Home Networks: Topology Discovery and Characterization of Traffic Dynamics

Frank den Hartog

Presentation at CAIA, Swinburne University
1 March 2012
• Frank den Hartog

• Senior Scientist Future Internet and Heterogeneous Consumer Networks at TNO
• Deputy chair of the Technical Working Group of the worldwide HGI.
• Project editor of the 2009-2011 CENELEC SmartHouse Roadmap project.
• Studies everything related to interoperability in and with private networks.
• Pioneered the home networking field at the Dutch incumbent operator KPN between 1998 and 2002.
• Published 70 technical articles and reports, 5 patents and over 40 contributions to standardization (in particular to HGI, OMA, Broadband Forum and ITU-T SG 16 FS-VDSL).
• http://sites.google.com/site/frankdenhartog
Agenda

- Managerial complexity in home networks
- Home network topology discovery for service providers
- Available bandwidth probing
- Home network traffic characterization
1994: monolithic systems in the home
1999: monolitic systems in the home, until...
>2011: trans-sector convergence?
Managerial complexity for the consumer: examples

- Increasing clutter of devices and networks in the home
- My content is everywhere, but where?
  - Desktop, NAS, laptop (which one?), cloud, ipod, car, ...
- I need to think about which phone to use?
  - Fixed, mobile, skype, ...
- I can’t print on my home network printer after I set up a VPN connection to my work
- I love Apple stuff, but they still do not sell every type of communicating device I need (such as an Apple Smart Meter)
- Why can’t I get a home contents insurance if my burglary alarm works on IP?
- Why can’t my set-top box from service provider XYZ not also play content from my NAS? Or be used by my tele-care provider also?
- Usernames, passwords, PINs, ...
Managerial complexity for the service provider….

43% of service provider help desk calls is home network related
Work partly done in the EU FP7 project FIGARO

Future Internet Gateway-based Architecture of Residential networks

2010-2013

Partners: Technicolor, Philips, Telefonica, TNO, University of Life, Eurecom, University of Waterloo, Martel

Total size: €8 mln
(of which €1 mln by TNO)

www.ict-figaro.eu
The issue: Take for instance the following use case...

- Service providers currently do not have any clue what the statics (topology) and the dynamics (traffic) are in the home network.
- Thus no clue what will happen with their IPTV stream.
- Just prioritizing IPTV in the residential gateways does not guarantee anything.
- And does the user want IPTV always having the highest priority?
- And expecting all devices in the home nicely doing diffserv, 802.11e, DLNA QoS, etc. is not yet realistic.
- This is a real-life problem, addressed in HGI (19 operators).
What about using existing monitoring methods? Well, ...

- Maybe the most obvious approach would be to have the residential gateway first do some serious device discovery…
  - Using UPnP, DHCP, SIP, ARP, TR-069, etc.
- And then do some link layer topology discovery…
  - Using LLTD, 802.1ab, G.hntd, …
  - Which need implementation on the end devices and bridges in the home
- And then do some link layer throughput estimation…
  - Lots of probing techniques available for this!
- And then some intelligent mixing and matching (“algorithm”) of the obtained values…
- And then you may still miss the information about the path that you are actually interested in
  - Even though the procedure is already very complex and gives you also lots of information that you do not need.
Overview of TNO research on home network diagnostics

› Home network topology discovery
  › Erik German Diaz Castellanos et al, Proc. of 9\textsuperscript{th} IEEE CCNC 2012, Las Vegas.

› Available bandwidth monitoring
  › Connected Home Global Summit 2011 \textit{Industry Award} for "Best Innovation in Software Modularity and Applications for Home Gateways".
Agenda

- Managerial complexity in home networks
- Home network topology discovery for service providers
- Available bandwidth probing
- Home network traffic characterization
Topology discovery: state of the art

- Use MAC Address Forwarding Tables (AFTs) and Spanning Tree Protocol (STP)
  - Needs management protocol (e.g. SNMP) to read out tables and needs heavy algorithms to obtain topology
- IEEE 802.1AB (LLDP) is developed for heterogeneous LANs and puts lesser requirements on the algorithms
- Microsoft’s LLTD also for heterogeneous LANs and puts lesser requirements on HNIDs than LLDP (but is proprietary)
- ITU-T is working on Home network Topology Identifying Protocol (HTIP) in G.phnt group
  - Based on a modified version of LLDP and UPnP, but without SNMP
  - But this technology is still under development
LLDP vs LLTD

