモニタリングすることができる．しかしながら，現在の家庭内ではリピータハブはほとんど用いられておらず，スイッチングハブや無線 LAN を用いる．そのため，イーサネットのプロミスキャスモードを用いたとしても通信をモニタリングできるとは限らない．

そこで DLNA Probe では ARP スプーフィングを用いて各 DLNA デバイスの ARP テーブルを外部から書き換え，DLNA デバイス間の通信が全て DLNA Probe 経由になるようにリダイレクトすることで DLNA デバイス間の通信をモニタリングする．図 3 に DLNA Probe の全体像を示す．DLNA Probe は，デバイス発見機構，デバイス管理機構，ARP テーブル書換機構，リダイレクト機構，操作履歴取得機構の 5 つの機構から構成される．

3.1 デバイス管理機構

デバイス管理機構はデバイス情報を管理するための機構である．デバイス管理機構では，デバイス発見機構から送られてくる各 DLNA デバイスの IP アドレス，MAC アドレス，タイムスタンプの組を管理し，ARP テーブル書換機構，リダイレクト機構，操作履歴取得機構に対して，デバイス情報をデバイステーブルとして提供する．

デバイス管理機構は TCP ポート 21401 で TCP 接続を待ち受けている．まず，デバイス発見機構，ARP テーブル書換機構，リダイレクト機構，操作履歴取得機構は TCP ポート 21401 に接続してデバイス管理機構と接続を確立する．次に ARP テーブル書換機構，リダイレクト機構，操作履歴取得機構はデバイステーブルを

`LIST\n`

のコマンドで取得する．取得要求を受け取ったデバイス管理機構は現在のデバイステーブルを

`LIST` *ip_address1*:*mac_address1*, *ip_address2*:*mac_address2*,...`\n`

の形式で要求元に対して返信する．

デバイス発見機構が新しいデバイスを発見した場合，デバイス管理機構に対して TCP セッションを介して

`ADD` *ip_address*/*mac_address*`\n`

の形式で追加コマンドを送信する．追加コマンドを受け取ったデバイス管理機構は，引数に含まれる IP アドレスと MAC アドレスの項目を既に持っている場合には，該当する項目の

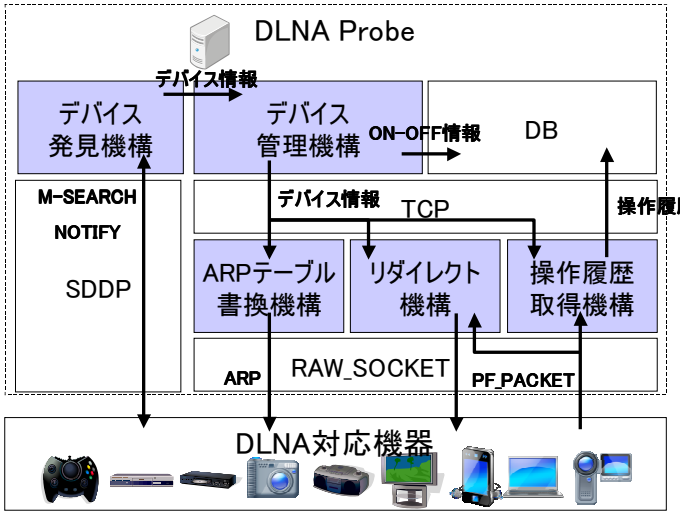

図 1 全体像

タイムスタンプを現在の時刻に更新する．引数に含まれる IP アドレスと MAC アドレスに一致する項目が無かった場合には新しい項目を作成し，ARP テーブル書換機構，リダイレクト機構，操作履歴取得機構に対してデバイスが追加されたことを知らせるメッセージ

