Anomaly Detection in Communication Networks

Prof. D. J. Parish

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

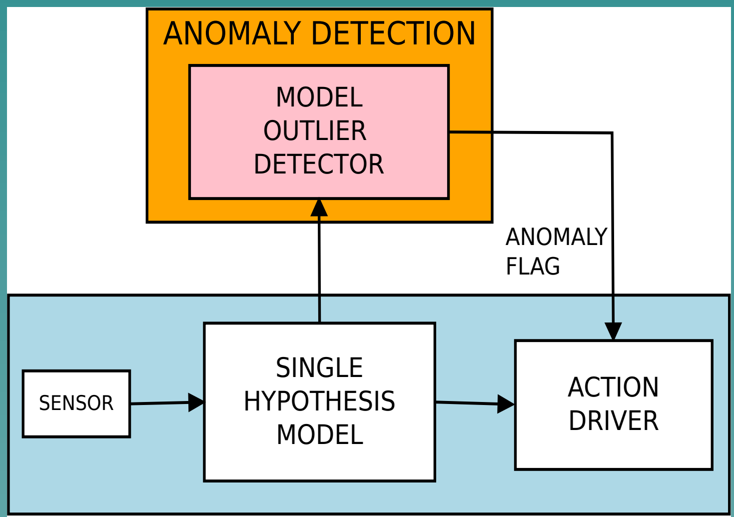
Loughborough University

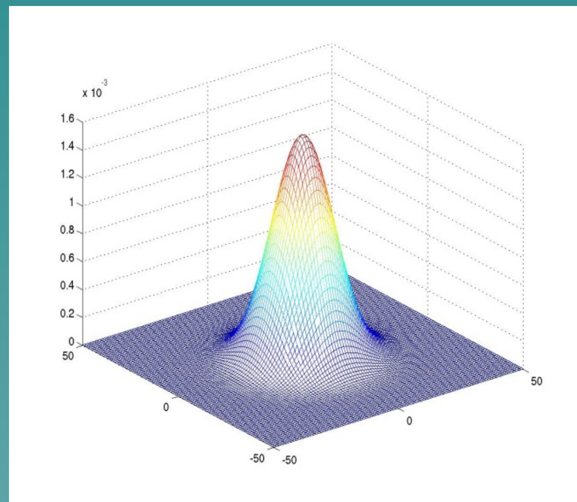
Overview

- Introduction
- Background
- What is an anomaly in the context of a communication network?
  - Network Traffic Characteristics
  - Intrusion Detection
  - Exception Detection
- Anomaly detection approaches.
  - Rule Based
  - Window Based
  - KS Statistic
  - Others
- Performance Metrics
- Examples
- Summary

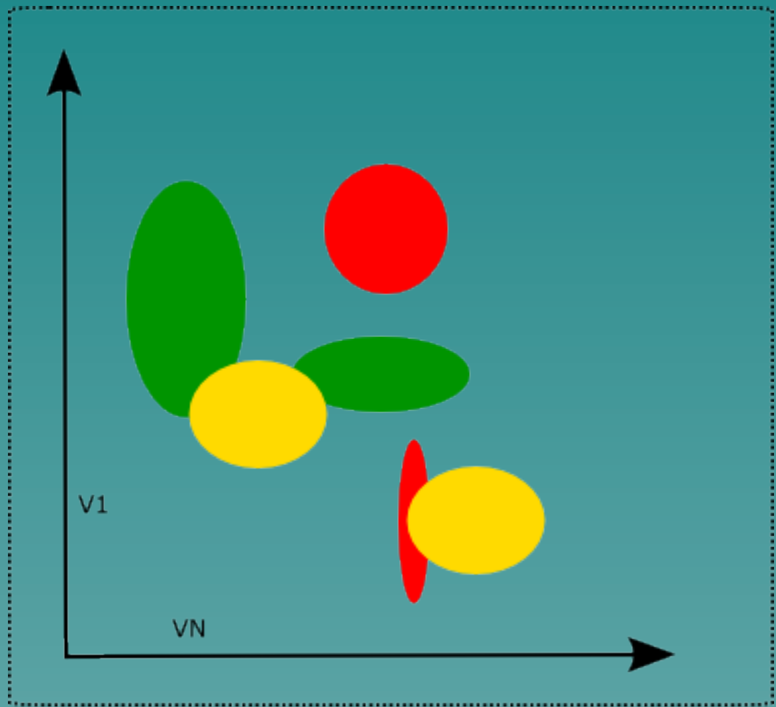
Classical Model

- *Anomaly* - unusual event
- *Conventional mathematical model*
  - Outlier of a distribution
  - Empirical distribution deviates from the model distribution