HNID: Home Network Infrastructure Device
MIB: Management Information Base
NMS: Network Management System
LLDP: Link Layer Discovery Protocol
LLTD: Link Layer Topology Discovery

LLDP

- Devices advertise their presence
- HNID stores neighbors’ information in a MIB
- NMS gets MIBs information using SNMP
- NMS generates map

LLTD

- MAPPER finds RESPONDERS
- MAPPER injects LLTD frames into the network
- MAPPER finds HNID
- MAPPER generates map
HGI requirements for topology discovery

• **Requirement 1**: The accuracy must be close to 100%, i.e. the obtained map must contain a negligible amount of mistakes.

• **Requirement 2**: The time between requesting a topology map and obtaining it must be less than 2 seconds.

• **Requirement 3**: The overhead traffic that the topology discovery procedure creates and the memory resources it confiscates must not disturb other services in the home.

• **Requirement 4**: The architecture should not depend on proprietary and IPR restricted standards or protocols, unless it is within the span of control of HGI.
We therefore decided on the following KPIs:

- **Discovery time**
  - Time between requesting a topology map and obtaining it

- **Average injected traffic rate**
  - Rate averaged over a relatively long period of time.

- **Required memory resources**
  - Total memory resources required for each protocol.

- **Accuracy**
LLTD and LLDP try to relate an unknown device to one type of device (SW, AP, HP, STA) based on its behavior or advertised information…….

The result of the match could be positive (P) or negative (N).

$$\text{Acc}_{class} = \frac{\#TP + \#TN}{\#P + \#N}$$
A ROC graph is a two dimensional graph that represents relative trade-offs between true positive rates (TPR) and false positive rates (FPR).

$$TPR = \frac{\#TP}{\#P}$$

$$FPR = \frac{\#FP}{\#N}$$

Classifier A is equally good or better than a classifier B if:

$$TPR_A \geq TPR_B \land FPR_A \leq FPR_B$$
Graph Accuracy

Network topology can be represented as an undirected graph, which can be represented as an adjacency matrix.

We compare adjacency matrices from original topology and from final map.
Test bed implementation: HG

Home Gateway:
The home gateway supporting the protocols under study is constructed from the following devices:

1. Linksys WRT54GL router as DHCP server
2. Dell Netbook LATITUDE 2100 with
   - Windows Vista supporting LLTD mapper
   - Network Management System (NMS, Solarwinds engineer's toolset)
   - Wireshark protocol analyzer
3. CISCO switch SF-300-08 (supporting LLDP)
Test bed basic configurations

Configuration Eth

Configuration SW

Configuration PLC

Configuration WL

SW Switch
AP Access Point
HP Home Plug
HG Home Gateway

Ethernet
Power Line

Wireless
Station / End Device
# Test bed implementation

<table>
<thead>
<tr>
<th>Device</th>
<th>Type</th>
<th>LLDP agent</th>
<th>LLTD</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Tx mode</td>
<td>Rx mode</td>
</tr>
<tr>
<td>HG</td>
<td>HG</td>
<td>No</td>
<td>yes</td>
</tr>
<tr>
<td>Station</td>
<td>End-device</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>Access Point</td>
<td>HNID</td>
<td>Yes</td>
<td>no</td>
</tr>
<tr>
<td>Switch</td>
<td>HNID</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Home Plug</td>
<td>HNID</td>
<td>no</td>
<td>no</td>
</tr>
</tbody>
</table>
Example of obtained LLTD maps

- **HPs represented as Eth Switches**
- **Configuration PLC**
Classification Accuracy results

<table>
<thead>
<tr>
<th></th>
<th>LLTD</th>
<th>LLDP</th>
</tr>
</thead>
<tbody>
<tr>
<td># TP</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td># TN</td>
<td>20</td>
<td>15</td>
</tr>
<tr>
<td># FP</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td># FN</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td># P</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td># N</td>
<td>24</td>
<td>17</td>
</tr>
<tr>
<td>$Acc_{class}$</td>
<td>82%</td>
<td>90%</td>
</tr>
</tbody>
</table>
### Graph Accuracy results