`ADDED` *ip_address*`/`*mac_address*`\n`

を送信する．それと同時に，データベースにデバイスの電源が入ったことを記録する．

デバイス発見機構は，DLNA デバイスがホームネットワークから離脱したことを検出した場合，デバイス管理機構に対して TCP セッションを介して

`DELETE` *ip_address*`/`*mac_address*`\n`

の形式で削除コマンドを送信する．削除コマンドを受け取ったデバイス管理機構は，引数に含まれる IP アドレスと MAC アドレスに一致する項目があった場合にはその項目を削除し，ARP テーブル書換機構，リダイレクト機構，操作履歴取得機構に対してメッセージ

`DELETED` *ip_address*`/`*mac_address*`\n`

を送信する．それと同時に，データベースにデバイスの電源が切られたことを記録する．デバイステーブルからの項目の削除の動作は，デバイス管理機構で管理している各 DLNA デバイスの項目のタイムスタンプが現在の時刻よりも 1 分経過した場合にも実行される．

3.2 デバイス発見機構

デバイス発見機構は定期的に SSDP（Simple Service Discovery Protocol）[8] を用いてデバイスの発見を行い，デバイス管理機構に対して発見したデバイスを通知する．デバイス発見機構では，DLNA の検索機能を用いた能動的な発見と，DLNA デバイスの広告の監視による受動的な発見の 2 つの仕組みによってネットワーク内の DLNA デバイスを発見する．能動的な発見は，広告をしないデバイスの発見に利用する．受動的な発見は，DLNA の検索に対して返信をしないデバイスの発見に利用する．能動的な発見と受動的な発見を組み合わせることで，DLNA デバイスをすばやく発見できるとともに，障害によって DLNA デバイスがホームネットワークから離脱した場合でもデバイステーブルを正しい状態に保つことができる．

能動的な発見では，定期的に M-SEARCH メッセージをマルチキャストすることでデバイステーブルを最新に保つ．M-SEARCH は，SSDP において他の DLNA デバイスを検索するための仕組みである．他のサービスを発見したい場合，端末は M-SEARCH メッセージを HTTPMU[9] で送信する．M-SEARCH を受け取った各端末は ST（search type）ヘッダに記述されたサービスに適合するサービスを持っていた場合にはマルチキャストパケットの送信元アドレスと送信元ポートへと HTTPU[9] でレスポンスメッセージを送信する．現在は 30 秒毎に M-SEARCH パケットを送信するように設定している．図 2 に送信する M-SEARCH メッセージの例を示す．MAN（mandatory）ヘッダではこのメッセージが SSDP における発見のためのメッセージであることを示している．ST ヘッダでは，ssdp:all を指定し，検索対象が全てのサービスであることを表している．

M-SEARCH を送るときには，宛先を管理スコープのマルチキャストアドレス `239.255.255.250`，宛先ポートを SSDP の `1900`，送信元アドレスを自端末のアドレス，送信元ポートを `21400` として投げる．DLNA Probe から M-SEARCH を受け取った DLNA デバイスは，HTTPU でポート 21400 に対して HTTP レスポンスを送信する．DLNA Probe は RAW ソケットを介して 21400 で HTTP レスポンスを受け取ると，HTTP レスポンスパケットに含まれる送信元 IP アドレスと送信元 MAC アドレスを取得し，デバイス管理機構へ ADD コマンドを送る．たとえば，DLNA デバイスの IP アドレスが「`192.168.0.5`」，MAC アドレスが「`00:21:6B:72:A2:2C`」だった場合には「`ADD 192.168.0.5/00:21:6B:72:A2:2C`」を送信する．

受動的な発見では，SSDP のポート 1900 に送られてくる GENA の NOTIFY メッセージを監視することでデバイスの発見を行う．各 DLNA デバイスは定期的に NOTIFY メッセージをマルチキャストアドレス「`239.255.255.250`」，ポート「`1900`」に対してマルチキャストする．NOTIFY メッセージを RAW ソケットで受け取った DLNA Probe は NOTIFY メッセージの IP アドレスと MAC アドレスを取得する．NOTIFY メッセージの NTS（notify sub-type）フィールドが DLNA デバイスの離脱を意味する「`ssdp:byebye`」だった場合には，デバイス管理機構に対して DELETE コマンドを送信し，NTS フィールドがそれ以外（例えば「`ssdp:alive`」）だった場合には ADD コマンドを送信する．

