Research Roadmap Driven by Network Benchmarking Lab (NBL): Deep Packet Inspection, Traffic Forensics, Embedded Benchmarking, WLAN/LTE, and Beyond
Areas of research interests
- Deep Packet Inspection
  - Attack, virus, spam, porno, P2P
  - Software, algorithm, hardware, SoC
  - Real traffic, beta site, botnet
- Internet security and QoS
- Wireless communications
- Test technologies of switch, router, WLAN, security, VoIP, 4G/LTE and embedded systems

Publications
- International journal: 94
- International conference: 50
- IETF Internet Draft: 1
- Industrial articles: 153
- Patents: 26
- Tech transfers: 8
- Well-cited paper: Multihop Cellular: A New Architecture for Wireless Communications, INFOCOM 2000, YD Lin and YC Hsu; #citations: 600; standardized into IEEE 802.11s, Bluetooth, WiMAX, and LTE
1. From development to research
2. System research with three side products
   - NBL, L7 Networks Inc., textbook
3. The blue track – product development
   - Development plane: L7 Networks Inc., textbook
   - Research plane: QoS, DPI (deep packet inspection)
4. The green track – product testing
   - Development plane: NBL, EBL, BML
   - Research plane: traffic forensics, embedded benchmarking
5. Lessons
From Development to Research

- Sources of research topics
  1. Literature repository: minor improvement on existing or pseudo problems
  2. Development projects: feasible solutions on real problems
  3. Industrial discussions: real problems but not necessarily feasible solutions

- D(development) → R(research)
  - Enabling resource: Linux
  - Research is the non-trivial part within the development process.
  - If I don’t know how to develop it, I would not research on it.

System Research with Three Side Products

- Linux QoS Router Development
- Security Gateway
- 7-in-1 Security Gateway
- L7 Inc. Startup
- Computer Networks: An Open Source Approach
- Network Benchmarking Lab (NBL)
- QoS
- Deep Packet Inspection
- RealFlow
- Embedded Benchmarking Lab (EBL)
- 4G LTE
- Traffic Forensics
- Embedded Benchmarking & 4G LTE
- Cable TV Networks
- Multi-hop Cellular
- Public Testing with a Magazine
- Network Benchmarking Lab (NBL)
- Development Plane
- Research Plane
Development Plane:
L7 Networks Inc.
Computer Networks: An Open Source Approach
Research Plane:
QoS
Deep Packet Inspection (DPI)

THE BLUE TRACK
7-in-1 System Prototyping and Benchmarking

- 7-in-1: VPN, Firewall, NAT, Routing, Content Filtering, Intrusion Detection, Bandwidth Management
- Launched a startup in 2002: L7 Networks Inc.
4-in-1 Proxy Architecture
Reducing IPC and Restructuring Modules

- Boosted Web throughput by 200% and mail throughput by 500%
Profiling String Matching Algorithms on Large Problem Size

- First profiled result for string matching algorithms on large problem size
- Appeared in IEEE Comm. Surveys & Tutorials, 2nd quarter, 2006;

![Diagram showing profiling results for different string matching algorithms and patterns](image)
Revisiting String Matching with Recent Developments on DPI

- Comprehensive review of string matching algorithms and realizations for DPI

Summary of string matching methods for DPI (underlines mean hardware-based)

<table>
<thead>
<tr>
<th>Automaton-based</th>
<th>Heuristic-based</th>
<th>Filtering-based</th>
</tr>
</thead>
<tbody>
<tr>
<td>rewrite and group regular expressions</td>
<td>get shift distance using heuristics based on the automaton that recognizes the reverse prefixes of a regular expression (RegularBNDM)</td>
<td>extract necessary substrings from regular expressions and filter the text with them (MultiFactRE)</td>
</tr>
<tr>
<td>reduce number of transitions (D²FA)</td>
<td>get shift distance from a fixed block in the suffix of search window (Wu-Manber)</td>
<td>filter with a set of Bloom filters for different pattern lengths</td>
</tr>
<tr>
<td>hardwire regular expressions on FPGA</td>
<td>get shift distance from the longest suffix of search window (BG)</td>
<td>filter with a set of hash functions sequentially in a Bloom filter (Hash-AV)</td>
</tr>
<tr>
<td>track a DFA that accepts the patterns (Aho-Corasick)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>reduce sparse transition table (Bitmap-AC, BNFA in Snort)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>reduce fan-out from the states (split automata)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>track multiple characters at a time in an NFA (JACK-NFA)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Traversing Aho Corasic State Machine: Hardware Acceleration on Root and Non-Root States

- New Parallel Architecture with Pre-Hashing and Root-Indexing
- 10Gbps on large pattern set with Xilinx ML310 SoC platform
- Appeared in ACM Transactions on Embedded Computing Systems, Apr 2009
BFAST: Bloom Filter Accelerated Sub-linear Time architecture

- Sub-linear with bounded worst-case performance
- Appeared in IEEE Transactions on VLSI Systems, Aug 2009

Patterns:
- \( P_1 = \text{abcdefgh} \)
- \( P_2 = \text{ijklmnop} \)
- \( P_3 = \text{zyxwvuts} \)