<table>
<thead>
<tr>
<th>Config.</th>
<th>#STAs</th>
<th>LLTD</th>
<th>LLDP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth</td>
<td>1</td>
<td>100%</td>
<td>100%</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>100%</td>
<td>100%</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>100%</td>
<td>100%</td>
</tr>
<tr>
<td>SW</td>
<td>1</td>
<td>100%</td>
<td>100%</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>100%</td>
<td>100%</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>100%</td>
<td>100%</td>
</tr>
<tr>
<td>PLC</td>
<td>1</td>
<td>63%</td>
<td>50%</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>72%</td>
<td>56%</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>83%</td>
<td>59%</td>
</tr>
<tr>
<td>WL</td>
<td>1</td>
<td>100%</td>
<td>78%</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>100%</td>
<td>75%</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>100%</td>
<td>76%</td>
</tr>
</tbody>
</table>
Topology discovery time

- LLTD Config Eth
- LLTD Config SW
- LLTD Config PLC
- LLTD Config WL
- LLDP Config Eth
- LLDP Config SW
- LLDP Config PLC
- LLDP Config WL

Time (s)

Number of Stations
Do LLTD and LLDP fulfill HGI’s requirements?

• **Requirement 1**: The time between requesting a topology map and obtaining it must be less than 2 seconds.

• **Requirement 2**: The accuracy must be close to 100%, i.e. the obtained map must contain a negligible amount of mistakes.

• **Requirement 3**: The overhead traffic that the topology discovery procedure creates and the memory resources it confiscates must not disturb other services in the home.

• **Requirement 4**: The architecture should not depend on proprietary and IPR restricted standards or protocols, unless it is within the span of control of HGI.

<table>
<thead>
<tr>
<th></th>
<th>Req 1</th>
<th>Req 2</th>
<th>Req 3</th>
<th>Req 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>LLTD</td>
<td>–</td>
<td>0</td>
<td>+</td>
<td>–</td>
</tr>
<tr>
<td>LLDP</td>
<td>–</td>
<td>0</td>
<td>+</td>
<td>+</td>
</tr>
</tbody>
</table>
Agenda

- Managerial complexity in home networks
- Home network topology discovery for service providers
- Available bandwidth probing
- Home network traffic characterization
So… let’s probe e2e on the UDP/IP layer!

› Advantages:
  › No need for device discovery or topology discovery
  › You already know whom you want to probe and don’t care about devices in between
  › Closer to the actual application
  › Also works with future link layer technologies

› Requirements:
  1. Easy to implement (server-side, i.e. only on the RG or in the cloud)
  2. Non-intrusive (should not disturb existing traffic)
  3. Fast convergence (in the order of seconds)
  4. As less pre-adaptation/pre-knowledge as possible (no knowledge of link layer topology needed)
  5. Accurate (1 Mbps for IPTV, 50 Kbps for VoIP)
Woops… no existing E2E IP probing tool satisfies

<table>
<thead>
<tr>
<th></th>
<th>Sender-based (req.1)</th>
<th>Technique type (req.2)</th>
<th>Convergence rate (req.3,5)</th>
<th>Designed for wireless (req.4,5)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pathload</td>
<td>N</td>
<td>PRM</td>
<td>Iterative</td>
<td>N</td>
</tr>
<tr>
<td>Pathchirp</td>
<td>N</td>
<td>PRM</td>
<td>Iterative</td>
<td>N</td>
</tr>
<tr>
<td>PTR</td>
<td>N</td>
<td>PRM</td>
<td>Iterative</td>
<td>N</td>
</tr>
<tr>
<td>DietTOPP</td>
<td>N</td>
<td>PRM</td>
<td>Iterative</td>
<td>Y</td>
</tr>
<tr>
<td>IGI</td>
<td>N</td>
<td>PGM</td>
<td>Direct</td>
<td>N</td>
</tr>
<tr>
<td>WBest</td>
<td>N</td>
<td>PGM</td>
<td>Direct</td>
<td>Y</td>
</tr>
<tr>
<td>Capprobe</td>
<td>N</td>
<td>PGM</td>
<td>Direct</td>
<td>Y</td>
</tr>
</tbody>
</table>

Especially probing devices currently available in the market seems tough
Histogram of probe delay

- Wifi random back-off
- delay caused by crossing traffic etc.

min[RTT]

RTT small probe (micro seconds)

Number of occurrence
Packet-pair probing: yields the e2e capacity...

\[ C = \frac{L}{\min_{i} (\Delta t_{out,i})} \]

- In round-trip with UDP: reply packets are too small to be further dispersed
- In round-trip with ping: reply packets have size L. Combining with UDP measurement yields forward and backward C separately
... but not in wireless!