3.3 ARP テーブル書換機構

ARP テーブル書換機構は，ARP スプーフィングを用いて，DLNA デバイスから送信されたパケットが全て DLNA Probe に送られるように ARP テーブルを書き換える．ARP スプーフィングは ARP を詐称して外部から端末の ARP テーブルを書き換える技術である．ARP テーブル書換機構は，デバイス管理機構より取得したデバイステーブルを基に全ての DLNA デバイスに対して ARP スプーフィングを行う．

図 3 に ARP スプーフィングの動作例として，DLNA Probe が端末 A の ARP テーブルを書き換えて，端末 B に対するパケットを DLNA Probe 宛てに変更する手順を示す．まず，端末 A の ARP テーブルには端末 B の IP アドレス「`192.168.0.2`」と MAC アドレス「`22:22:22:22:22:22`」が記録されている．1) この状態では端末 A が IP アドレス

Vol.2010-MBL-52 No.9
2010/1/29

```
M-SEARCH * HTTP/1.1
HOST: 239.255.255.250:1900
MAN: "ssdp:discover"
ST: ssdp:all
MX:3
```

図 2 M-SEARCH パケット

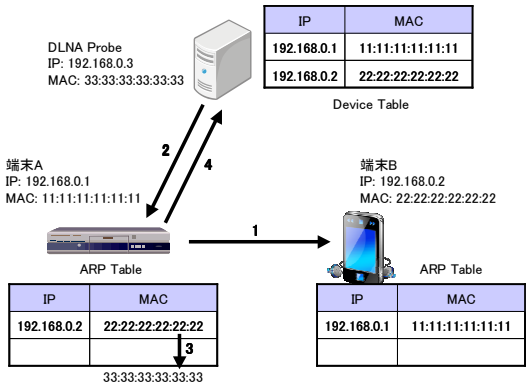

図 3 ARP スプーフィングの動作

「192.168.0.2」宛てにパケットを送信すると正しい宛先である端末 B がパケットを受信する．2) 次に DLNA Probe が送信元 IP アドレスが「192.168.0.2」，送信元 MAC アドレスが「33:33:33:33:33:33」の詐称した ARP パケットを端末 A に対して送信する．3) すると端末 A の ARP テーブルの「192.168.0.2」に対応付けられている MAC アドレスが「33:33:33:33:33:33」に書き換わる．4) その後，端末 A が端末 B の IP アドレス「192.168.0.2」に対してパケットを送ろうとすると詐称された宛先である DLNA Probe がパケットを受信する．

ARP スプーフィングには偽造した ARP リプライをブロードキャストする方法（ブロードキャスト ARP リプライ），偽造した ARP リクエストをブロードキャストする方法（ブロードキャスト ARP リクエスト），偽造した ARP リプライをユニキャストする方法（ユニキャスト ARP リプライ），偽造した ARP リクエストをユニキャストする方法（ユニキャスト ARP リクエスト）の 4 つが存在する．DLNA Probe で ARP スプーフィングを用いる場合，DLNA デバイスに悪影響を与えないこと，DLNA デバイス間の通信のみをモニタリングすることの 2 点を満たす必要がある．本研究は実環境に簡単に導入できることが目的であるため，ARP スプーフィングを用いることによって DLNA デバイスがサービス不能となるなどの悪影響は避けなければならない．また，ホームネットワークで発生するありとあらゆるトラフィックをモニタリングした場合，スループットの低下や遅延の増加などの副次的な問題が発生するため，DLNA デバイス間の通信のみをモニタリングする仕組みが求められる．

表 1 ARP スプーフィング手法の比較

	ブロードキャスト ARP リプライ	ブロードキャスト ARP リクエスト	ユニキャスト ARP リプライ	ユニキャスト ARP リクエスト
検出されにくさ	×	×	×	○
範囲	全端末	全端末	指定端末	指定端末
トラフィック量	△	△	○	×