Grouping:
- \( G_0 = \{\text{efgh, mnop, vuts}\} \)
- \( G_1 = \{\text{defg, lmno, wvut}\} \)
- \( G_2 = \{\text{cdef, klmn, xwvu}\} \)
- \( G_3 = \{\text{bcde, jklm, yxwv}\} \)
- \( G_4 = \{\text{abcd, ijkl, zyxw}\} \)
- \( G_5 = \{\text{abc, ijk, zyx}\} \)
- \( G_6 = \{\text{ab, ij, zy}\} \)
- \( G_7 = \{\text{a, i, z}\} \)

The search window can be shifted by 2 characters.

\[ \text{text} \]

\[ \text{uvwxyzabcdef} \]

\[ m=8 \]

\[ \text{search window} \]
Multi-core Design of a Scalable String Matching Algorithm
Appeared in IEEE Transactions on Computers, Apr 2011

Best shift distance:
1. B is not a factor of any $\Gamma_i \in \Gamma$.
   - No suffix of B is a prefix of any $\Gamma_i \in \Gamma$.
   - One suffix of B is a prefix of some $\Gamma_i \in \Gamma$.
     Let $k$ be the maximum length of such a suffix. $\text{SHIFT}[h(B)] = l_{\text{min}} - k$.

2. B is a factor of some $\Gamma_i \in \Gamma$.
   - Let $l$ be the rightmost occurrence of B.
     $\text{SHIFT}[h(B)] = l_{\text{min}} - l$.
   - Verify if $\text{SHIFT}[h(B)] = 0$

Observation in virus signature set:
- A large number of long signatures plus a small number of short signatures
- Either curbing long shift (if BH only) or needing a huge data structure (if AC only)

Solutions:
- Long signatures for BH
  - The shift window can skip fast
- Short signatures for AC
  - A small data structure

Running in a multi-core design
Hardware Software Co-design for DPI

- Experimenting (1) pure Linux software, (2) Linux + HW, (3) Linux + HW /w less copy, (4) pure HW

Time of writing data into TextRAM occupies about 90% of matcher-bfast*.

### Time distribution when ClamAV transfer data into TextRam

- **user space to kernel space** (21%)
- **copy data to DMA buffer** (66%)
- **DMA transfer data into TextRam** (13%)
Computer Networks: An Open Source Approach considers why a protocol, designed a specific way, is more important than how a protocol works. Key concepts and underlying principles are conveyed while explaining protocol behaviors. To further bridge the long-existing gap between design and implementation, it illustrates where and how protocol designs are implemented in Linux-based systems. A comprehensive set of fifty-six live open source implementations spanning across hardware (8B/10B, OFDM, CRC32, CSMA/CD, and crypto), driver (Ethernet and PPP), kernel (longest prefix matching, checksum, NAT, TCP traffic control, socket, shaper, scheduler, firewall, and VPN), and daemon (RIP/OSPF/BGP, DNS, FTP, SMTP/POP3/IMAP4, HTTP, SNMP, SIP, streaming, and P2P) are interleaved with the text.
Key Features of the Book

- Logically reasoned *why*, *where*, and *how* of protocol designs and implementations.
- Fifty-six explicitly numbered open source implementations for key protocols and mechanisms.
- Four appendices on Internet and open source communities, Linux kernel overview, development tools, and network utilities.
- “A Packet’s Life” to illustrate the book roadmap and packet flows.
- Sixty-nine sidebars of Historical Evolution (33), Principle in Action (26), and Performance Matters (10).
- End-of-chapter FAQs and “Common Pitfalls.”
- Class support materials including PowerPoint lecture slides and solutions manual available via the textbook website [www.mhhe.com/lin](http://www.mhhe.com/lin).
Quotes from Reviewers:

• “The exposure to real life implementation details in this book is phenomenal... Definitely one of the better books written in the area of Computer Networks.” – Mahasweta Sarkar, San Diego State University

• “I have never seen a book giving such details on explaining the design and implementation of such practical systems...Those open source implementations are excellent demonstrations for practical networking systems.” – Fang Liu, University of Texas-Pan American

• “This is a solid textbook with strong emphasis on technical (implementation) details of computer network protocols.” – Oge Marques, Florida Atlantic University

• “Written by RFC and open source contributors, this book definitely is an authentic guide for network engineers.” – Wen Chen, Cisco Fellow

• “Interleaving designs and implementations into the same book bridges the long-existing gap and makes this an ideal text to teach from.” – Mario Gerla, University of California, Los Angeles

• “The sidebars of Historical Evolution and Principle in Action make the reading more enjoyable, while Performance Matters treat computer networking quantitatively.” – H. T. Kung, Harvard University
Final Comments on the Book

• The first attempt
  ◆ Interleaved vs. separated
  ◆ Live running codes in daily usage

• Follow-up on other courses?
  ◆ Algorithms
  ◆ Operating systems
  ◆ Computer organizations
Development Plane:
  Network Benchmarking Lab (NBL)
  Embedded Benchmarking Lab (EBL)
  Broadband Mobile Lab (BML): 4G LTE
Research Plane:
  Traffic Forensics
  Embedded Benchmarking & 4G LTE