- due to the 2nd probe packet contending with the 1st reply packet...
- REP2 will arrive late -> larger measured dispersion -> underestimation of capacity
So instead of 2 packets b2b... we send 1 packet of size 2xMTU!

Mind you: in a one-way measurement one must measure the minimum dispersion of two consecutive packets, because the devices do not have synchronized clocks

In round-trip that is not needed anymore!
Some formulas...

Path (e2e) capacity is now calculated like this:

\[ C = \frac{L}{\min_{i=1...n} \left[ RTT_2(i) \right] - \min_{i=1...n} \left[ RTT_1(i) \right]} \]

Instead of this:

\[ C = \frac{L}{\min_{i=1...n} \left[ RTT_2(i) - RTT_1(i) \right]} \]

Available bandwidth is calculated like this:

\[ A = \frac{L}{\left( \frac{L}{C} + \overline{d_r} \right)} \]

With \( \overline{d_r} \) the average delay of a packet caused by random effects (crossing traffic, interference, ...):

\[ \overline{d_r} = \text{avg} \left[ RTT_1(i) \right] - \min_{i=1...n} \left[ RTT_1(i) \right] \]

Yielding for the available bandwidth:

\[ A = \frac{L}{\min_{i=1...n} \left[ RTT_2(i) \right] + \text{avg} \left[ RTT_1(i) \right] - 2 \min_{i=1...n} \left[ RTT_1(i) \right]} \]
### Results for Wifi-g

<table>
<thead>
<tr>
<th>Crossing traffic $X$</th>
<th>$A$ (Iperf)</th>
<th>$A(X=0)-X$ (Iperf)</th>
<th>$A$ (Wbest)</th>
<th>$A(X=0)-X$ (Wbest)</th>
<th>$A$ (Allbest)</th>
<th>$A(X=0)-X$ (Allbest)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>32±3</td>
<td>32±3</td>
<td>20±4</td>
<td>20±4</td>
<td>30±1</td>
<td>30±1</td>
</tr>
<tr>
<td>6</td>
<td>26±5</td>
<td>26±3</td>
<td>14±4</td>
<td>14±4</td>
<td>23±1</td>
<td>24±1</td>
</tr>
<tr>
<td>11</td>
<td>17±4</td>
<td>21±3</td>
<td>8±4</td>
<td>9±4</td>
<td>19±1</td>
<td>19±1</td>
</tr>
<tr>
<td>6 (cont)</td>
<td>20±8</td>
<td>26±3</td>
<td>14±5</td>
<td>14±4</td>
<td>21±1</td>
<td>24±1</td>
</tr>
</tbody>
</table>

- $C = 38$ Mbit/s.
- $A(X=0)$ must be > 26 Mbit/s (depending on how many packets actually undergo random backoff). Wbest underestimates $A(X=0)$, but the effect of crossing traffic $X>0$ is quite well measured.
- Iperf underestimates $A$ slightly (given $A(X=0)-X$)
- Standard deviations in Allbest really low
- Allbest shows clear supremacy here
And this is just the beginning!

- Other link layer technologies (HomePlug, Zigbee, Wifi-n, …)
  - We have assumed that the link layer works more or less ethernet-like
- Other performance indicators
- Other queuing mechanisms
- Higher accuracies (VoIP)
- Bring to standardization (HGI, Broadband Forum, UPnP Forum, …)
- Etc. Etc.

But a really tricky one is the following: How does the residential gateway know the accuracy of the result after a probing session?

- Needs to know that to make a proper decision what to do with the IPTV stream in waiting

And then: how is the decision made, and how frequent should one repeat the probing sessions?