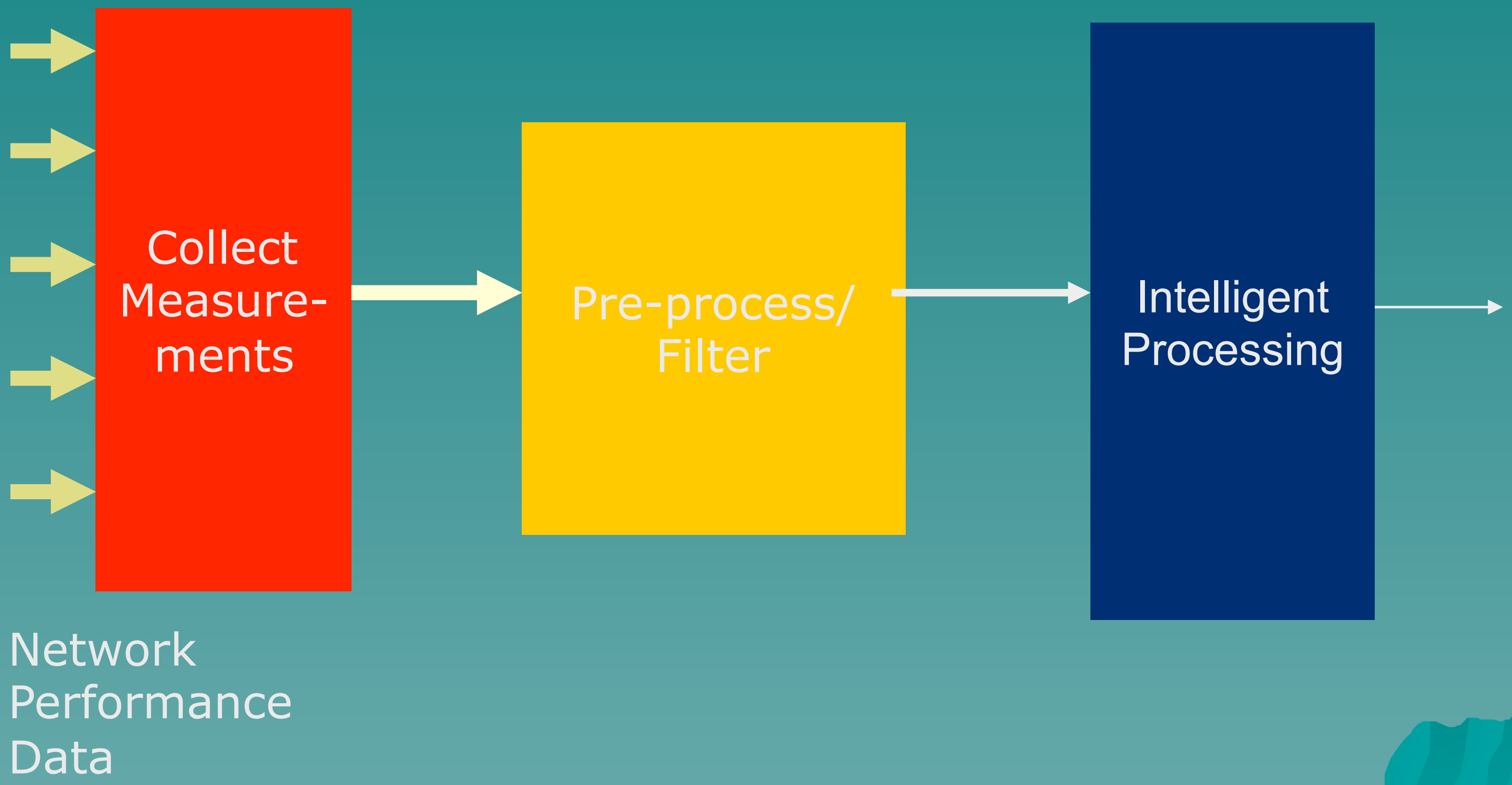
Anomaly Approach



Common Problems

- Collecting the data
  - Source, location, number
- FPs, FNs,
- Learning Normal
- Identifying a Change
- Updating

