Communication Network Measurement Reuse

Prof. D. J. Parish

High Speed Networks Group
Department of Electronic and Electrical
Engineering
D.J.Parish@lboro.ac.uk

Loughborough University

Overview

Loughborough University

- Introduction
- What is "Communication Network Measurement Reuse?"
- Collecting Network Measurements
  - Approaches
  - Cost
- Using the Measurements
  - Examples
- Problems to be addressed
  - Technical
  - Legal
  - Financial
- Conclusions

Communication Network Measurement Reuse

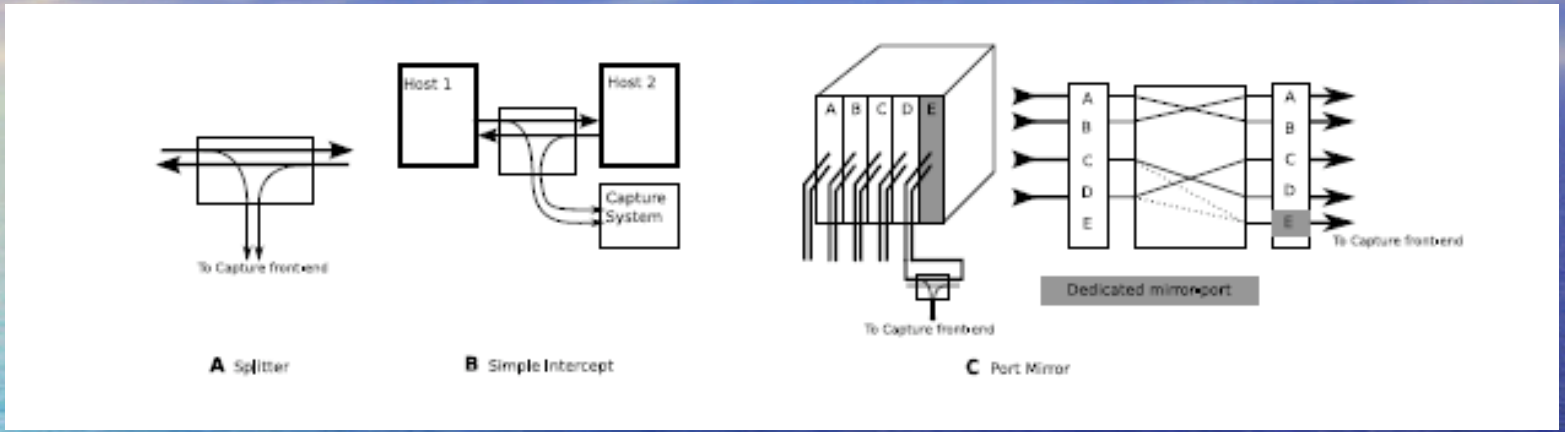
- Using the same fundamental network performance data to meet multiple different requirements
- Measurements are a cost overhead and
- Networks face multiple challenges

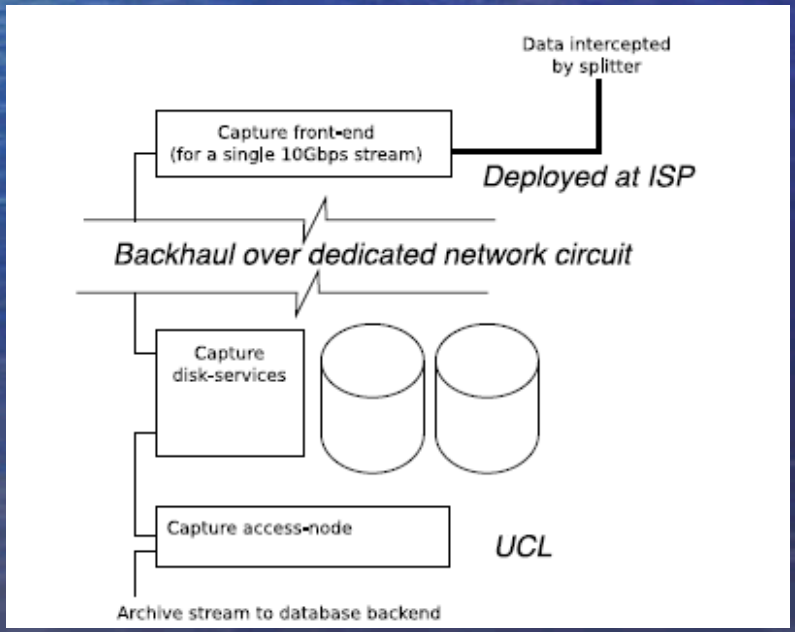
Collecting Communication Network Performance Measurements - Issues

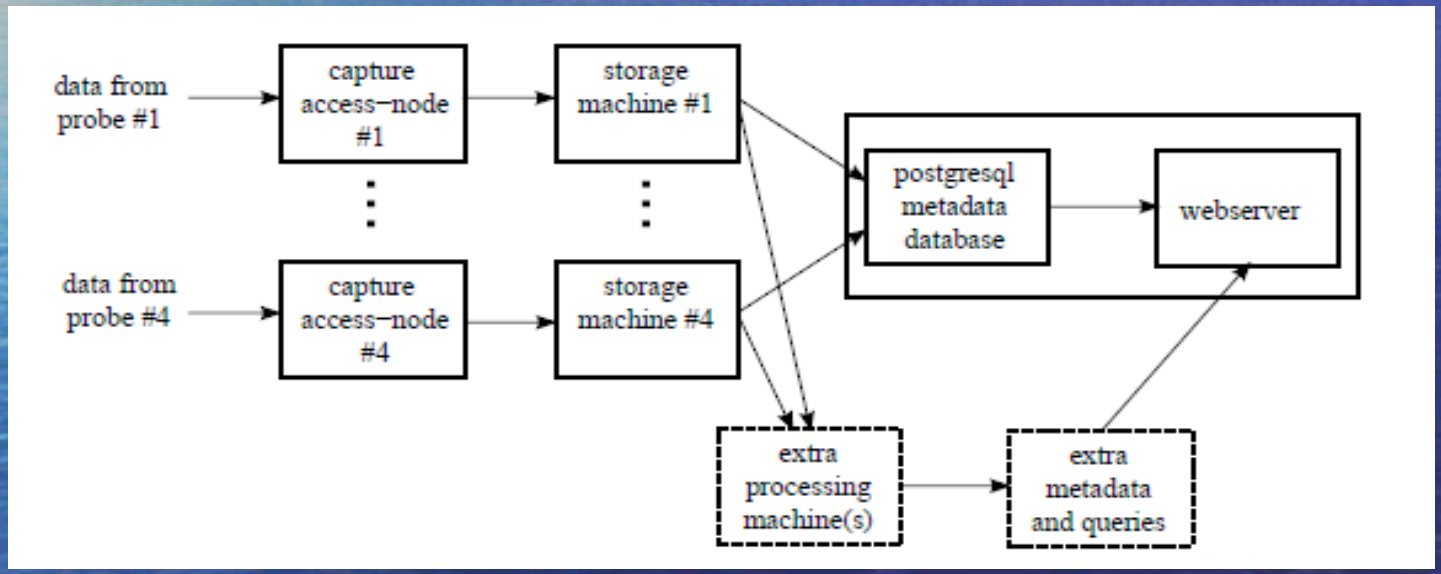
Loughborough University

- An Expensive Activity!
- A Hard problem if high data rate network to be measured
  - Where to measure
  - What to measure
- Commercial or Proprietary Solutions
- Storage and Dissemination
- Use to Maximum Benefit

An example – the MASTS Architecture






data from probe #1
capture access–node #1
storage machine #1
data from probe #4
capture access–node #4
storage machine #4
postgresql metadata database
webserver
extra processing machine(s)
extra metadata and queries

