Visualisation of Protocol Exchange

By Jacky So (2271487)
Supervisor: Dr T. Moors
Background on packet capturer

- Example: Interface of Ethereal

Summary of all captured packets

Details of the selected packet (in blue)

By Jacky So, S1 2003
Motivation

Why are diagrams better?

- Used in every textbook
- Educational purposes
- Debugging
Similar work

- The Visual TCP/UDP Animator (VTA) by Michigan Tech University, America
  - One function of VTA is to plot times-pace diagrams
Similar Work (2)

Limitations of VTA

1. **Platform**
   - VTA runs on Linux
   - My thesis aims to build a tool that runs on all systems

2. **Protocol**
   - VTA captures TCP and UDP packets
   - My thesis aims to visualise exchange for any protocols

3. **Input**
   - VTA captures and visualises traffic itself or from `TCPDUMP`
   - My thesis aims to visualise trace files from all the most popular interface capturers and simulator: TCPDUMP, ETHEREAL, NS
   - VTA plots with one trace file
   - My thesis also aims to use two or more trace files (from source and destination node) to visualise losses and errors in an exchange
Similar Work (3)

4. Output

- VTA shows diagrams while it is running
- **VTA cannot generate accurate time-space diagrams.**
  VTA cannot show the packet receiving/sending time of the other nodes, because it uses captures from local machine only
- My thesis aims to visualise exchange with true times, because the use of multiple trace files
- My thesis aims to show diagrams as it runs and be able to export those diagrams for documentations
Aim of Topic

Packet capturer

OR

Simulator

Text file

Software

Time-Space Diagram

+ 1.845 0 2 cbr 210 ------- 0 0.0 3.1 225
- 2.347 0 3 syn 350 ------- 0.2 0 4.5 129
+ 1.001 1 2 cbr 230 ------- 0 1.0 2.3 128
+ 4.845 0 2 cbr 210 ------- 0.0 0.0 3.1 225

By Jacky So, S1 2003
Underlying theory (1)

- Time-Space diagrams

End points
Underlying theory (2)

- Information (of interest) in the header of packets
  - Source and Destination address
  - Sequence number
  - Packet type
  - Packet size
  - Error checking bits
Underlying theory (3)

Types of Activity shown:

1. **Sending/receiving of packets**
   - Simplest form of data exchange
   - E.g. UDP
Underlying theory (4)

2. Establish/Release of connection
   - E.g. connection set up for TCP

---

Connection Request

Acknowledgement

Data
Underlying theory (5)

3. Loss of packets/Recovery mechanisms

- Loss due to physical loss or error bits
- E.g. Recovery mechanisms in TCP
  - Retransmission Time Out (RTO)
  - Fast Retransmit
Consideration of alternatives

Language
- C/C++: can run on Windows or Linux
- Java: runs on any platform

Output
- Static
  - Bitmap: Large, very well supported, loses quality when enlarged
  - JPEG: Much smaller than Bitmap, portable, widely used, loses quality when enlarged
  - Postscript: compact, diagrams can be resized without losing quality
  - PDF: similar to Postscript, but supports fonts, images, hyperlinks, etc
- Animated
  - GIF: Most widely used, yet is patented
  - PNG: Relatively new, less supported, but not patented
Work Plan for Thesis Part B

- **Task structure**

- 2 week
  - Further research

- ½ week
  - Finalise design

- 4~7 weeks
  - Programming (Basic functionalities)

- 2~4 weeks
  - Programming (Refining)

- 1 week
  - Preparation for demonstration

- Testing & debugging

- Documentations