Generic Approach



Types of Anomalies in Communication Network Data

- Performance related Data.
  - Delay, Throughput, loss, Faults, Routing Changes
- Security related.
  - Intrusions; Misuse(?), DDoS
- Content related.
  - Application usage, Data Type/Content

Network Traffic Characteristics

- Bandwidth – Average, Peak etc.
- Delay – Absolute and Variance.

The end-to-end delay of a packet can be given by:

$$D + W.$$

Where D is a fixed element of delay and W is a variable element of delay.

The inter-arrival time of two packets at a receiver can be given by:

$$\text{Delta} = (D + W[1]) - (D + W[2])$$

- Loss.

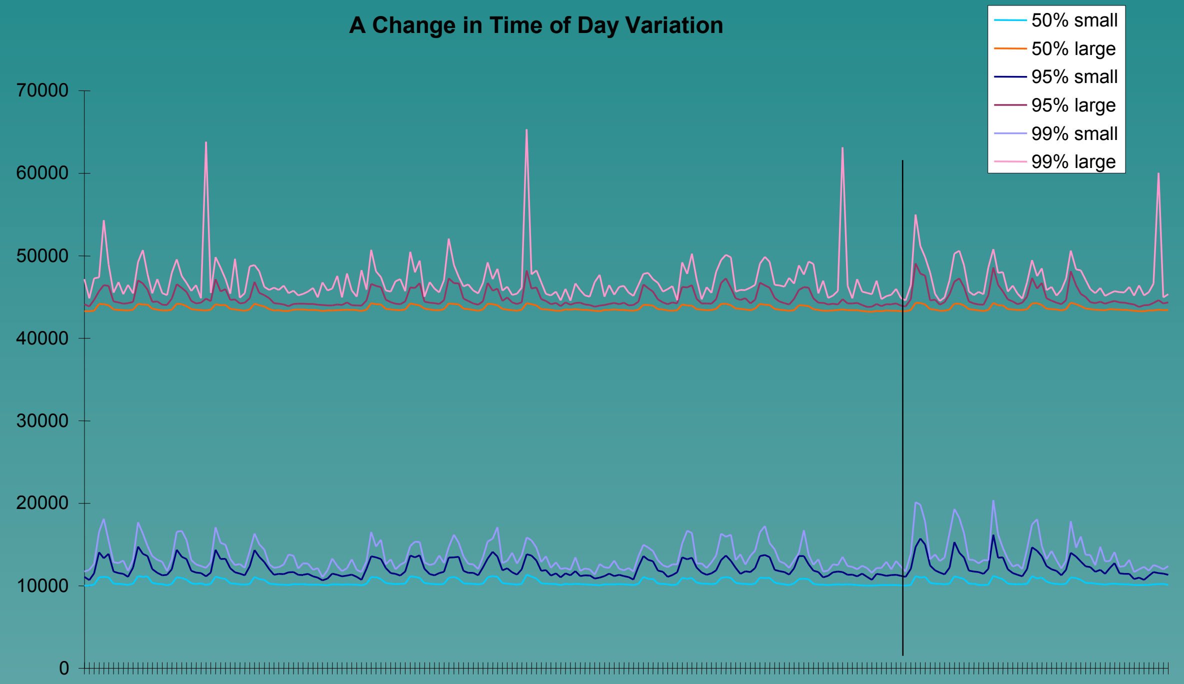
Anomalies in Network Traffic Measurements

Loughborough University

- Results used to provide delay and loss measures for BT Operations.
- Identifies changes in performance- termed Exceptions.

Example Data Exception- Step

Example Data Exception- Time of Day Delay Variation



Intrusion Definitions (Computer)

Loughborough University

"An incident of unauthorized access to data or an automated information system"

"To compromise a computer system by breaking the security of such a system or causing it to enter into an insecure state"

- A Active Process in which various aspects of a computer and network system are monitored and analysed for evidence of intrusion
- Passive elements needed as well for prevention such as checking password strength etc.