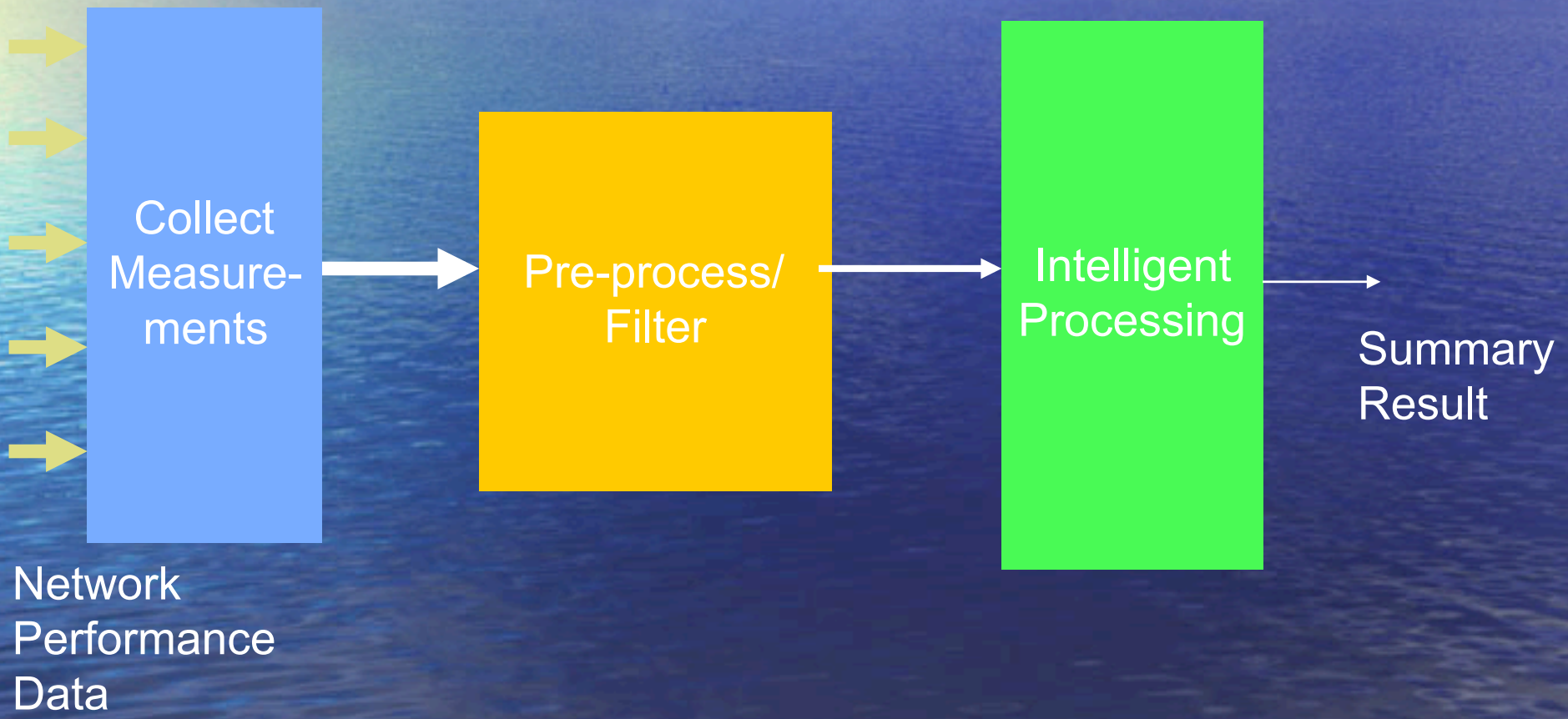
Using Measurements

- Understanding network performance
- Diagnostics
- Planning Upgrades
- Predicting Application Performance
- Identifying Applications
- Identifying Attacks and Abuse
- Security
- Identifying SPAM Relays and BotNets
- Reducing energy usage

Often each area (if active) collects its own data.

Loughborough University

Generic Approach



Loughborough University

Some Specific Examples:

Loughborough University

Application Detection

- An approach to the identification of applications generating traffic on a network.
  - Port Number not always valid
  - Deep Packet analysis not usable due to high data rates or encryption.
- Using the Packet Size Distribution as a "fingerprint".

Loughborough University

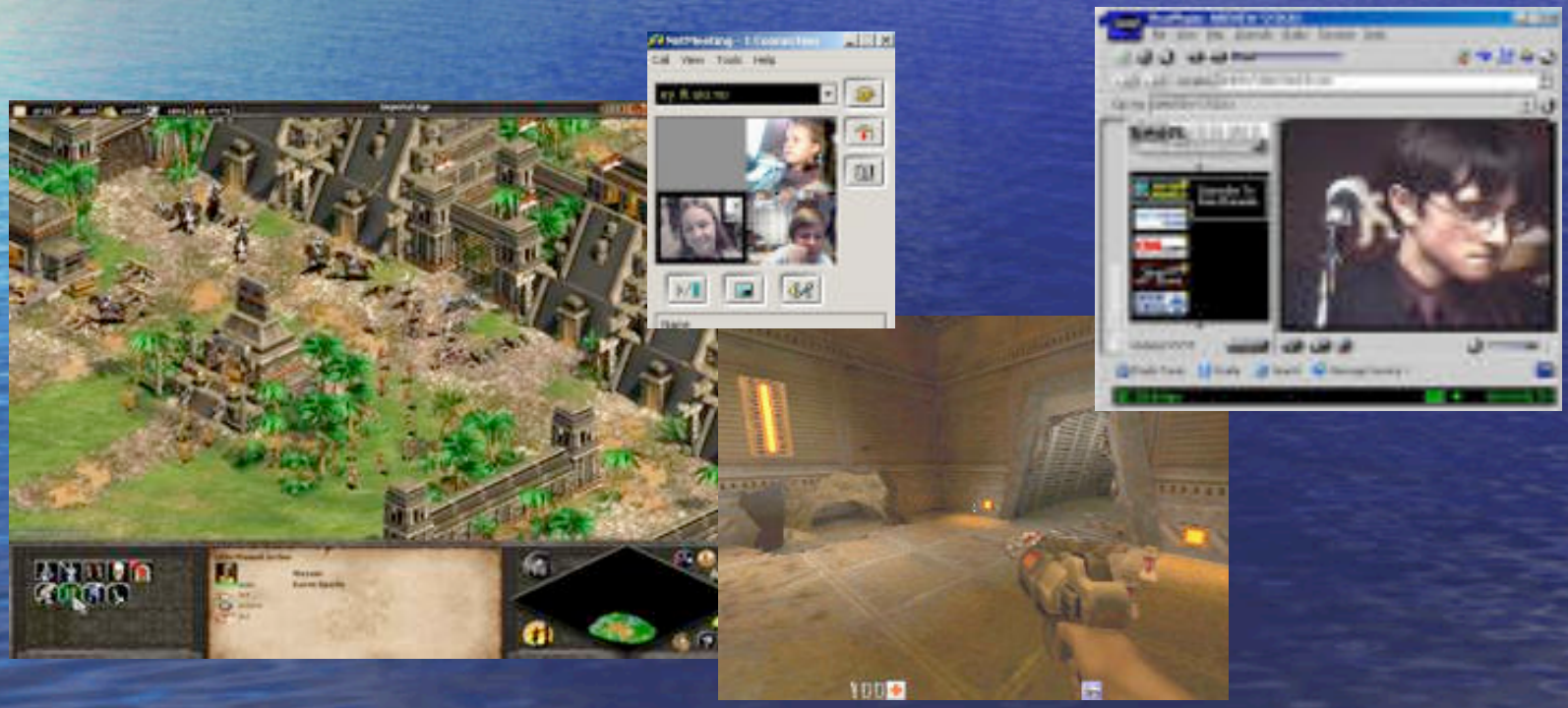
Using Packet Size Distributions

- Packet Size Distribution used as an alternative application 'Signature'
  - Statistical approach
  - Doesn't require every packet to be captured
  - Doesn't rely on the data portion of the packet

