Packet Level Traffic Visualisation: The Network Lava Lamp

Jamie Curtis, Richard Nelson

University of Waikato, New Zealand

APRICOT 2007

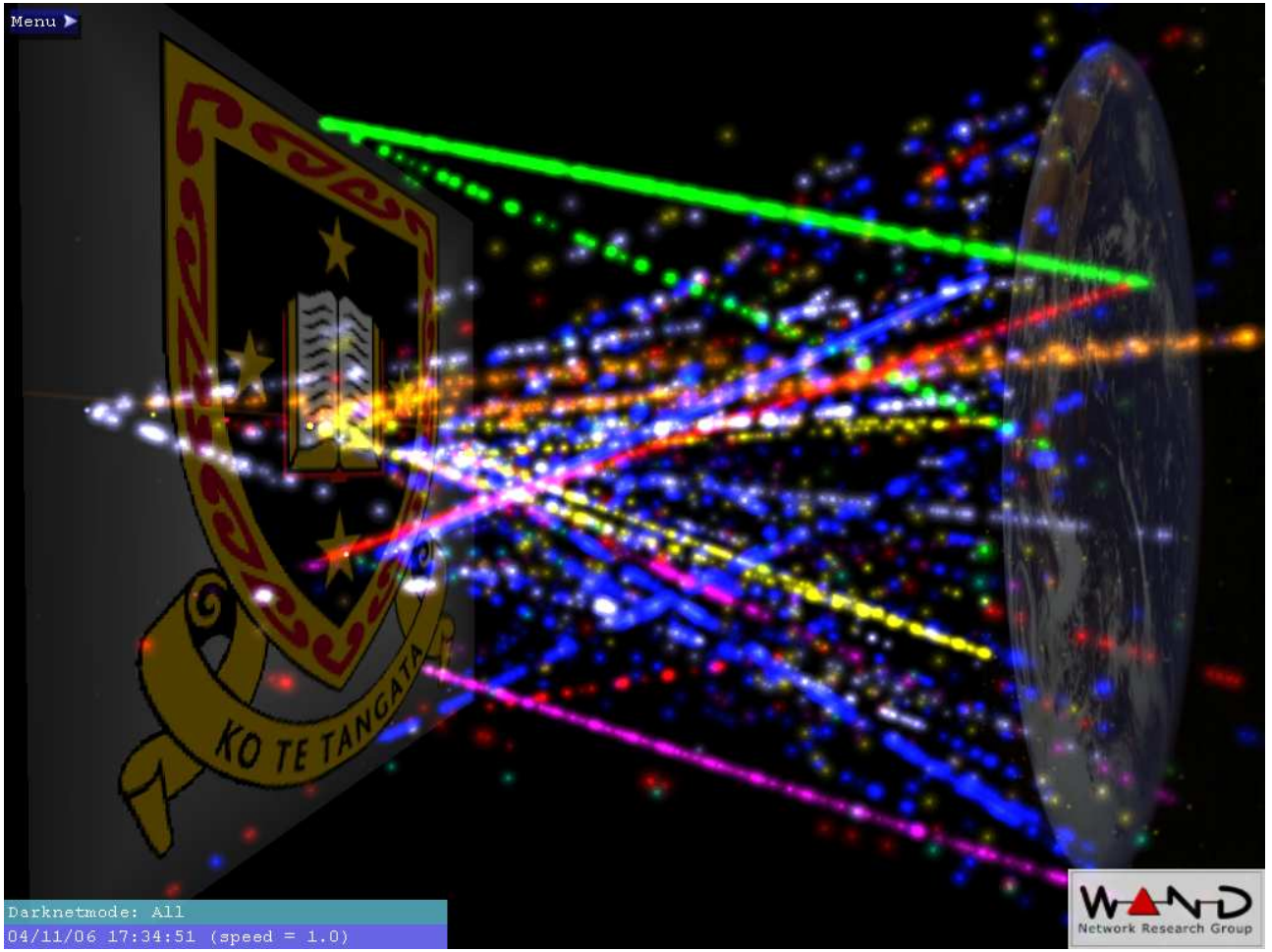
The most important part…

- ….. what does our visualisation look like ?
- Then why we started working on visualisations
- How the visualisation works
- Finally, how could it be useful to you ?