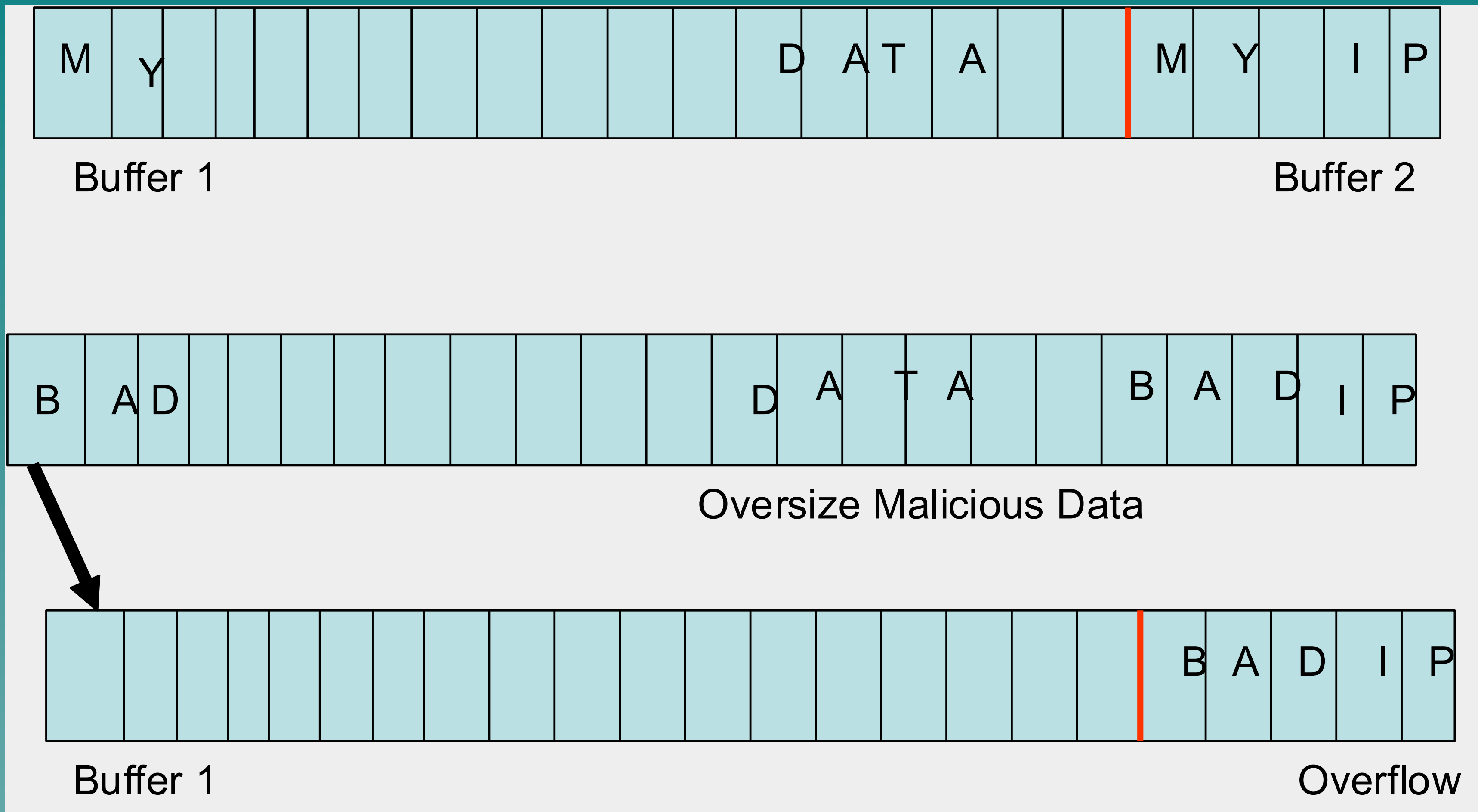
IDS Characteristics

CHARACTERISTIC	DEFINITION	CATEGORY
Source of Information	Defines from where the information used by IDSs is gathered.	Network-based
		Host-based
		Router-based
Learning Approach	Defines how IDSs learn the difference between normal and malicious information.	Supervised
		Unsupervised
Detection Systems Cooperation	Defines the level of cooperation between different IDSs.	Autonomous
		Cooperative
Cooperative Systems Deployment	Defines the way cooperative IDSs share the information.	Centralised
		Hieratical
		Distributed
Detection Timing	Defines how long takes to implement the intrusions detection.	Off-Line
		On-Line
Detection Methodology	Defines the methodology utilised to implement the intrusions detection.	Misuse
		Anomaly
		Hybrid

How can Intrusion Occur?