表 1 に各 ARP スプーフィングの特徴を示す．ブロードキャスト ARP リプライやブロードキャスト ARP リクエストでは，乗っ取りたい IP アドレスが分かっていればブロードキャストを用いてサブネット内の全ての端末の ARP テーブルを書き換えることができる．しかしながら，これらの手法ではブロードキャストを用いるので IP アドレスを乗っ取られた端末が IP アドレスが乗っ取られたことを検出してしまう．たとえば Windows XP では，自分と同じ IP アドレスと自分と異なる MAC アドレスを含む ARP リクエストを受け取った場合にはユーザに IP アドレスが重複していることを通知し，ネットワークが切断される．また，本研究では DLNA デバイス間の通信だけをモニタリングする必要があるが，ブロードキャストを用いた手法では ARP を受け取った端末全ての ARP テーブルが書き換えられ，DLNA デバイス以外の端末が送信するパケットも全て DLNA Probe に送られてくるという問題が発生する．さらに，ブロードキャストを定期的に送る必要があるのでトラフィック量が多くなるという問題も発生する．

ユニキャスト ARP リプライでは，ARP リクエストに対応した形でパケットが送信される．そのため，ARP リクエストを監視して必要なときだけ偽造した ARP リプライを送ることができるので ARP スプーフィングに要するトラフィックを低く抑えることができる．偽造された ARP リプライを受け取った端末は ARP テーブルを ARP リプライの内容に応じて書き換える．しかしながら，ARP リクエストを送った端末は正しい端末からも ARP リプライを受け取るため，1 つの ARP リクエストに対して 2 つの ARP リプライを受け取ることになり，ネットワーク内に IP アドレスを乗っ取っている端末がいることを検出されてしまう．また，ARP リプライを送るタイミングによっては ARP テーブルを書きかえれない場合もある．

ユニキャスト ARP リクエストでは，ARP リクエストをユニキャストで送信した宛先の ARP テーブルのみを書き換えることができる．ユニキャスト ARP リクエストを用いた場合には，IP アドレスを乗っ取られた端末も，ユニキャスト ARP リクエストを受け取った

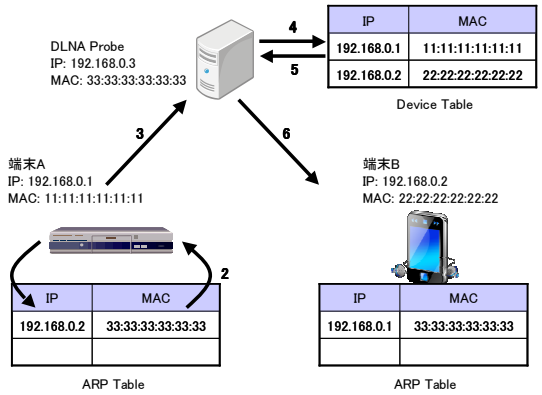

図 4 リダイレクト機構の動作

端末も，IP アドレスが乗っ取られたことを検出しない．一方でユニキャスト ARP リクエストを用いた場合には詐称した ARP リクエストを定期的に送る必要がある．さらに，一度のユニキャスト ARP リクエストでは 1 つの端末の ARP テーブルの 1 つの項目しか更新することができないので，N 台の DLNA 対応端末が存在した場合には $N \times N$ 個のユニキャスト ARP リクエストを送る必要があるのでトラフィックの量が多くなる．

本研究では，既存の DLNA デバイスに影響を与えない，DLNA デバイス間の通信のみを傍受可能という 2 点の特徴からユニキャスト ARP リクエストを ARP スプーフィングに用いる．ユニキャスト ARP リクエストでは DLNA デバイスの数が増えたときにトラフィック量が問題になるが，DLNA Probe は操作履歴取得のための過渡的な技術であること，現在のホームネットワークではせいぜい 10 台程度の DLNA デバイスしか存在しないことから問題とならないと想定している．