THE GREEN TRACK
Pre-NBL: Public Benchmarking

- Benchmarking, Workshop, and Publishing

2004
Wireless LAN SOHO Router
VoIP

2003
Network Security
IPv6 Router
LAN L2/L3 Switch
Backbone Switch/Router

2002
E-Commerce
WLAN
Security Gateway
Content Delivery Network

2001
Security Gateway
Bandwidth Management
Web Switch
QoS

2005
VoIP Plugfest
Network/Content Security

2006
Intrusion Detection Systems
10GbE Ethernet Switch
VoWLAN

2007
P2P Friendly Properties of NAT
Wireless SIP Residential Gateways

2009
SOHO under RealFlow
NBL Funding and Features

- Founded in May 2002

- Funding sources
  - Industry for test services and tools
  - Government seed money

- Features
  - A real-world traffic test lab (from 2007)
  - A developer for test tools
  - Providing SPEC Verification & RealFlow Certification
  - Experienced in benchmarking products
### NBL Staff

- Advisory Committee
- Director + 20 full-time + 15 students
- Operation model: 3-line

<table>
<thead>
<tr>
<th>Type</th>
<th>Analog</th>
<th>Who</th>
<th>Mission</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test Service</td>
<td>Infantry</td>
<td>Mostly full-time</td>
<td>1. Conducting tests</td>
</tr>
<tr>
<td>(1st line)</td>
<td></td>
<td>Some students</td>
<td>2. Writing test plans</td>
</tr>
<tr>
<td>Test Tool</td>
<td>Artillery</td>
<td>Some full-time</td>
<td>1. Developing test tools</td>
</tr>
<tr>
<td>(2nd line)</td>
<td></td>
<td>Mostly students</td>
<td>2. Licensing tools to vendors</td>
</tr>
<tr>
<td>Test Research</td>
<td>Supply</td>
<td>Professors and</td>
<td>1. Researching test methodologies on test beds</td>
</tr>
<tr>
<td>(3rd line)</td>
<td></td>
<td>students</td>
<td>2. Researching product bottlenecks</td>
</tr>
</tbody>
</table>
## Initial NBL Test Coverage and Tools

<table>
<thead>
<tr>
<th>Area</th>
<th>DUT/FUT</th>
<th>Test Coverage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>UTM, Anti-Virus, IPS, SSL VPN, IPSec VPN, P2P/IM Management</td>
<td>Functionality, Interoperability, Session Capacity and Rate, Accuracy</td>
</tr>
<tr>
<td>VoIP And WLAN</td>
<td>SOHO Router, DSL Router, IAD Gateway, SIP Phone, SIP Gateway, SIP Proxy, Access Point</td>
<td>Voice Quality, Mobility, Functionality, Interoperability, Session Capacity and Rate</td>
</tr>
<tr>
<td>Bridging and Routing</td>
<td>Ethernet L2/L3 Switch</td>
<td>Functionality, Conformance, RFC 2544/2889</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Area</th>
<th>Type</th>
<th>Commercial Test Platforms</th>
<th>Commercial Test Tools</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch/Router</td>
<td>Smartbits 2000</td>
<td>ANVL</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Smartbits 6000B</td>
<td>SmartFlow ・ SmartWindow</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Smartbits 6000C</td>
<td>SmartMulticastIP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SmartMetrics XD 3324A*4, totally 16 * Giga ports</td>
<td>TeraDot1x ・ TeraRouting</td>
<td></td>
</tr>
<tr>
<td>WLAN</td>
<td>Azimuth 800W-platform</td>
<td>Azimuth Director</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IxWLAN</td>
<td>IxChariot</td>
<td></td>
</tr>
<tr>
<td>VoIP</td>
<td>Abacus 5000</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Emutel Edge Bulk call generator</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NCSec</td>
<td>Smartbits 600</td>
<td>Avalanche ・ TeraVPN ・ WebSuite</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TeraMetrics 3301A*2, totally 4 * Giga ports</td>
<td>Traffic IQ Professional</td>
<td></td>
</tr>
</tbody>
</table>
NBL Industrial Customers

- Over 100 vendors served, over 600 products tested
## Switch and Router

<table>
<thead>
<tr>
<th>Performance</th>
<th>Conformance</th>
<th>Functionality &amp; Interoperability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forwarding Rate</td>
<td>Spanning Tree (STP)</td>
<td>Management</td>
</tr>
<tr>
<td>Forwarding Latency</td>
<td>Multi/Rapid STP</td>
<td>Firmware Upgrade</td>
</tr>
<tr>
<td>Congestion Control</td>
<td>Virtual LAN</td>
<td>Spanning Tree (STP)</td>
</tr>
<tr>
<td>Broadcast Control</td>
<td>GVRP/GMRP</td>
<td>Virtual LAN</td>
</tr>
<tr>
<td>Address Learning</td>
<td>IP v4/v6 Gateway</td>
<td>GVRP/GMRP</td>
</tr>
<tr>
<td>Address Caching</td>
<td>ICMP/IGMP</td>
<td>Link Aggregation</td>
</tr>
<tr>
<td>IP Forwarding</td>
<td>Routing: RIP/OSPF,</td>
<td>Authentication (.1X)</td>
</tr>
<tr>
<td>IP Multicasting</td>
<td>DVMRP, and PIM</td>
<td>IP Configuration</td>
</tr>
<tr>
<td>Routing: RIP/OSPF</td>
<td>SNMP, RMON</td>
<td>Routing: RIP/OSPF, DVMRP, and PIM</td>
</tr>
<tr>
<td>Redundancy: VRRP</td>
<td></td>
<td>DHCP, NAT, etc.</td>
</tr>
<tr>
<td>Quality of Service</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Diagram:**