- Often Two Phases:
  - 1. Penetration
    - Trojan via Email
    - Worm via an Open Port
  - 2. Exploitation
    - Compromising the Target via an Exploit
    - Buffer OverFlow Example

Buffer OverFlow Attack



Loughborough University

Identifying Anomalies in Communication Networks

- Rule Based (Misuse Detection)
- Window Based Algorithms
- KS (Kolmogorov–Smirnov) Statistic
- Data Mining (including Clustering Algorithms)

Detecting Intrusion

- Two Fundamental Approaches:
  - Rule Based (E.g. Snort)
  - Free ID software
  - Windows, Linux

  - Anomaly Based:
  - Often uses AI algorithms including
  - Baysian Belief, ANN, GA, Data Mining,
  - Case Based Reasoning

Rule Based IDS

- Snort: (from http://www.snort snort)

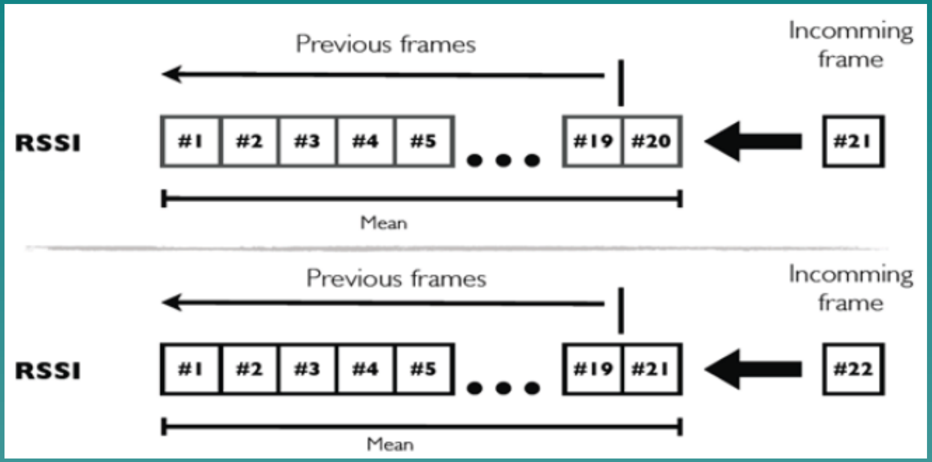
"Snort can perform protocol analysis and content searching/matching. It can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, and much more. It uses a flexible rules language to describe traffic that it should collect or pass, as well as a detection engine that utilizes a modular plug-in architecture"