- Why the “Network Lava Lamp” ?
  - Has the same addictive quality, once you start watching it’s hard to look away
  - The more you watch it the more patterns you see

What does it look like ?

- Video 1



Video explanation

- Depicts a view of every packet crossing a single network link
- IP addresses space mapped onto planes
  - Each IP maps to a unique point on the plane
  - Typically internal on left and external on right
- Particles placed on vector from original packets source IP to destination IP
  - Direction determined by direction of packet across original link

Video explanation cont.

- Size of particle depends on size of packet
- Colour of particle depends on protocol
- Speed of particle depends on RTT estimation
- Client has a simple control menu
  - Filtering packets by protocol (colour)
  - Adjust speed of packets
- Visualisation is a true 3D space that the user can move around in

Motivations

- WAND's history is in network simulation and measurement
  - NLANR's Active Measurement Project (AMP) is run by WAND members
- Designed DAG cards for passive monitoring
  - Endace started to continue DAG development
- Been taking lots of header traces
  - Over 800 days of headers of every packet entering and leaving the University Campus (> 3TB traces)
  - Various other networks around the world

Visualisation History

- Visualisation project started to try to explore this huge dataset
- Started using Cichlid from NLANR, now a custom 3D engine because of speed constraints
- Visualisation is also now a tool to help explain networks and passive network analysis
- Acknowledgments:

Brendon Jones and Sam Jansen

Sebastian Dusterwald

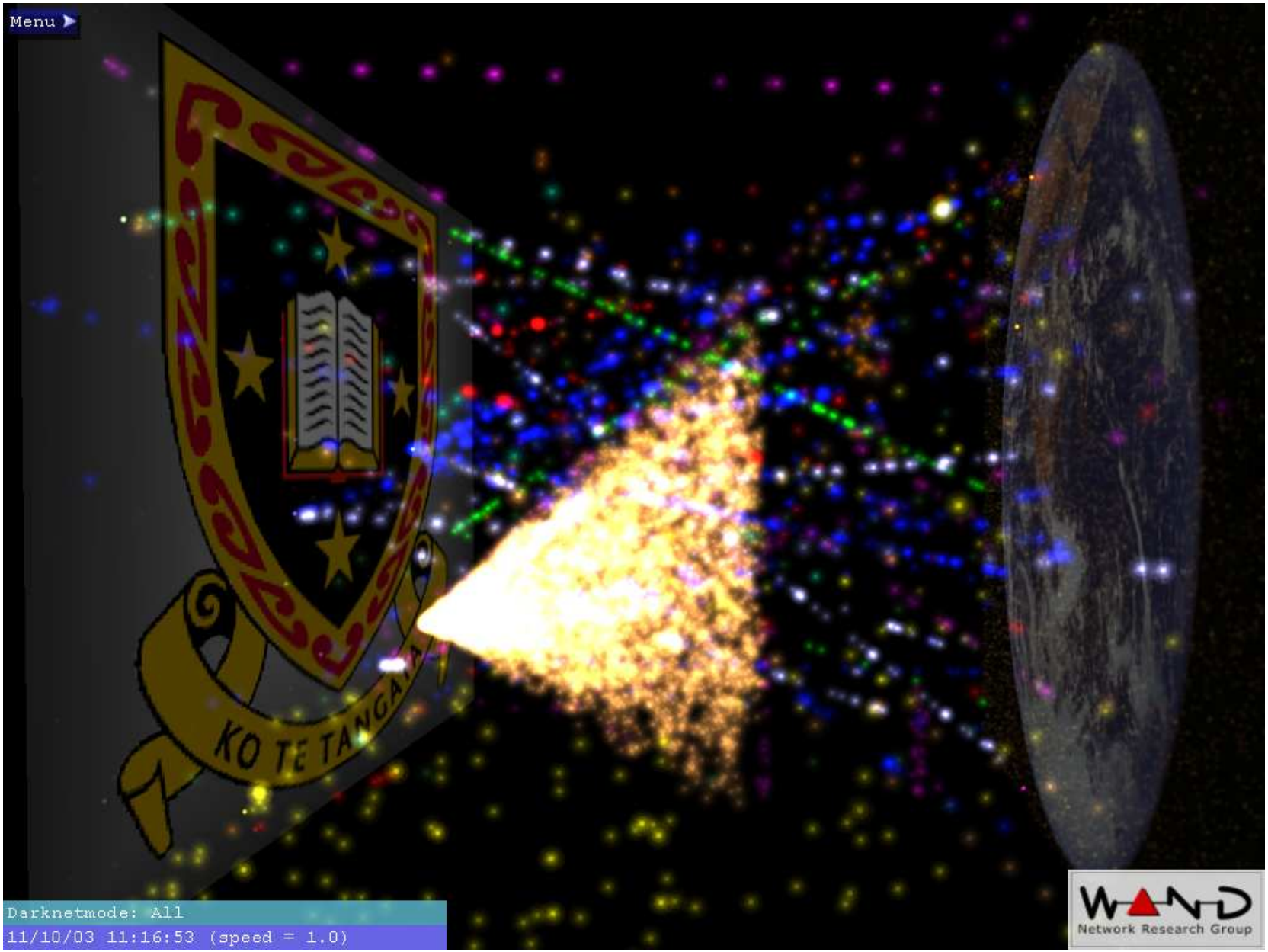
Daniel Lawson, Perry Lorier, Shane Alcock