- **Route Flapping**
- **Virtual Area Differentiation**
- **Traffic Flow Prioritization**
- **Loop-Free Path Construction**
- **Optimal Route Manipulation**
- **System Under Test**
- **Test Equipment**
### WLAN

<table>
<thead>
<tr>
<th>Performance</th>
<th>Functionality &amp; Interoperability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forwarding Rate</td>
<td>SSID/Channel</td>
</tr>
<tr>
<td>Association Capacity</td>
<td>WEP/WPA-PSK/TLS</td>
</tr>
<tr>
<td>Association Latency</td>
<td>Power Saving Mode</td>
</tr>
<tr>
<td>Rate vs. Range</td>
<td>Roaming Ability</td>
</tr>
<tr>
<td>Rate vs. Channel</td>
<td>Site Survey/Profile</td>
</tr>
<tr>
<td>Failover Roaming</td>
<td>WDS Bridge Mode</td>
</tr>
<tr>
<td>Smooth Roaming</td>
<td>TX Rates/Beacon Int.</td>
</tr>
<tr>
<td>WDS Forwarding Rate</td>
<td>MixedBG/PureG Mode</td>
</tr>
<tr>
<td>Rate vs. WDS Range</td>
<td>RTS/Fragment Threshold</td>
</tr>
<tr>
<td>Rate vs. WDS Channel</td>
<td>Firmware Upgrade</td>
</tr>
<tr>
<td>MixedBG Throughput</td>
<td>User Interfaces, etc.</td>
</tr>
<tr>
<td>Secure Throughput</td>
<td></td>
</tr>
<tr>
<td>PowerSaved Throughput</td>
<td></td>
</tr>
<tr>
<td>Interfered Throughout</td>
<td></td>
</tr>
<tr>
<td>App/VoIP Distance</td>
<td></td>
</tr>
<tr>
<td>App/VoIP Switch Roam</td>
<td></td>
</tr>
<tr>
<td>App/VoIP Motion Adapt</td>
<td></td>
</tr>
<tr>
<td>App/VoIP Motion Roam</td>
<td></td>
</tr>
</tbody>
</table>
## VoIP

### Performance
- Voice Quality (PESQ, PSQM+, PAMS, MOS), Echo Doubletalk, Signal Loss, VAD, Call Processing (Bulk Call Generation), Security, Vulnerability Scanning, etc.

### Functionality
- Management, Firmware Update, Voice Message, DTMF, Authentication, Three-Way Conference, Call Features (Call Hold, Call Transfer, etc.), NAT Traversal, Networking (DHCP, DNS, PPPoE, etc.), Phone Book, etc.

### Interoperability
- Signaling, Conversation, CODEC, Call Features (Call Hold, Call Transfer, etc.), NAT Traversal, ENUM trial, etc. (Communicate with Different CPE and CO Devices)

### Conformance
- SIP Signaling (Testing in Normal and Abnormal Call Flows)

### Table

<table>
<thead>
<tr>
<th>Hours</th>
<th>DUT</th>
<th>Abacus Attempts</th>
<th>DUT Answers</th>
<th>Errors</th>
<th>Completion Ratio</th>
<th>Call Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>IAD Gateway</td>
<td>1,370</td>
<td>1,370</td>
<td>0</td>
<td>100.00</td>
<td>114</td>
</tr>
<tr>
<td>24</td>
<td>IAD Gateway</td>
<td>2,578</td>
<td>2,576</td>
<td>2</td>
<td>99.92</td>
<td>107</td>
</tr>
<tr>
<td>36</td>
<td>IAD Gateway</td>
<td>3,669</td>
<td>3,659</td>
<td>10</td>
<td>99.73</td>
<td>101</td>
</tr>
<tr>
<td>48</td>
<td>IAD Gateway</td>
<td>4,577</td>
<td>4,565</td>
<td>12</td>
<td>99.74</td>
<td>95</td>
</tr>
</tbody>
</table>

![Graph showing performance metrics like echo emulation and WAN emulation.](image)
# Security

<table>
<thead>
<tr>
<th>Functionality</th>
<th>Performance</th>
<th>Interoperability &amp; Conformance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet Filter</td>
<td>Capacity&amp;Rate : TCP Connection IPSec Session SMTP/POP3 Session FTP Session Telnet Session HTTP(S) Session Streaming Session DNS Session Utilities : WebSuite, TeraVPN, Avalanche, In-Lab Live Testing, URL Filtering Analyzer</td>
<td>IPSec Interop Time for purging SA Initiator/Responder Phase 1 Phase 2 ID Key Group and PFS IPSec Keep Alive NAT-Traversal Dead Peer Detection Conformance : IKE, ESP, AH, PPTP, and L2TP Utility : 10+ VPN Devices ANVL</td>
</tr>
<tr>
<td>IPSEC, SSL VPN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firewall</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPS/IDP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Content Filter</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Anti-Virus</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Anti-Spyware</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Anti-Spam</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IM Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Endpoint Security</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Capacity & Rate:**
- TCP Connection
- IPSec Session
- SMTP/POP3 Session
- FTP Session
- Telnet Session
- HTTP(S) Session
- Streaming Session
- DNS Session
- Utilities: WebSuite, TeraVPN, Avalanche, In-Lab Live Testing, URL Filtering Analyzer