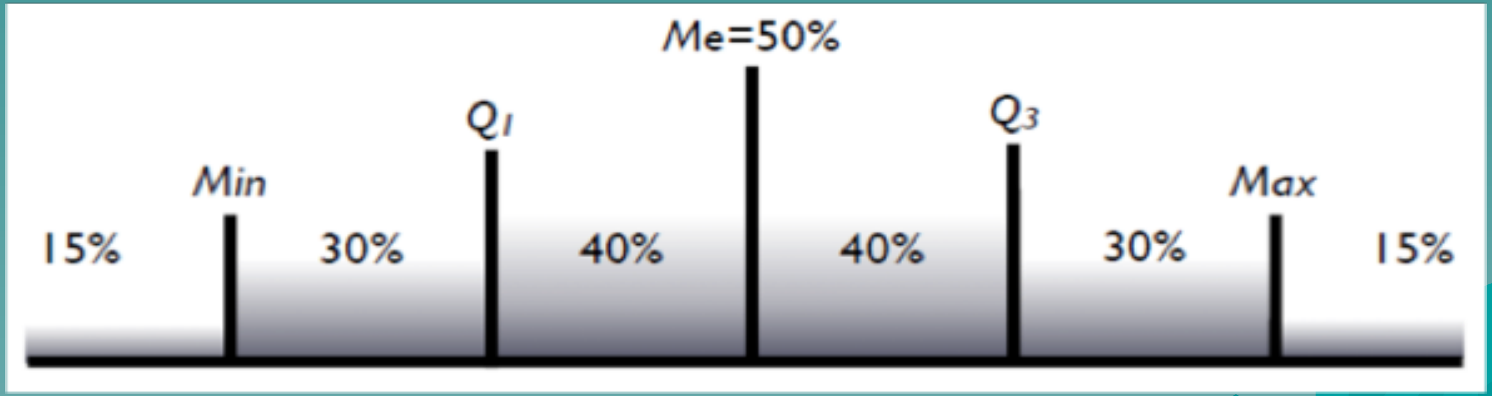
Example Snort Rules

```
alert tcp $TELNET_SERVERS 23 -> $EXTERNAL_NET any (msg:"TELNET Attempted SU
➡from wrong group"; flow:
   from_server,established; content:"to su root"; nocase;
➡classtype:attempted-admin; sid:715; rev:6;)
```

- The variable $TELNET_SERVERS is defined in `snort.conf` file and shows a list of Telnet servers.
- Port number 23 is used in the rule, which means that the rule will be applied to TCP traffic going from port 23. The rule checks only response from Telnet servers, not the requests.
- The variable $EXTERNAL_NET is defined in the `snort.conf` file and shows all addresses which are outside the private network. The rule will apply to those telnet sessions which originate from outside of the private network. If someone from the internal network starts a Telnet session, the rule will not detect that traffic.
- The flow keyword is used to apply this rule only to an established connection and traffic flowing from the server.
- The content keyword shows that an alert will be generated when a packet contains “to su root”.
- The nocase keyword allows the rule to ignore case of letters while matching the content.
- The classtype keyword is used to assign a class to the rule. The attempted-admin class is defined with a default priority in classification.config file.
- The rule ID is 715.
- The rev keyword is used to show version of the rule.