Power of Visualisations

- Easy enough for almost anyone to read after a simple explanation
- Humans are really good at visual pattern recognition
- Don’t need to have much technical understanding to recognise unusual events
  - but with more experience and understanding you can interpret what the event indicates
- It’s a fun, interesting (and very addictive) way to look at you network
  - while still being a useful tool

Pick the event

- Watch video 2 and see if you can pick the unusual event


Menu
KO TE TANGA
Darknetmode: All
11/10/03 11:16:53 (speed = 1.0)
WAND
Network Research Group

SQL Slammer

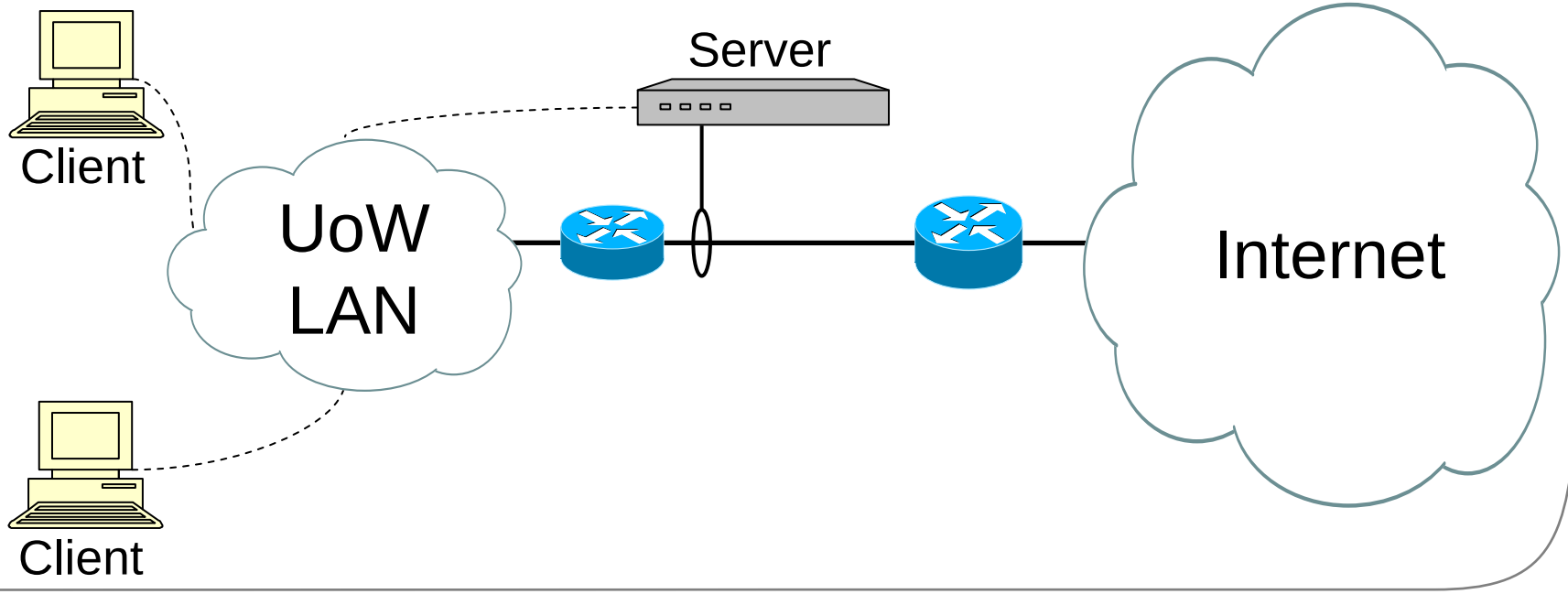
- The video was taken from a live capture at the University of Waikato
- Very obvious at which point the machine was exploited
- BGP session died shortly afterwards because of the UDP flood
- Operators got BGP back up without realising the actual cause of the session dying
- Visualisation made it very obvious what the root cause really was