**Interoperability & Conformance:**
- IKE, ESP, AH, PPTP, and L2TP
- Utility: 10+ VPN Devices ANVL
Where the Traditional Didn’t Touch – Stability

• Traditional test
  ◆ Functionality
  ◆ Performance
  ◆ Conformance
  ◆ Interoperability

• Lab test vs. field test
  ◆ Traffic: artificial vs. real
  ◆ Executed program space: limited vs. exhaustive

• Stability test!!
  ◆ Customer Found Defect (CFD)
  ◆ Triggered by real traffic
## Test Coverage: An Example

### Test Cases vs Functions

<table>
<thead>
<tr>
<th>Test Cases</th>
<th>Functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>1</td>
</tr>
<tr>
<td>B</td>
<td>2</td>
</tr>
<tr>
<td>C</td>
<td>3</td>
</tr>
<tr>
<td>D</td>
<td>4</td>
</tr>
<tr>
<td>E</td>
<td>5</td>
</tr>
<tr>
<td>F</td>
<td>6</td>
</tr>
<tr>
<td>G</td>
<td>7</td>
</tr>
</tbody>
</table>

### Test Cases | Cost | Functions

<table>
<thead>
<tr>
<th>Test Cases</th>
<th>Cost</th>
<th>Functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>10</td>
<td>1, 2, 3</td>
</tr>
<tr>
<td>B</td>
<td>5</td>
<td>2, 4</td>
</tr>
<tr>
<td>C</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>D</td>
<td>5</td>
<td>5, 6</td>
</tr>
<tr>
<td>E</td>
<td>4</td>
<td>3, 4, 6</td>
</tr>
<tr>
<td>F</td>
<td>3</td>
<td>5, 7</td>
</tr>
<tr>
<td>G</td>
<td>2</td>
<td>7</td>
</tr>
</tbody>
</table>

### Modified Functions: 2, 3, 7

### Methods

<table>
<thead>
<tr>
<th>Methods</th>
<th>Selected Test Cases</th>
<th>Cost</th>
<th>Reached Functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traditional selection</td>
<td>A, B, C, D, E, F, G</td>
<td>31</td>
<td>7</td>
</tr>
<tr>
<td>Safe selection</td>
<td>A, B, C, E, F, G</td>
<td>26</td>
<td>7</td>
</tr>
<tr>
<td>Minimize Numbers</td>
<td>A, F</td>
<td>13</td>
<td>5</td>
</tr>
<tr>
<td>Minimize Cost</td>
<td>B, C, G</td>
<td>9</td>
<td>4</td>
</tr>
<tr>
<td>Balance Cost and Coverage (1:1)</td>
<td>E, F, A</td>
<td>17</td>
<td>7</td>
</tr>
<tr>
<td>Maximize Coverage with Given Cost (10 minutes)</td>
<td>E, F</td>
<td>7</td>
<td>5</td>
</tr>
<tr>
<td>Minimize Cost with Given Coverage (Cover 6 functions)</td>
<td>E, F, A</td>
<td>17</td>
<td>7</td>
</tr>
</tbody>
</table>
Relationship Between Test Technologies

- **Test Automation** (To improve Test Efficiency)
- **Field Test** (To improve Test Quality)
- **RealFlow Test** (To improve Field Test Environment — Quality & Efficiency)
- **Traffic Diversification & Test Coverage Optimization** (To improve security testing & quality assurance)

- 一般測試步驟
- 互相影響反饋
Automation: ACTS (Auto-Control Test System)
Real Traffic: RealFlow
Test Coverage: TestCov

NBL TECHNOLOGIES
FROM TEST SERVICE PROVIDER TO TEST SOLUTION PROVIDER
Switch and Router
Network Security
WLAN
4G LTE
Handhelds

NBL TECHNOLOGY APPLICATIONS
FROM NETWORK DEVICES TO HANDHELDs
<table>
<thead>
<tr>
<th>編號</th>
<th>技術名稱</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>自動控制測試系統 - ACTS (Automatically Controlled Test System)</td>
</tr>
<tr>
<td>2</td>
<td>真實流量錄製與重播工具 – ILLT (In-Lab Live Testing)</td>
</tr>
<tr>
<td>3</td>
<td>真實流量資料庫 – PCAP Lib</td>
</tr>
<tr>
<td>4</td>
<td>測試涵蓋率分析與最佳化之技術 – Test Coverage Analysis and Optimization</td>
</tr>
<tr>
<td>5</td>
<td>惡意程式收集分析之工具與資料庫 – Malware Tool-chain and Malware Lib</td>
</tr>
<tr>
<td>6</td>
<td>無線區域網路流量與訊號之錄製與重播工具 – WLAN Capture and Replay of Traffic and Environment</td>
</tr>
<tr>
<td>7</td>
<td>第四代無線行動通訊之協定測試環境 – LTE Conformance and Interoperability Testing</td>
</tr>
<tr>
<td>8</td>
<td>第四代無線行動通訊之多重輸入出之測試環境與工具 – LTE MIMO OTA (Over-the-Air)</td>
</tr>
<tr>
<td>9</td>
<td>手持裝置耗時耗電與穩定度之自動測試工具 – Android AKL (Automatic Key Logger)</td>
</tr>
</tbody>
</table>
Auto-Control Test System (ACTS) 1/2

#1

Network Benchmarking Lab

Test System Overview:

- **Auto-Control Test System (ACTS)**
- **Measurement Method**
  - **Network**: Internet
  - **Device**: Server
  - **Test Object**: Traffic Generation Equipment
  - **Flow Generation Equipment**:Win8, Win7, Mac 10.8
  - **Flow Generation Equipment**:iPad, Android Pad, Win Pad

Transmission Mediums:

- Ethernet
- Fiber
- WiFi
- LTE
- PLC
- RS232

Test Process Control Server

Flow Generation Equipment:

- iPhone, gPhone, wPhone
- iPad, Android Pad, Win Pad
- iPhone, gPhone, wPhone
- iPad, Android Pad, Win Pad
- iPhone, gPhone, wPhone

Network Benchmarking Lab

A Real Traffic Test Lab
Auto-Control Test System (ACTS) 2/2

User Interface
- Customization
- GUI
- CLI

Runner
- Customization
- General

Modules
- GLOBAL
- CONSOLE
- WEB
- DOSAPP
- GUI APP
- IMAGEAPP

Display or Debug

Report
ACTS Application Case

• Control Commands (API)

<table>
<thead>
<tr>
<th>Control Interface</th>
<th>Control Commands</th>
<th>功能</th>
</tr>
</thead>
<tbody>
<tr>
<td>RS232</td>
<td>22</td>
<td>Issue commands to DUTs through RS232</td>
</tr>
<tr>
<td>Web GUI</td>
<td>31</td>
<td>Configure Web modules on DUTs</td>
</tr>
<tr>
<td>iOS</td>
<td>5</td>
<td>Configure iPhone or iPad</td>
</tr>
<tr>
<td>Win APP</td>
<td>18</td>
<td>Control Windows Application, e.g. Filezilla</td>
</tr>
<tr>
<td>DOS APP</td>
<td>22</td>
<td>Control DOS Application, e.g. Ping</td>
</tr>
<tr>
<td>Others</td>
<td>Extensible</td>
<td>TCL Scripting</td>
</tr>
</tbody>
</table>

• NBL has developed over 3000 test scripts, for 7 functionality tests.
# Comparing Automatic Testing Platforms

<table>
<thead>
<tr>
<th></th>
<th>AutoMate</th>
<th>QTP</th>
<th>Rational</th>
<th>ACTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capture</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Partial(Web)</td>
</tr>
<tr>
<td>Ease of use</td>
<td>Easy</td>
<td>Difficult</td>
<td>Difficult</td>
<td>Medium</td>
</tr>
<tr>
<td>Script language</td>
<td>Self-defined</td>
<td>Self-defined +VB</td>
<td>Self-defined +Java</td>
<td>TCL</td>
</tr>
<tr>
<td>Self-defined functions</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Debug mode</td>
<td>No</td>
<td>Yes (break point)</td>
<td>Yes (break point)</td>
<td>Yes (debug tag)</td>
</tr>
</tbody>
</table>

- Parameterized test scripts
- Supporting the control of commercial platforms (Smartbits, Android)
- Supporting Web control (Ajax, Javascript, .NET)
- Increased test productivity by 100%
- Shortened test script deployment by 50%
- Hosting over 3000 test scripts
Beta Site with 6 DUT Zones

- A world-wide unique model of applying campus traffic to testing
- Appeared in IEEE Communications Magazine, Dec 2010

- Zone 1
  - End-user software
- Zone 2
  - Ethernet L2/L3 Switch
  - Wireless AP
- Zone 3
  - Core Router
- Zone 4 (Inline, one-in-one-out)
  - UTM, IPS, Anti-Virus, QoS Firewall
- Zone 5 (Sniff)
  - Network Forensic
  - Anti-Malware/Botnet
- Zone 6 (ILLT)
  - SOHO Router, Home Gateway
  - Broadband Gateway
  - DSL Router, IAD Gateway
Time to Fail (TTF)

- TTF: Time to trigger a defect during product testing
  - TTF $\geqslant$ 4 weeks $\rightarrow$ convergence!
  - convergence ratio: percentage of SUTs that could converge in a period of time
- Among 100 SUTs
  - TTF $\uparrow$ as test duration $\uparrow$, which means improved product quality
  - Under a test duration of 1 month and 1 year, we have a convergence ratio of 7% and 20%, respectively.
  - Only a few SUTs could survive well under real traffic.
RealFlow Certification

• RealFlow Test
  ◆ Applying real traffic, *live* or *replayed*, to test products

• RealFlow Certification
  ◆ Converged under RealFlow Test, i.e., TTF $\geq 4$ weeks
  ◆ Iterative testing for 6 months to 1 year, with a pass ratio of ….