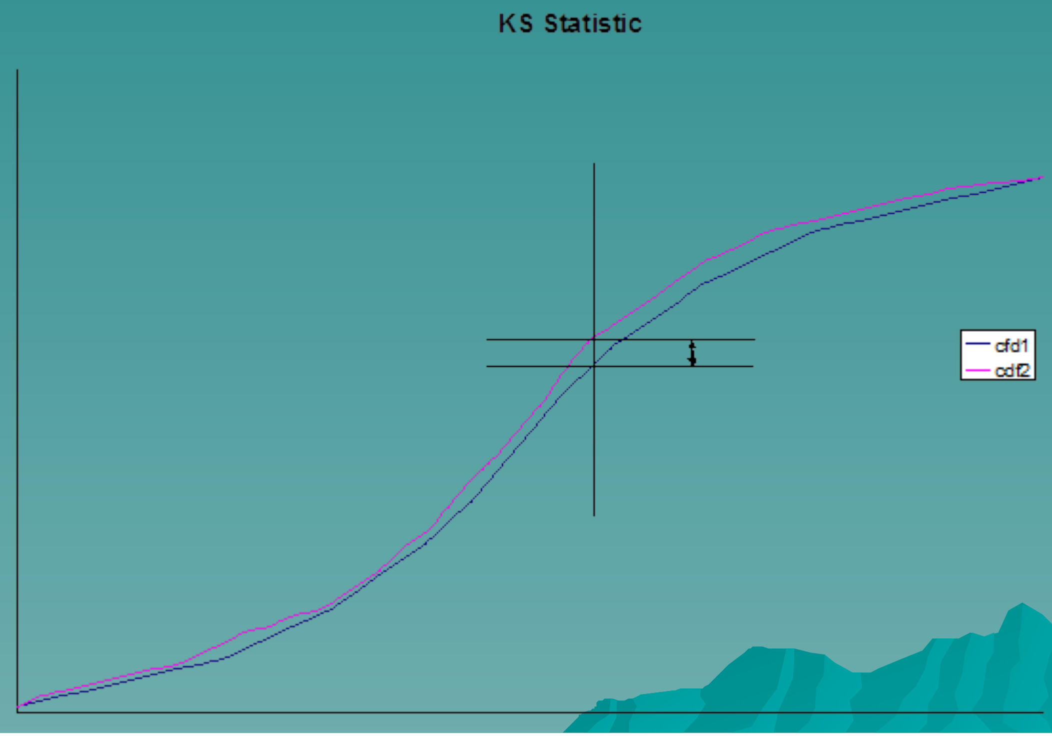
Window Based Approaches





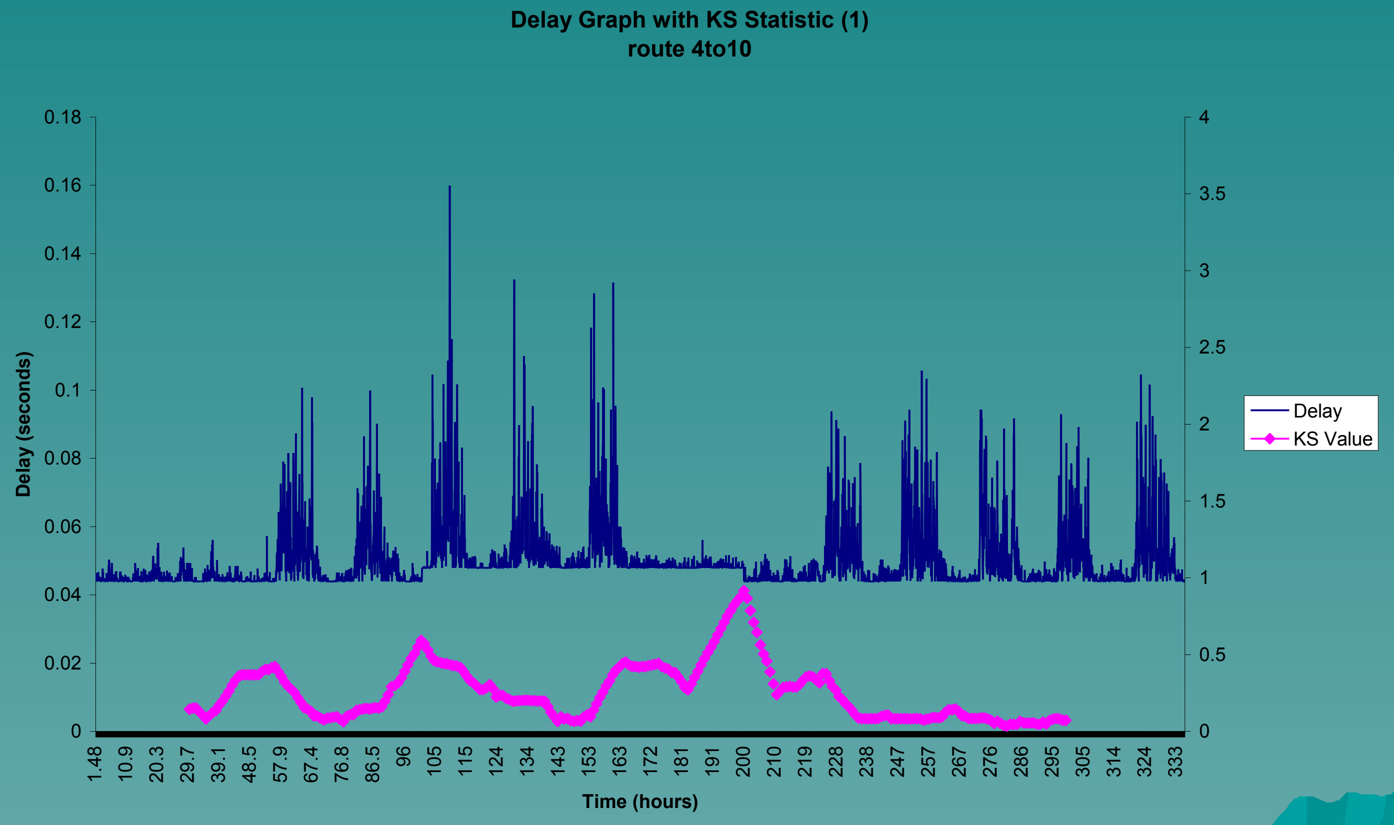
The KS Statistic

- A non-parametric (i.e. Distribution type does not matter) test of similarity between two distributions.