Loughborough University

Using Packet Size Distributions

- Traces of Applications Required

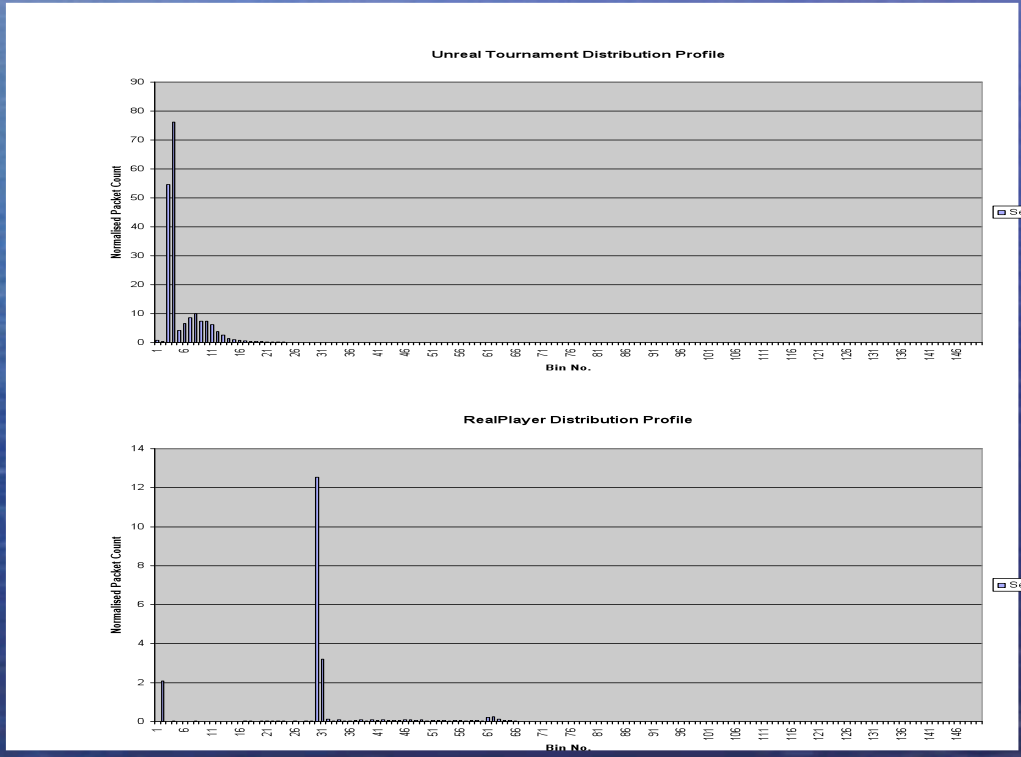


Loughborough University

Using Packet Size Distributions

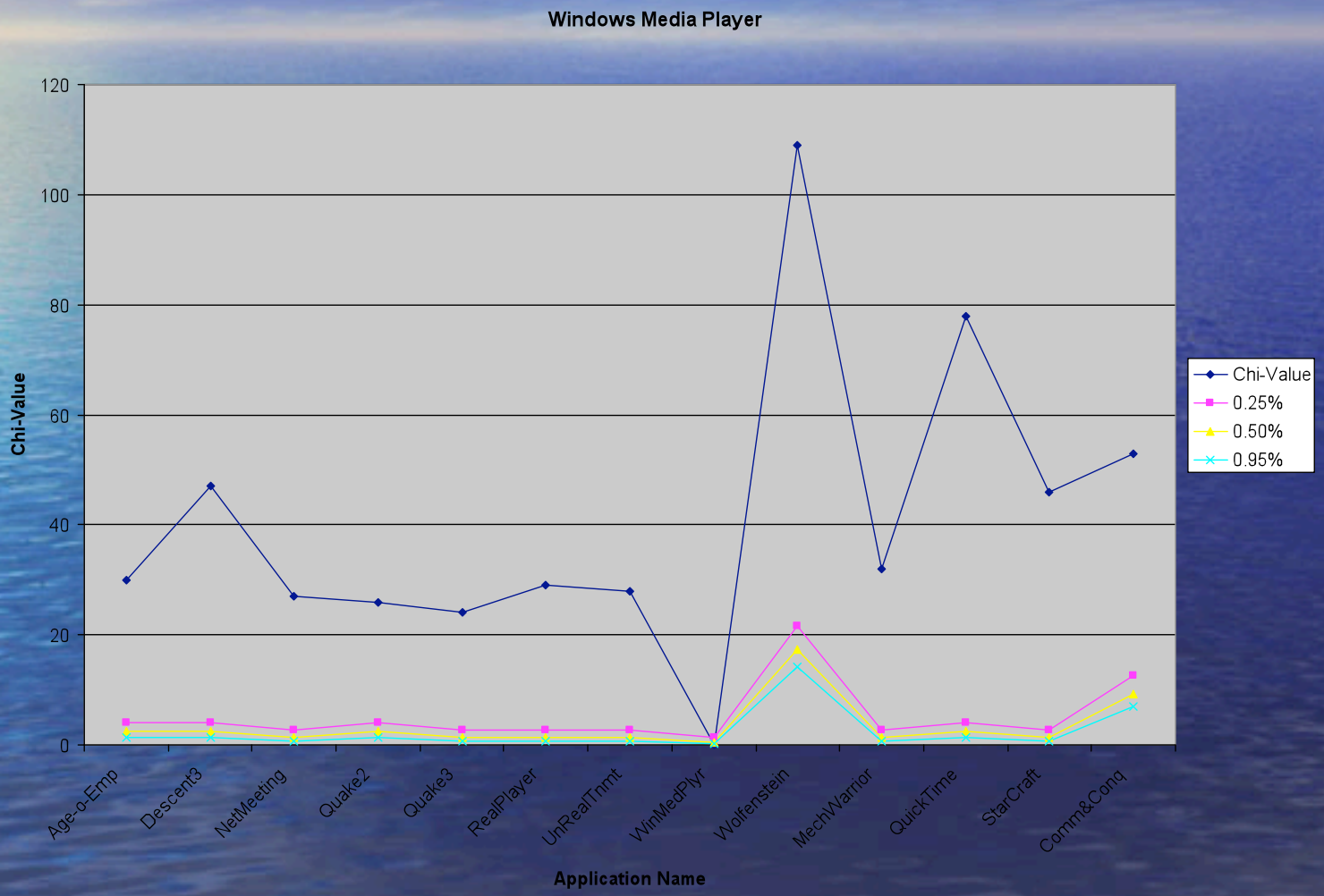
Unreal Tournament

Real Player



Loughborough University

Using Packet Size Distributions



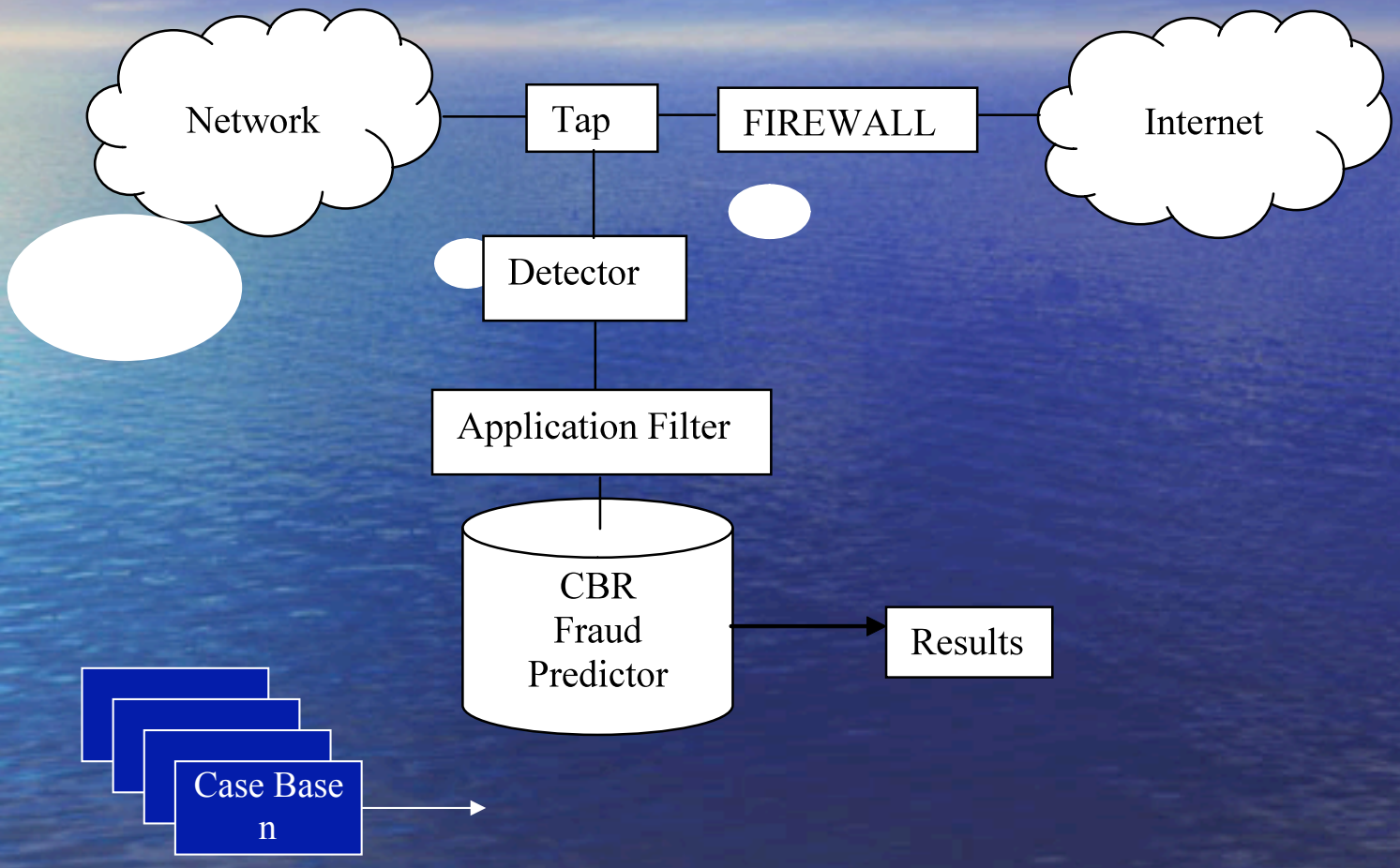
Loughborough University

Identifying Unauthorised Use

- Use Case Based Reasoning
  - Build a "profile" for each user group