5%
1. 重播流量
2. 透過syslog蒐集各設備偵測結果
3. 將偵測結果分類存入資料庫
4. 分析結果
PCAP Lib: Classifying, Extracting, and Anonymizing Packet Traces

- PCAP Lib: classified, extracted, and anonymized
- In revision at IEEE Systems Journal, 2013
## PCAP Lib for Scholars 1.0

<table>
<thead>
<tr>
<th>Category</th>
<th>T1</th>
<th>T2</th>
<th>T3</th>
<th>T4</th>
<th>T5</th>
<th>T6</th>
<th>T7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web</td>
<td>HTTP (125)</td>
<td>POP3 (5)</td>
<td>SMTP (11)</td>
<td>IMAP (5)</td>
<td>FTP (28)</td>
<td>SMB (22)</td>
<td>TFTP (1)</td>
</tr>
<tr>
<td>Email</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>File Transfer</td>
<td></td>
<td>FTP (28)</td>
<td>SMB (22)</td>
<td>TFTP (1)</td>
<td>Telnet (6)</td>
<td>SSH (4)</td>
<td>RDP (4)</td>
</tr>
<tr>
<td>Remote Access</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encryption</td>
<td>SSL (11)</td>
<td>FTPs (1)</td>
<td>HTTPs (1)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chat</td>
<td>IRC (7)</td>
<td>ICQ (4)</td>
<td>Yahoo Messenger (4)</td>
<td>MSN (1)</td>
<td>AIM (1)</td>
<td>Skype (1)</td>
<td>Google talk (1)</td>
</tr>
<tr>
<td>File Sharing</td>
<td>BitTorrent (2)</td>
<td>eDonkey (1)</td>
<td>Gnutella (1)</td>
<td>Pando (1)</td>
<td>SoulSeek (1)</td>
<td>Winny (1)</td>
<td>Xunlei (1)</td>
</tr>
<tr>
<td>Streaming</td>
<td>PPLive (2)</td>
<td>QuickTime (1)</td>
<td>Octoshape (1)</td>
<td>Orb (1)</td>
<td>Slingbox (1)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VoIP</td>
<td>SIP (4)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>NetBIOS (21)</td>
<td>DNS (19)</td>
<td>SNMP (3)</td>
<td>Socks (1)</td>
<td>STUN (1)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Extracting Attack Sessions from Real Traffic with Intrusion Prevention Systems

- Leveraging product signature databases to classify and extract attack sessions
Session Classification Based on Flow Classification, Association and Arbitration

- Classifying with packet size distribution as signatures
- Appeared in Computer Networks, Jan 2012
SocketReplay: Low-Storage Packet Capture and Loss-Recovery Stateful Replay of Real Flows

- Socket Replay: a stateful replay tool that tolerates capture loss
- Appeared in IEEE Communications Magazine, Apr 2012
Replay Test – In-Lab Live Test (ILLT)

- **DUT**
  - Device Under Test

- **NBL PCAP Library**
  - Packet trace repository in PCAP format

- **NBL Checkdev**
  - Probing the DUT status
  - Collecting statistics of replayed traffic

- **NBL Traffic-Replay**
  - Replaying PCAP packet traces
Live SOHO Public Testing
SOHO Routers “Wall”
ILLT Test Results

- Replayed traffic volume > 4 TB
Market Impact

• Forums and blogs
  ◆ Mobile01, Xfastest, 巴哈姆特, PCZone, 滄者極限, 中國無線論壇, PALMiséLife, FAME中隊, 香港高登, HKEPC, Plus….
  ◆ Blog
  ◆ Plurk
  ◆ PTT (BBS)

• Well recognized models
  ◆ Buffalo WZR-HP-G300NH, WCR-G54
  ◆ PCI MZK-WNH
  ◆ SMC WBR14S-NL
  ◆ ASUS RT-N16
  ◆ Apple Airport Extreme
TestCov: Coverage Analysis and Optimization

**Traffic diversification system**

- Captured Traces
  - beta site
  - artificial
  - replay

- Traffic Mutator (NBL-Fuzzer)

- Testing Trace

- DUTs

**Test case generator**

- Testing requirements
- Test case design

- Instrumentation selection
- Code coverage analyzer
- Matrix coverage analyzer

**Coverage visualization**

- TreeMap

**Test coverage visualization system (TestCov)**

- Traces storage
- Coverage mapping database

- Testing requirements/specification
- Test case selection (algorithms)

**Test case selection system with optimal test coverage (TestSel)**

- Regression testing

**Testbed**

**Output**

- Test confidence evaluation
- Coverage Analyzer/Visualization

- Captured Traces
- Traffic Mutator (NBL-Fuzzer)
- Testing Trace

- DUTs

**Coverage mapping database**

- Regression testing

**Output**

- Test confidence evaluation
- Coverage Analyzer/Visualization
Test Coverage Analysis and Optimization for Large Code Problems

- Function reachability of test cases: how many functions a test case can reach
- Test intensity of functions: how often a function is reached
- Formulated and solved 6 optimization problems
- Appeared in Journal of Systems and Software, Jan 2012
Redefining Security Criteria

- Best-of-breed from Common Criteria, ICSA, NSS, and RealFlow
- NCC Security Criteria: switch, router, WLAN, firewall, IDS, WAF, anti-virus, anti-spam, application control
Malware Tool-Chain: Collection, Detection, Analysis

- Malware collection: active vs. passive
- Malware propagation: passive vs. active
- To appear in IEEE Computer, 2014

PMC&D: Proactive Malware Capture & Detection
HBA: Host Behavior Analysis
NBA: Network Behavior Analysis
EAR: Real Traffic Replay over WLAN with Environment Emulation

Appeared in IEEE WCNC, Apr 2012

EAR: Event-driven Automata-synchronized Replay

EAR Evaluation Testbed

AP (DUT)

WLAN Adapter

RF Cable

USB

Noise Generator

Monitor 1

Chamber

GPIB

USB

STA (Replay)