3.4 リダイレクト機構

ARP テーブル書換機構によって全ての DLNA デバイス間の通信は DLNA Probe へと送信される．リダイレクト機構では，受信したパケットの MAC アドレスを正しい MAC アドレスへと書き換えて送信することで正しい宛先へとリダイレクトする．

図 4 にリダイレクト機構の動作例を示す．まず，リダイレクト機構はデバイス管理機構よりデバイステーブルを取得する．デバイステーブルには端末 A と端末 B の IP アドレスと MAC アドレスが記録されている．まず，端末 A が IP アドレス 192.168.0.2 にパケットを送信する場合，1)ARP テーブルを参照して「192.168.0.2」に対応付けられている MAC アドレスを取得する．2)ARP テーブルは ARP テーブル書換機構によって書き換えられているため，取得される MAC アドレスは「33:33:33:33:33:33」となる．3) 次に端末 A は宛先 IP アドレスが「192.168.0.2」，宛先 MAC アドレスが DLNA Probe の MAC アドレス「33:33:33:33:33:33」，送信元 IP アドレスが端末 A の IP アドレス「192.168.0.1」，送信元 MAC アドレスが端末 A の MAC アドレス「11:11:11:11:11:11」でパケットを送信する．4) パケットを受け取った DLNA Probe は，デバイステーブルを参照して IP アドレス「192.168.0.2」を持つ端末の MAC アドレスを調べる．5) ここでは MAC アドレスとして「22:22:22:22:22:22」が得られる．6)DLNA Probe は得られた「22:22:22:22:22:22」を宛先 MAC アドレスに設定し，送信元 MAC アドレスを DLNA Probe の MAC アドレス「33:33:33:33:33:33」に書き換え，ネットワークに送信する．以上の手順で端末 A から送信されたパケットが DLNA Probe を経由して端末 B に到達する．

3.5 操作履歴取得機構

リダイレクト機構によってパケットをリダイレクトすると同時に，操作履歴取得機構がパケットの中身をチェックし，パケット中に DLNA デバイスの操作に関するメッセージが含まれていた場合にはそのメッセージをデータベースへと保存する．

パケットの中身をチェックする方式ではチェックにかかる計算コストと保存するログで消費するストレージ容量のトレードオフを考慮する必要がある．パケットの中身を全て閲覧する場合，閲覧のための計算コストが大きくなり，DLNA デバイス同士の通信に影響を与える．例えば，DLNA では一部に SOAP を用いてコマンドの送受信を行っているが，SOAP の解析を行うには計算コストの高い XML の構文分析を扱う必要がある．一方でパケットをチェックせずに全てのパケットをキャプチャして保存した場合には膨大な量のストレージを消費してしまう．

そこで DLNA Probe では，低い計算コストでパケットを処理するために，HTTP メッセージのリクエスト行に含まれるメソッドのみをチェックする．DLNA で扱うメソッドは，ファイルの取得が確認できる GET，コマンドの送信を確認できる POST，ファイルの送信が確認できる PUT の 3 種類のメッセージが存在する．パケットのデータフィールドの先頭が「GET，PUT，POST」のいずれかであった場合には，パケットの宛先アドレスがデバイステーブルに含まれるかどうかをチェックし，パケットのデータフィールドをデータベースに対して書き込む．データベースへは，送信元 IP アドレス，宛先 IP アドレス，メソッド名，メッセージが書き込まれる．HTTP リクエスト行は毎回パケットの同じ位置（TCP

データフィールドの先頭）に記述されており，メソッドは最大でも最も長い HTTP メソッド「POST」の 4 バイトのメモリ比較演算で実装可能である．

4. 初期的評価

DLNA Probe の初期的な評価として，DLNA Probe を用いた時に DLNA Probe のリダイレクト処理が通信遅延とスループットに与える影響の検証を行った．検証環境として，100Mbps のスイッチに DLNA デバイスを模した PC を接続して計測を行った．DLNA Probe は CPU が 2.26GHz のインテル Core2Duo プロセッサ P8400，メモリが 1GB の Lenovo X200 上で動作させた．