- Filter "acceptable" applications at the Detector
- Use CBR to identify known usage

Loughborough University

Outline Solution



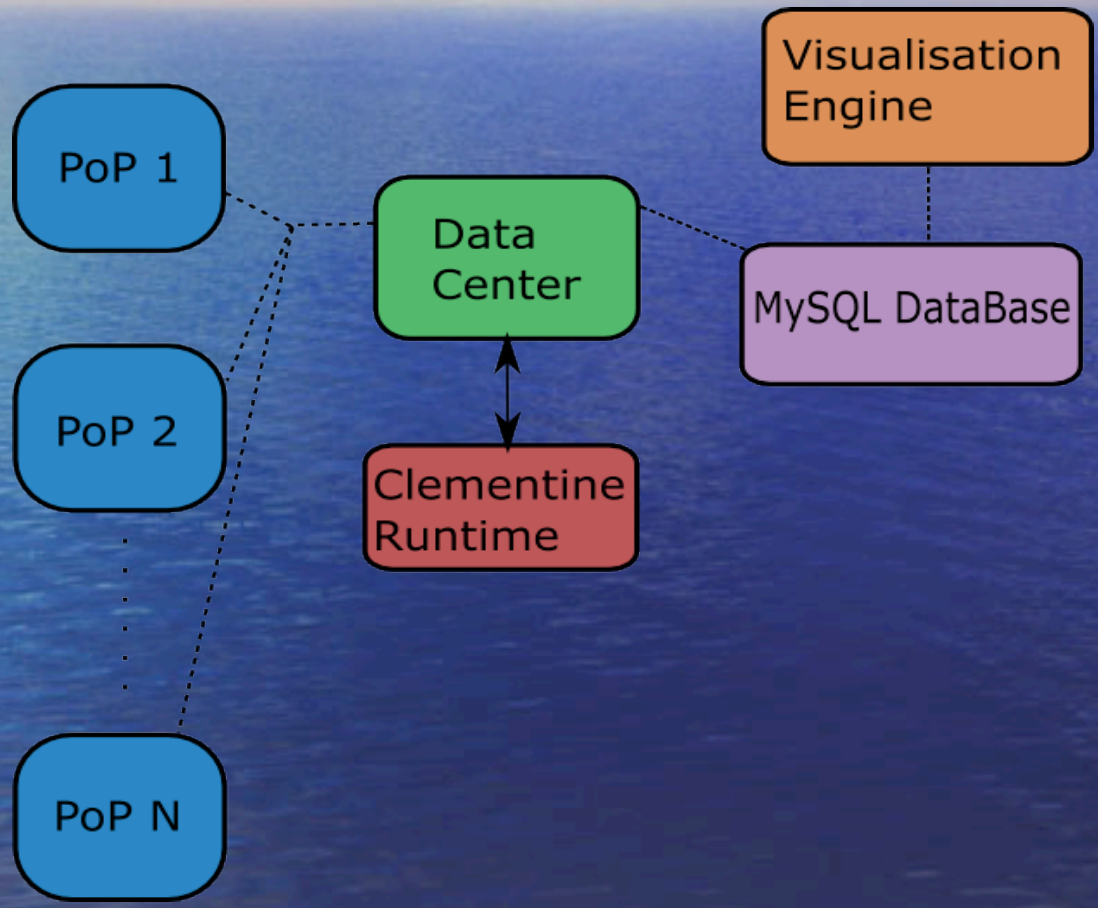
Loughborough University

Detecting Criminal Activities in the Internet

- Identify illegal activity inside the network core
  - Sometimes Necessary
  - Some prevention best done here
  - Use statistical traffic summaries of headers to identify anomalies using Data Mining
    - Processing Overhead
    - High Throughput
    - No user data