- Needs characterization of the dynamics of traffic in home networks
- We did that, submitted to ACM SIGCOMM
- It’s not the same as in the Internet!
Agenda

- Managerial complexity in home networks
- Home network topology discovery for service providers
- Available bandwidth probing
- Home network traffic characterization
proposal

› measure $A$ every 500 s (1-2)
› predict how dynamic the home network traffic will be for the coming 500 s (3-4)
› For this we need an empirical model
› Correct the measured $A$ accordingly (5)
› Compare the results to the required $A$
› Make a decision (6-7)
### Home Network traffic measurement campaign in 15 Dutch households (1)

<table>
<thead>
<tr>
<th>Profile Parameter</th>
<th>Type</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>House</td>
<td>Regular houses (i.e. adjacent, 3-floor houses). Apartments. Suburb house.</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Network type</td>
<td>Cable-based broadband connection. ADSL subscribers broadband connection.</td>
<td>2 households</td>
</tr>
<tr>
<td></td>
<td>Ethernet, Wireless LAN. Ethernet, Wireless LAN, and Powerline.</td>
<td>13 households</td>
</tr>
<tr>
<td>Average number of network devices per household</td>
<td>Laptop or PC. Multimedia servers e.g. Network Attached Storage, IPTV Set-Top-Box, Web server. Personal handheld device e.g. PDA, Smartphone, or Internet tablet. Game console. Others.</td>
<td>4.6</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0.7</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.0</td>
</tr>
<tr>
<td>User</td>
<td>Families with children (professional). Families without children (student, professional).</td>
<td>12 houses</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3 houses</td>
</tr>
<tr>
<td></td>
<td>The average number of users per house.</td>
<td>3 persons</td>
</tr>
<tr>
<td></td>
<td>The average daily time spent on network applications.</td>
<td>4 hours</td>
</tr>
</tbody>
</table>
Home Network traffic measurement campaign in 15 Dutch households (2)
In-home traffic was recorded by replacing peoples HGs with a WRT-54GL and a PRTG traffic recorder 1 week, every 10 s.
Measured traffic rates follow a pareto distribution
Application session time $d$ is the time between jumps in $x$ larger than 250 kbit/s. Average $d = 500$ s.

$$pmf(d) \approx gpf(d|\xi, \sigma, \theta) = \left(\frac{1}{\sigma}\right) \left(1 + \frac{\xi}{\sigma} \cdot \frac{d - \theta}{\sigma}\right)^{-\frac{1}{\xi}}$$

$$= gpf(d|\xi = 0.92, \sigma = 3.98 s, \theta = 0 s)$$
A measure of the dynamics of home networking traffic is given by the entropy of $x$ over 500 s

$$h(m) = - \sum_{x \in S(m)} [Pmf(x) \cdot \log(Pmf(x))]$$
We found that the home network traffic dynamics can be well represented by a 4-state continuous-time Markov chain.

- $z_1 =$ normalized entropies between 0 and 0.4
- $z_2 =$ normalized entropies between 0.4 and 0.6
- $z_3 =$ normalized entropies between 0.6 and 0.8
- $z_4 =$ normalized entropies between 0.8 and 1

**Transition Matrix:**

$$M = \begin{bmatrix}
0.95 & 0.04 & 0.01 & 0 \\
0.2 & 0.5 & 0.2 & 0.1 \\
0.1 & 0.2 & 0.5 & 0.2 \\
0 & 0 & 0.1 & 0.9 \\
\end{bmatrix}$$

**Stationary Distribution:**

$$\pi = \{0.61, 0.1, 0.08, 0.21\}$$
How valid is the model if it is based on measurement is “only” 15 households? 
For this we adapted the LOOCV method to make it applicable to stochastic models. 
With the current model, states are predicted with a 70% precision (whereas 85% is the theoretical maximum).
Conclusions

- Service providers need home network monitoring tools
- Current home network topology discovery protocols are not good enough
- TNO developed an “award-winning” e2e IP-path available bandwidth monitoring tool for which pre-knowledge about the topology is not needed. It only needs adaptation of the home gateway.
- Bandwidth probing only needs to happen every ~500 s
- For IPTV admission control we developed an empirical model which can be used to predict the activity (traffic dynamics) on the home network for the next 500 s (and beyond)
- The model is built upon measurements in 15 households and has an accuracy of 70%
- To obtain this accuracy we had to adapt the LOOCV method