DLNA における著作権保護技術である DTCP-IP の要求遅延が 7ms 以下であるため[5]，DLNA Probe によって生じる遅延も 7ms 以下に抑える必要がある．遅延の評価は，ping を用いて DLNA Probe を用いた場合，用いない場合の RTT（往復遅延時間）の計測を行った．

図 5 にデバイス数に応じた平均遅延を示す．図 5 から分かるように，DLNA Probe を用いた場合では，平均で約 1ms の遅延が増加する．この 1ms の遅延は，DLNA Probe の処理遅延である．また，DLNA Probe を用いた場合では，デバイス数を増やすにつれて遅延が増加しており，デバイス数 100 台の時は 1.6ms の平均遅延が発生している．この遅延の増加は，ARP スプーフィングのトラフィックがデバイス数の増加によって増えていることに起因する．

DLNA では動画の転送などを行うため，DLNA Probe のリダイレクト処理や操作履歴取得処理によってスループットが著しく低下することは避けなければならない．スループットの評価は，A，B，C，D とラベル付けされた端末 4 台を用いて，netperf と iperf で計測を行った．端末 4 台の間の通信は全て DLNA Probe を経由する．A から B への通信は netperf を用いて TCP の実行スループットを計測し，C から D への通信は iperf を用いて一定の帯域の UDP トラフィックを流した．

図 6 にスループットの計測結果を示す．iperf の設定トラフィックが 50Mbps になるまでは C から D への通信は設定通りのスループットが観測されたが，A から B のスループットは C から D のトラフィックが増えるにしたがって減少した．iperf の設定トラフィックが 50Mbps を超えると A から B への実効スループット，C から D への実効スループットが共に 50Mbps 前後となった．全ての場合において A から B へのスループットと C から D へのスループットの合計が DLNA Probe が無い場合の最大スループットである約 94Mbps を超えることは無かった．これは，全てのトラフィックが DLNA Probe を経由するため，全てのスループットの合計が DLNA Probe が持つリンク速度に制限されること起因する．また，全てのスループットの合計は DLNA Probe が無い場合のスループットである約 94Mbps とほぼ同じであった．これは DLNA Probe の処理が DLNA デバイス間の通信のスループットに与える影響がほとんど無いことを意味している．

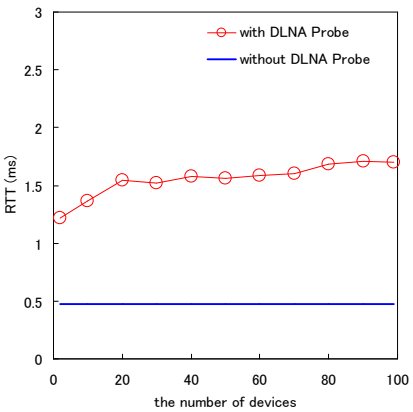

図 5 デバイス数に応じた平均遅延

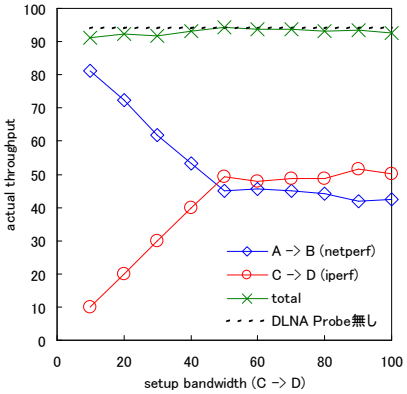

図 6 2 つのフローのスループット

5. おわりに

本稿では，DLNA デバイスの操作履歴を取得するソフトウェア，DLNA Probe の設計について述べた．現在，DLNA Probe の詳細な性能評価と，DLNA Probe を実環境に適用してユーザの行動情報の蓄積を行っている．