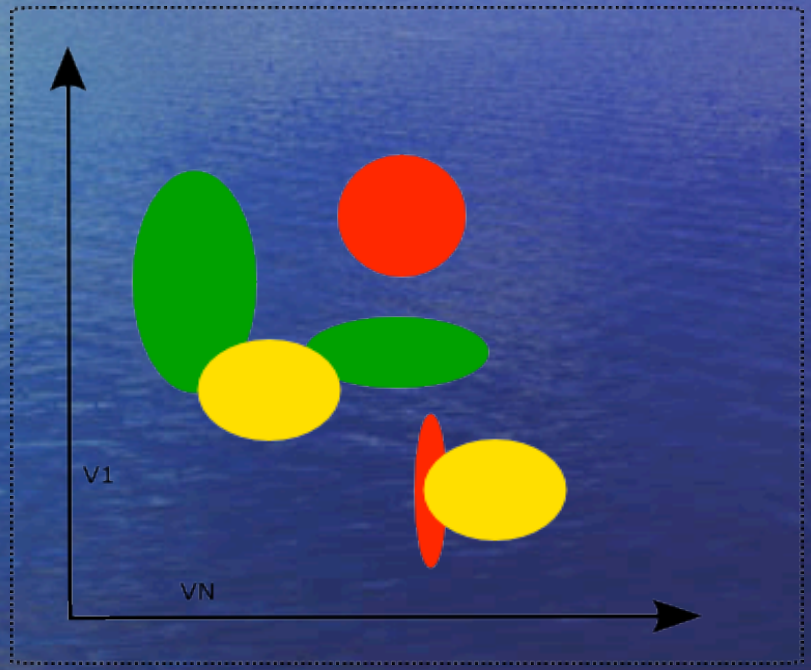
Loughborough University

Overall System Concept



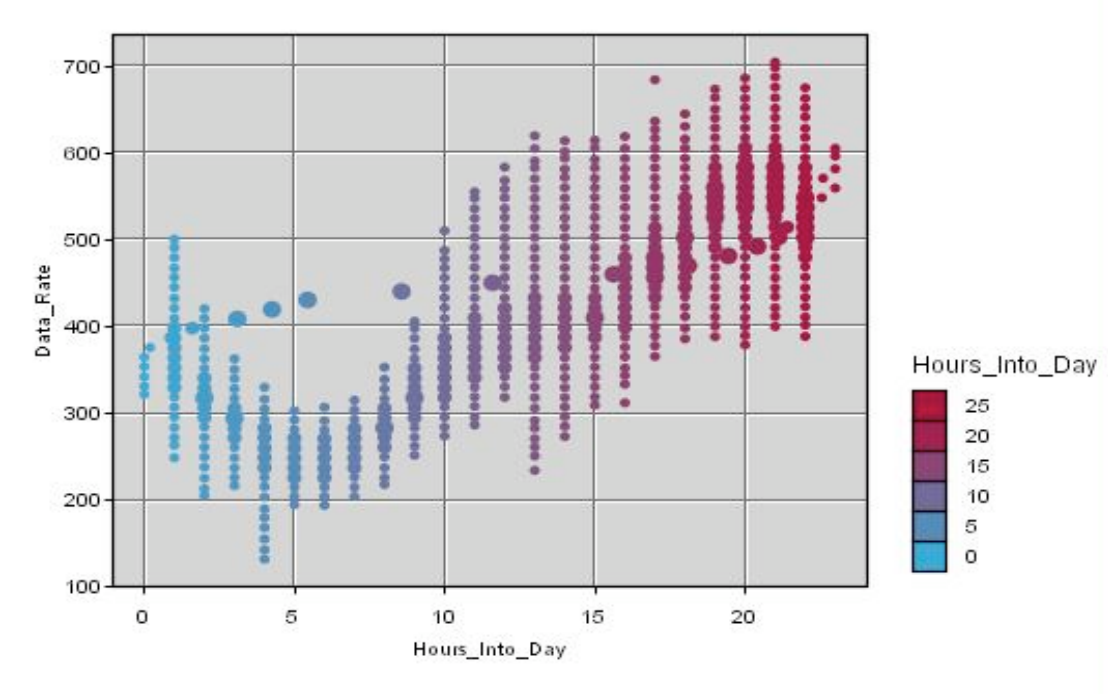
Loughborough University

Anomaly Approach

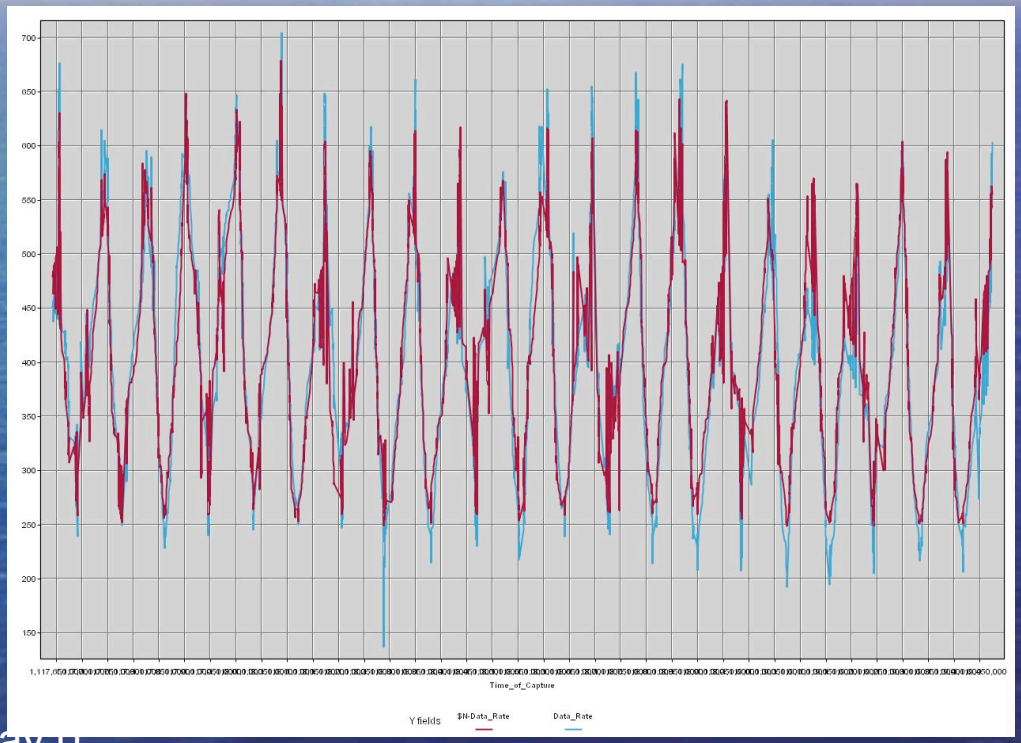


Loughborough University

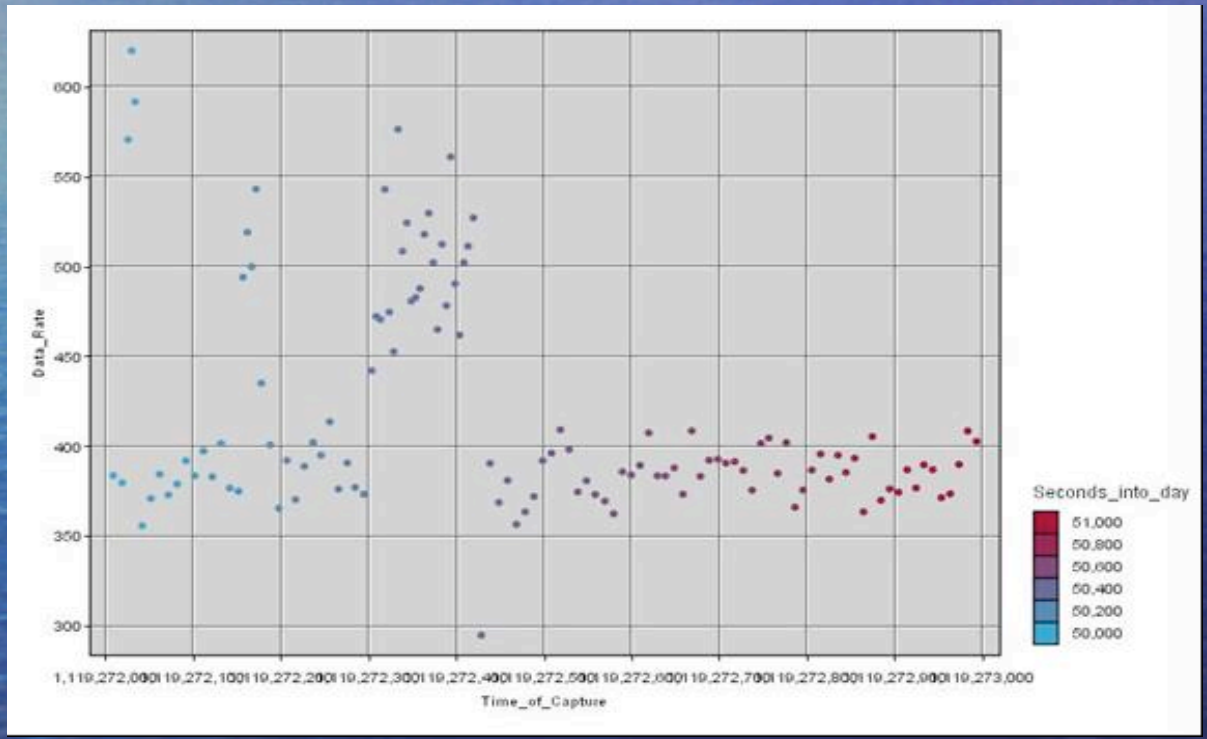
Data Rates



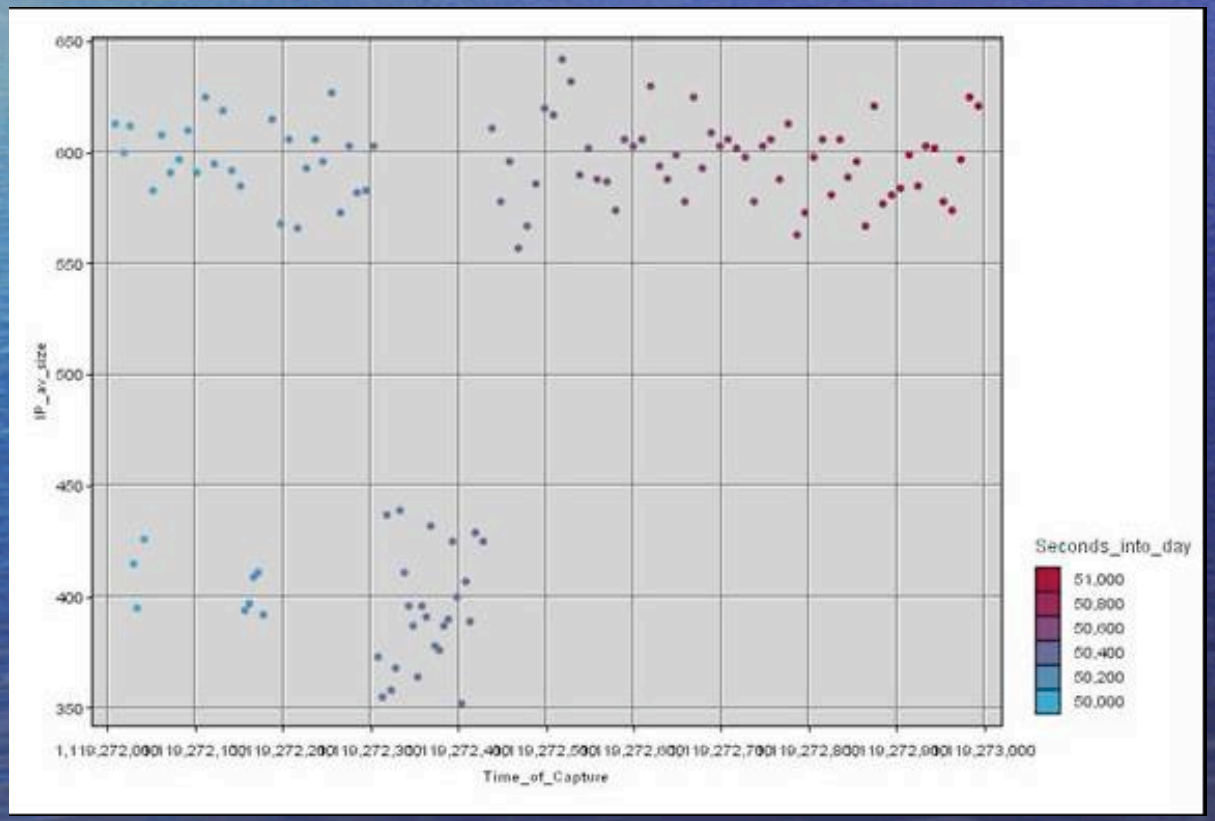
Model of Data Rate



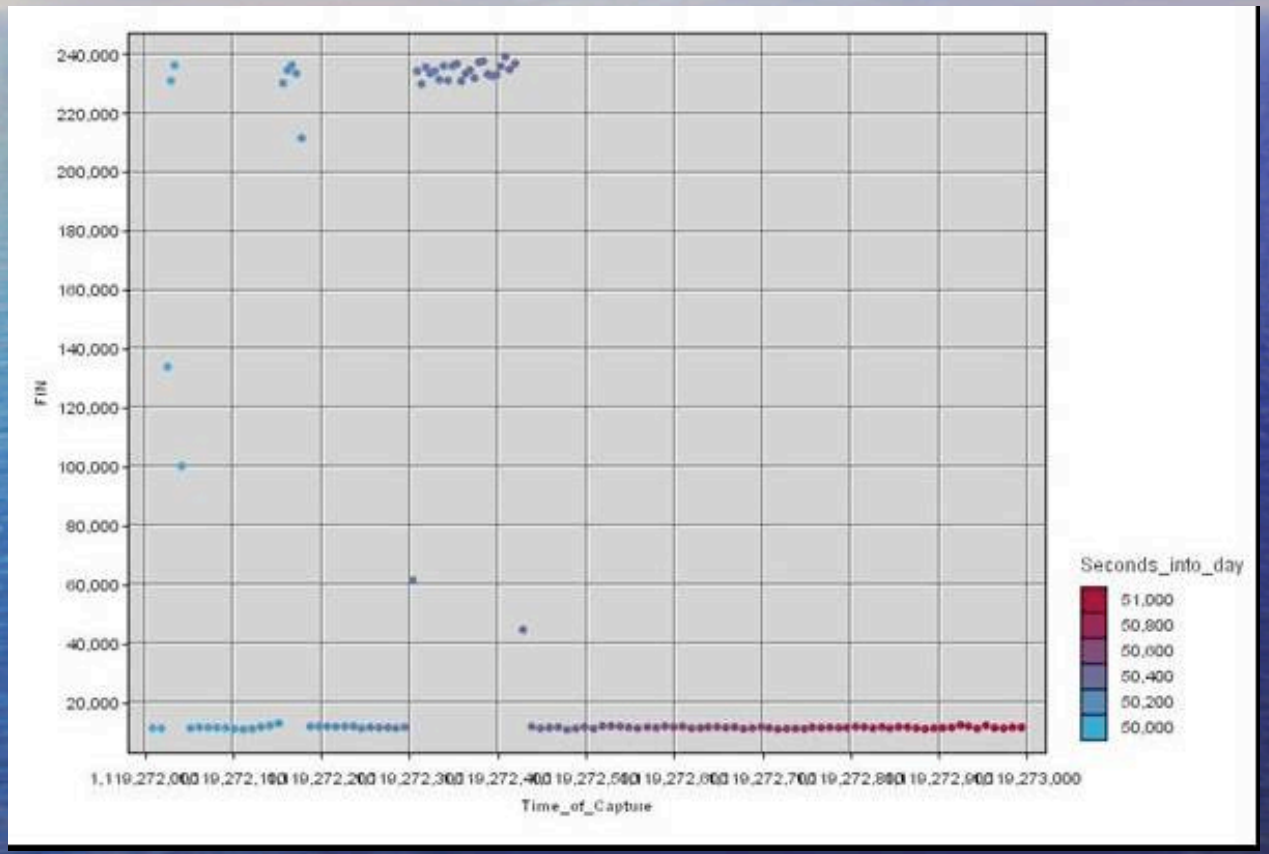
Anomaly Example – Data Rate



Anomaly Example – Average Packet Size

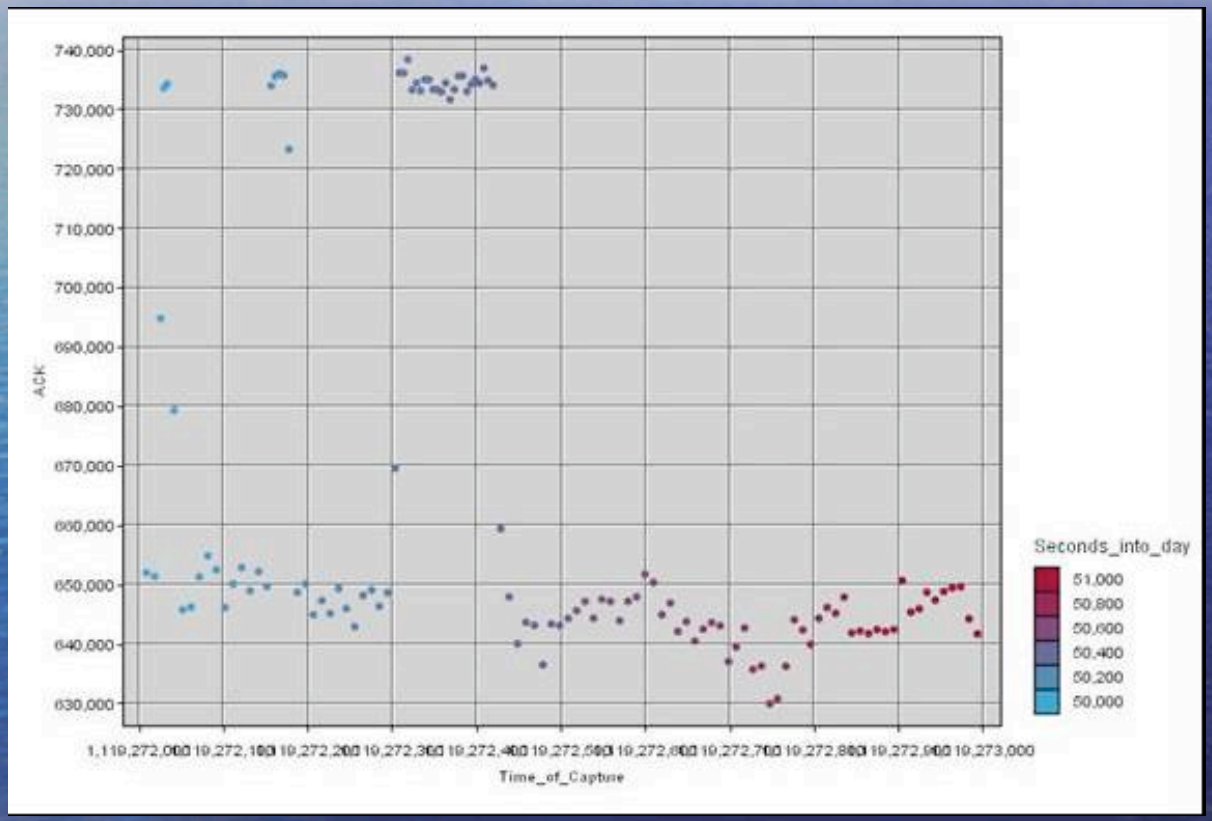


Anomaly Example – FIN Count