WLAN Adapter

RF Cable

Attenuator

RF Cable

Interference Generator

Monitor 2

A Real Traffic Test Lab
Event Reproduction Ratio of EAR

- Graph 1: Reproduction ratio (%) vs. Percentage of atomic events (%)
  - Without packet-replay control
  - EAR

- Graph 2: Reproduction ratio (%) vs. Signal strength (dBm)
  - Without environment emulation
  - EAR

- Graph 3: Reproduction ratio (%) vs. Percentage of non-atomic events (%)
  - Without packet-replay control
  - EAR
LTE 4-stage Testbeds

- Stage 1
  - eNB emulator
  - Test purposes
    - Conformance Test
    - Design verification
- Stage 2
  - eNB/EPC of diff. vendors
  - Test purposes
    - Interoperability Test
    - Capacity verification
- Stage 3
  - OTA chamber/channel emulator
  - Test purposes
    - Operator-IOT
    - Performance test for mobile devices
- Stage 4
  - Experimental band in NCTU campus
  - Test purposes
    - Field Trials
Throughput vs. Channel Power and Angle (DUT2)

DUT-2 Open Loop Spatial Multiplexing
Single Cluster SCME Umi 30km/h 10000 Subframes

Throughput vs. Channel Power and Angle (DUT2)
Effect of Attitude Angle to Throughput (-74.4dBm)
A Spin-Off: EBL (Embedded Benchmarking Lab)

- AKL (stand-alone)
- Dynamic Multi-Level Profiler
- Cross Layer Bottleneck Detector
- Bottleneck Analyzer
- H-Profile
  - Power Measurer (System Level)
  - Battery Use Extension (App Level)
  - Power Memo (Function Level)
Android Key Logger (AKL)

The AKL can record, then replay user events.
Application Power Measurer

- **Purpose**
  - To measure power consumption for android Apps automatically

- **Test tools**
  - Power meter
  - Android Key Logger
Battery Rundown Test

- Decide user scenario
- Set execution loop
- Get battery life time

<table>
<thead>
<tr>
<th>Elapsed Time (HH:MM)</th>
<th>Battery Capacity (%)</th>
<th>Duration (Min)</th>
<th>Power Consumption (%)</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:00</td>
<td>100%</td>
<td>0</td>
<td>0%</td>
<td></td>
</tr>
<tr>
<td>00:59</td>
<td>87%</td>
<td>59</td>
<td>13%</td>
<td></td>
</tr>
<tr>
<td>02:01</td>
<td>70%</td>
<td>62</td>
<td>17%</td>
<td></td>
</tr>
<tr>
<td>03:00</td>
<td>54%</td>
<td>59</td>
<td>16%</td>
<td></td>
</tr>
<tr>
<td>04:00</td>
<td>36%</td>
<td>60</td>
<td>18%</td>
<td></td>
</tr>
<tr>
<td>05:02</td>
<td>18%</td>
<td>62</td>
<td>18%</td>
<td></td>
</tr>
<tr>
<td>06:00</td>
<td>2%</td>
<td>58</td>
<td>16%</td>
<td></td>
</tr>
<tr>
<td>06:03</td>
<td>0%</td>
<td>3</td>
<td>2%</td>
<td>Device Auto Shutdown</td>
</tr>
</tbody>
</table>

Browse web and receive email on Wi-Fi (Unit: hour)
System Stability Test

Android System Stability Test Result

- DUT_2(None): 20.5 hours
- DUT_3(W): 24 hours
- DUT_1 (D): 24 hours
- DUT_3: 24 hours
- DUT_2(W): 1.86 hours
- DUT_1 (D): 24 hours
- DUT_3(None): 24 hours
- DUT_2(W): 20 hours
- DUT_1 (D): 17.5 hours
- DUT_3(None): 48 hours
- DUT_2(W): 15 hours
- DUT_1 (D): 48 hours

DUT Issue
Automated GUI Testing for Embedded Systems

- SPAG (Smart Phone Automatic GUI)
- Record and replay user behaviors with accuracy improvement

(a) Record stage

(b) Replay stage

Diagram symbols:
- Component
- Document
- Control
- Data
- Substance
Lessons (1/2)

- Development vs. research
  - R only, R→D, D→R, or parallel R&D?
  - Front line (D) → back line (R), D first then R
  - Industry: D&r, academia: R&d
    → grow r in industry & d in academia!
  - Good balance between D & R: but not in ComSoc

- NBL experiences
  - Duplicating others (e.g. UNH/IOL) has no value.
  - Real traffic testing is indeed unique.
  - 3rd-party lab only for 2nd-tier vendors?
    ■ Large/small projects with large/small vendors

- Research roadmap vs. random picks
  - A series of works with deeper understanding
  - But random picks have their chances

- Publication strategy: conferences vs. journals/magazines
  - Conference-driven vs. journal-driven: travel budget
  - Time-to-publish
Lessons (2/2)

- Academic services vs. academic cooperation
  - Editorial boards, program committees, technical committees
  - Extra effort for new thoughts and resources
  - Research: collaboration > work alone

- Impacts
  - A work with high impact on the industry might not have high impact on the academia, and vice versa.
  - A high-impact paper might be rejected in its early version.
  - Many papers in top journals or conferences have low impact eventually. The review process can screen regarding *quality* but usually not *impact*.
  - Keep a few of your favorite problems in your mind and review them with new inputs.