参考文献

1) Belimpasakis, P., Michael, M.P. and Moloney, S.: The Home as a Content Provider for Mash-ups with External Services, *Proceedings of the 6th IEEE Consumer Communications and Networking Conference (CCNC'09)*, Las Vegas, Nevada (2009).
2) Belimpasakis, P., Moloney, S., Stirbu, V. and Requena, J.C.: Home Media Atomizer: Remote Sharing of Home Content - without Semi-trusted Proxies, *IEEE Transactions on Consumer Electronics*, Vol.54, No.3, pp.1114–1122 (2008).
3) Cagenius, T., Fasbender, A., Hjelm, J., Horn, U., Ivars, I.M. and Selberg, N.: Evolving the TV experience: Anytime, anywhere, anydevice, *Ericsson Review*, No.3, pp.107–111

(2006).
4) Cohen, J. and Aggarwal, S.: General Event Notification Architecture Base, Internet Draft (1999).
5) Digital Transmission Licensing Administrator: *DTCP Volume 1 Supplement E Revision 1.2 (Informational Version)* (2007). http://www.dtcp.com/.
6) Digital Living Network Alliance, http://www.dlna.org/.
7) Gallego, I.L., Garcia, F.R., Valverde, J. M.P., Rizaldos, J.L. and Vidal, F.G.: DLNA-based IPTV Platform, *Proceedings of the 6th IEEE Consumer Communications and Networking Conference (CCNC'09)*, Las Vegas, Nevada (2009).
8) Goland, Y., Cai, T., Leach, P. and Gu, Y.: Simple Service Discovery Protocol, Internet Draft (2000).
9) Goland, Y.Y.: Multicast and Unicast UDP HTTP Messages, Internet Draft (1999).
10) Haruyama, T., Mizuno, S., Kawashima, M. and Mizuno, O.: Dial-to-Connect VPN System for Remote DLNA Communication, *Proceedings of the 5th Consumer Communications and Networking Conference (CCNC'08)*, Las Vegas, Nevada (2008).
11) Hwang, T., Park, H. and Chung, J.W.: Personal Mobile A/V Control Point for Home-to-Home Media Streaming, *Proceedings of the International Conference on Consumer Electronics (ICCE'08)*, Las Vegas, Nevada (2008).
12) Intille, S.S., Larson, K., Tapia, E.M., Beaudin, J.S., Kaushik, P., Nawyn, J. and Rockinson, R.: Using a Live-In Laboratory for Ubiquitous Computing Research, *Proceedings of 4th International Conference on Pervasive Computing (Pervasive'06)*, Dublin, Ireland (2006).
13) Jiang, X., Ly, M.V., Taneja, J., Dutta, P. and Culler, D.: Experiences with A High-Fidelity Wireless Building Energy Auditing Network, *Proceedings of the 7th ACM Conference on Embedded Networked Sensor Systems (SenSys'09)*, Berkeley, California (2009).
14) Kidd, C.D., Orr, R., Abowd, G.D., Atkeson, C.G., Essa, I.A., MacIntyre, B., Mynatt, E., Starner, T.E. and Newstetter, W.: The Aware Home: A Living Laboratory for Ubiquitous Computing Research, Proceedings of the 2nd International Workshop on Cooperative Buildings. Integrating Information, Organizations and Architecture (CoBuild '99), Pittsburgh, Pennsylvania, pp.191–198 (1999).
15) Kim, Y., Schmid, T., Charbiwala, Z.M., Friedman, J. and Srivastava, M.B.: NAWMS: Nonintrusive Autonomous Water Monitoring System, *Proceedings of the 6th ACM Conference on Embedded Networked Sensor Systems (SenSys'08)*, Raleigh, North Carolina, pp. 309–322 (2008).