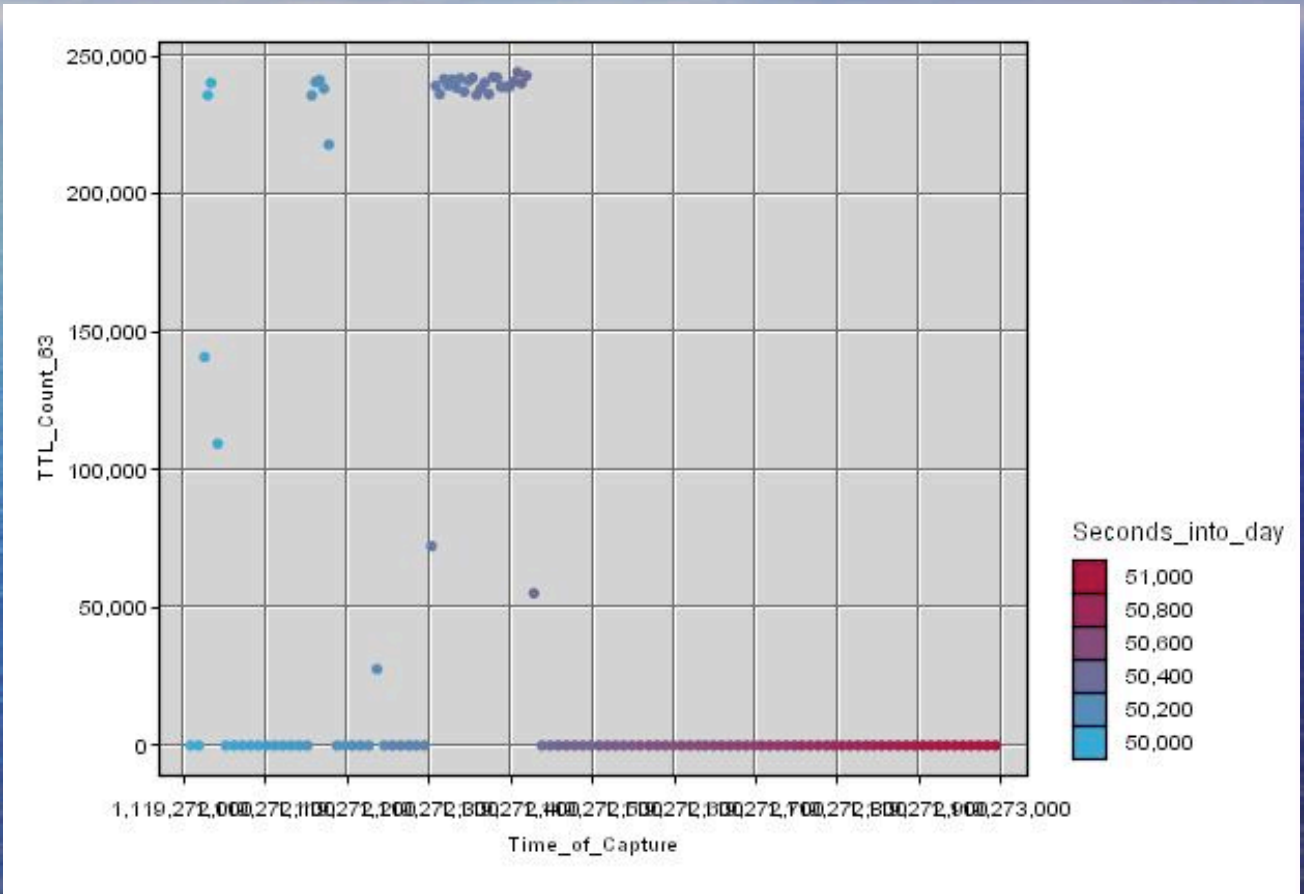


Loughborough University

Anomaly Example – Ack Count



Anomaly TTL - 63



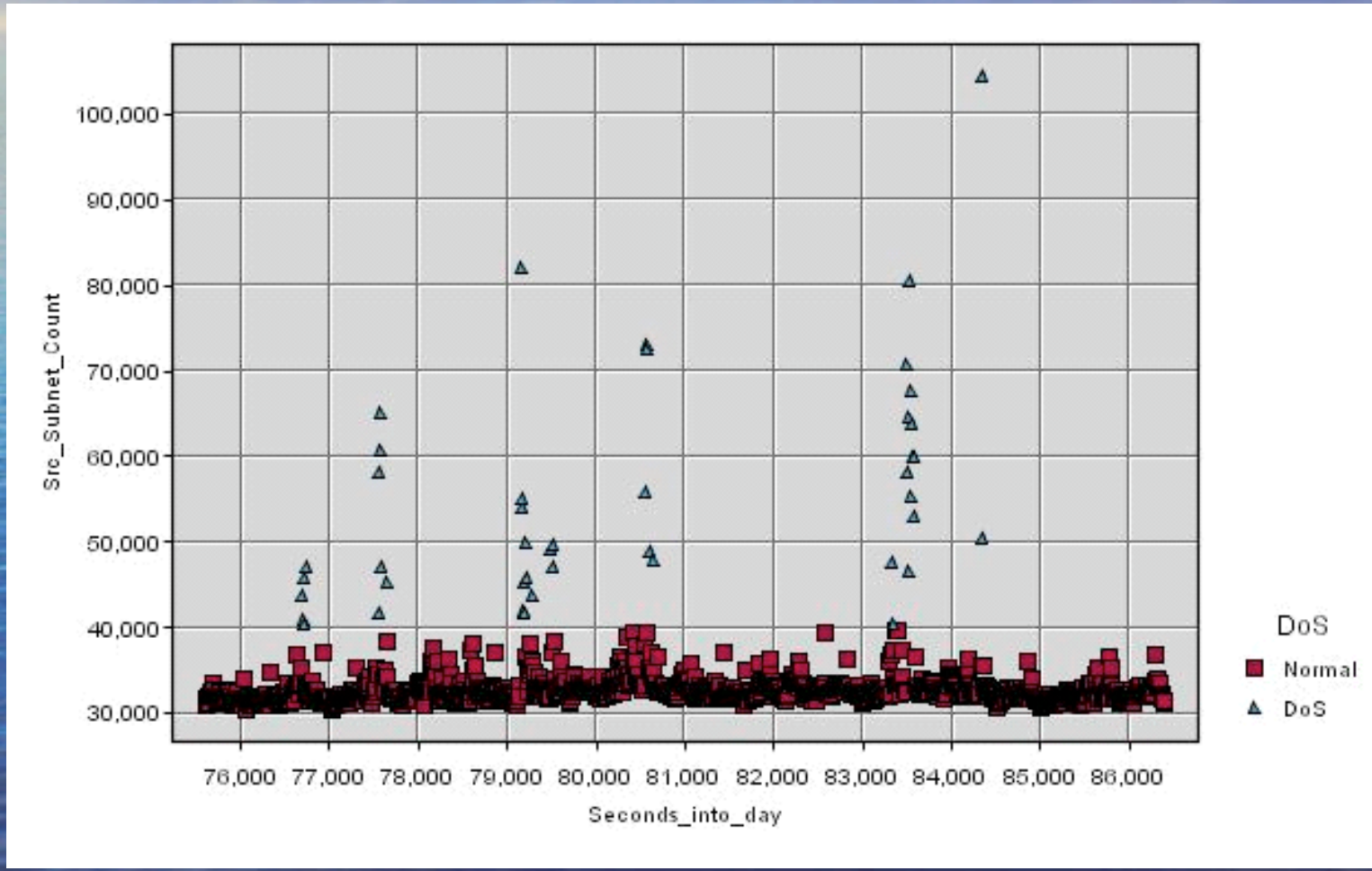
Loughborough University

Header Significance for Detection

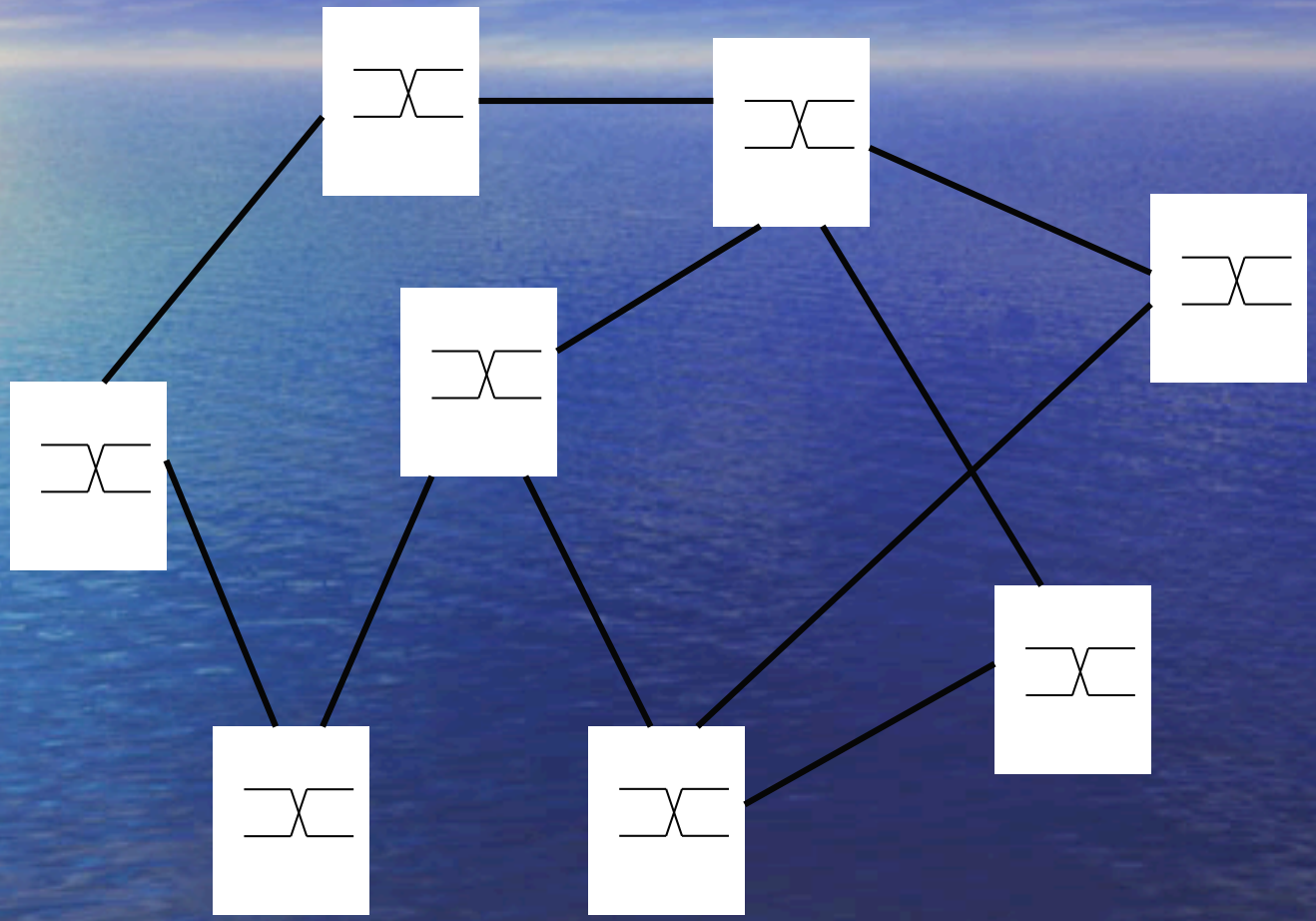
Input Field	*Value*
Values of most common packet sizes	1
ID Ratio	0.85
TTL Field	0.45
TCP Flags	0.30
Average Packet Size	0.23
IP Address Counts	0.20
Frequency of most common packet sizes	0.17

Loughborough University

DDoS Abnormalities



Concept for Reducing Energy Usage



Issues to be Tackled (1) Technical

Loughborough University

- How do we collect the required measurement data?
  - Dealing with data rates
  - Dealing with volume
  - Dealing with location
- How do we store and access the data?
  - Dealing with volume
- What forms of processing should be used?
  - To extract maximum value
  - At the lowest cost

Issues to be Tackled (2) Legal

Loughborough University

- Data Security
  - Must be anonymous
  - Yet contain sufficient richness
  - And processing must be manageable
- Access
  - Legal Agreements
  - Acceptable use defined for all parties

Issues to be Tackled (3) Financial

Loughborough University

- Financial
- Funding the Research
  - Instrumenting a network
  - Developing the mechanisms and algorithms
- Making a Business case
  - Upfront costs
  - Savings on security/management/fault detection/energy efficiency
  - Overall Savings

Loughborough University

Conclusions

- Network Performance Measurement Reuse could answer many of the problems facing communication networks today.
- MUST be holistic to achieve maximum benefits.