More examples

- More videos of other types of scans and unusual traffic patterns

Visualisation Architecture

- Split into server and client packages
- Server is responsible for data collection and manipulation
- Client is responsible for data display



Visualisation Server

- Written in C for Unix platforms (primarily Linux)
- Server collects packets
  - PCAP and DAG (hardware capture) input sources
  - Capture from SPAN port or passive network tap
  - Can also replay captured traces
- Server optionally uses BPF to provide filtered views of the link
- Server attempts to estimate the RTT of the flows
  - It provides an appropriate multiplier to the client for speed based on this estimate

Server Modules

- Server uses replaceable modules to determine position, colour and direction
  - Complete packet passed to modules allowing modules to be arbitrarily complex
  - Can be as simple as looking at IP's, ports etc or as complex as L7 analysis
- Modules use **`libtrace`** API that makes writing them easy
- **`libtrace`** is WAND's packet trace, capture and analysis library
  - All of the server is based around this library

Visualisation Client

- Written in OpenGL / C++ for Unix or Windows
- Server passes co-ordinates and colour information for client to display
- Client allows for interactive filtering based on colour
- Protocol between the client and server reduces traffic to approximately 6 bytes per packet
- Users can find out IP addresses by clicking on flow end-points

Example Customisations

- Colour doesn't have to refer to protocol
  - Server passes client the colour and label at startup
  - Could refer to department or division
  - L7 analysis could be used to colour based on file type of P2P (eg, movie, music, iso etc)
- Position modules can be tuned for the number of IP addresses expected on each side of the link
  - Layout each machine individually in a server farm with a picture of the host on the plane
  - Geographic IP placement for the "world" exists (but tends to clump IP's together too much)

Limitations

- The visualisation can become cluttered
  - TCP or UDP packets without payload removed (ACKs)
  - Adjusting speed according to quantity of data
  - Adjusting size of particles
  - Pre-filtering input source at server
- Raw packet capture is often harder to obtain than netflow or similar
- It is a link visualisation
  - Packets have to travel in one of two directions on the link

Future

- More interactive customisation from the client
  - Pushing and pulling options between client and server
- Investigating netflow as input
  - Will lose the ability to do detailed analysis in modules
  - Will have to “fake” the packets out of the flow data
- Also working on separate visualisation focusing on topology analysis
- Always interested in working with Operators in any area of measurement and visualisation

Obtaining

- Source to client, server and **`libtrace`** is all available under the GPL
- Client binaries for Windows available
- The visualisation package is called

  "**B***rendon and* **S***ams* **O***nline* **D***isplay*"

- or BSOD for short
- (Don't let students name their projects !)

`http://research.wand.net.nz/`

WAND Network Research Group
Department of Computer Science
The University of Waikato
Private Bag 3105
Hamilton, New Zealand

www.crc.net.nz
www.wand.net.nz
www.waikato.ac.nz