16) Lee, H.Y. and Kim, J.W.: An Approach for Content Sharing among UPnP Devices in Different Home Networks, *IEEE Transactions on Consumer Electronics*, Vol.53, No.4, pp. 1419–1426 (2007).
17) Miyake, M., Yoshikawa, T. and Takeshita, A.: Technology for Controlling Access to Content between Different Home Networks, *NTT DOCOMO Technical Journal*, Vol.10, No.3, pp.37–43 (2008).
18) Motegi, S., Tasaka, K., Idoue, A. and Horiuchi, H.: Proposal on Wide Area DLNA Communication System, *Proceedings of the 5th Consumer Communications and Networking Conference (CCNC'08)*, Las Vegas, Nevada (2008).
19) Mozer, M.C.: The Neural Network House: An Environment that Adapts to its Inhabitants, *Proceedings of the American Association for Artificial Intelligence Spring Symposium*, Menlo Park, Canada, pp.110–114 (1998).
20) Oh, Y.J., Lee, H.K., Kim, J.T., Paik, E.H. and Park, K.R.: Design of an Extended Architecture for Sharing DLNA Compliant Home Media from Outside the Home, *IEEE Transactions on Consumer Electronics*, Vol.53, No.2, pp.542–647 (2007).
21) Olguin, D.O.: Sociometric Badges: Wearable Technology for Measuring Human Behavior, Master's thesis, Massachusetts Institute of Technology (2007).
22) Si, H., Saruwatari, S., Minami, M. and Morikawa, H.: A Ubiquitous Power Management System to Balance Energy Saving and Response Time based on Device-level Usage Prediction, *IPSJ Journal*, Vol.18 (2010). (To appear).
23) Song, T.Y., Kawahara, Y. and Asami, T.: Using SNS as Access Control Mechanism for DLNA Content Sharing System, *Proceedings of the 6th IEEE Consumer Communications and Networking Conference (CCNC'09)*, Las Vegas, Nevada, pp.1–2 (2009).
24) Tapia, E.M., Intille, S.S., Lopez, L. and Larson, K.: The Design of a Portable Kit of Wireless Sensors for Naturalistic Data Collection, *Proceedings of 4th International Conference on Pervasive Computing (Pervasive'06)*, Dublin, Ireland (2006).
25) UPnP Forum: *UPnP Device Architecture 1.0* (2003).
26) Venkitaraman, N.: Wide-Area Media Sharing with UPnP/DLNA, *Proceedings of the 5th Consumer Communications and Networking Conference (CCNC'08)*, Las Vegas, Nevada, pp.294–298 (2008).
27) Wu, S.C., Ku, Y.C. and Lee, T.L.: Zero-Configuration Personal Firewall for DLNA DMS, *Proceedings of the IEEE Asia-Pacific Services Computing Conference (APSCC'08)*, Yilan, Taiwan, pp.847–850 (2008).
28) Yamazaki, T.: Ubiquitous Home: Real-life Testbed for Home Context-aware Service, *Proceedings of the 1st International Conference on Testbeds and Research Infrastructures for the Development of Networks and Communities (Tridentcom'05)*, Trento, Italy, pp.54–59 (2005).
29) Zancanaro, M., Kuflik, T., Boger, Z., Goren-Bar, D. and Goldwasser, D.: Analyzing Museum Visitors' Behavior Patterns, *Proceedings of the 11th international conference on User Modeling (UM'07)*, Corfu, Greece, pp.238–246 (2007).
30) 鈴木秀和，渡邊　晃：NAT-f を用いたホームネットワーク間相互接続方式の検討，情報処理学会マルチメディア, 分散, 協調とモバイル (DICOMO) シンポジウム，pp.1675–1682 (2008).
31) 小山卓視，呉　敬源，武藤大悟，吉永　努：Mobile-Wormhole Device: DLNA 情報家電の相互遠隔接続支援機構の携帯端末への応用，情報処理学会研究報告, MBL，pp.1–8 (2008).
32) 矢野和男：センサは Web を超える：省力化から知覚化へ，情報処理，Vol.48, No.2, pp.160–170 (2007).