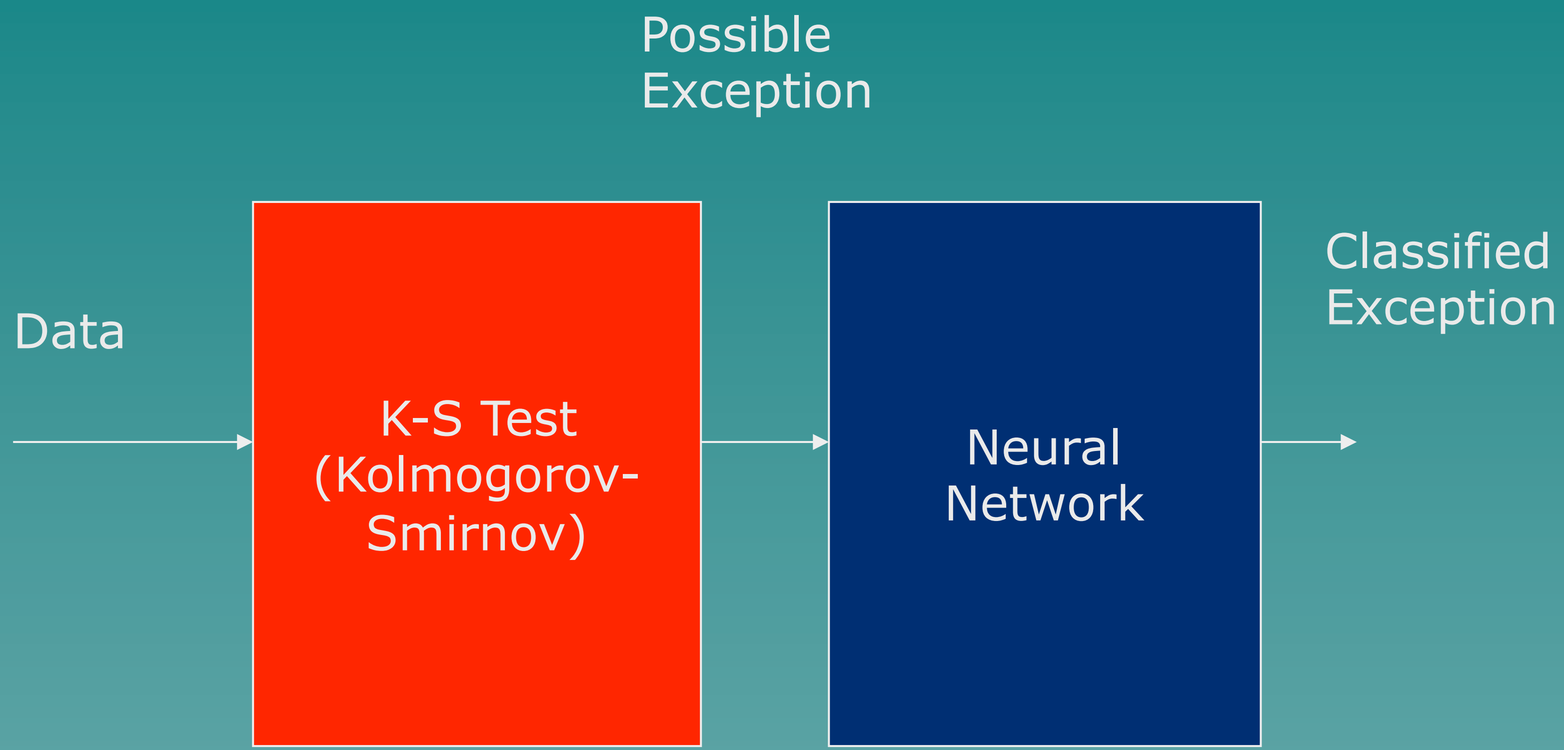


- The Kolmogorov-Smirnov test statistic is defined as
- $D=max1\leq i\leq N(F(Yi)-i-1N,iN-F(Yi))$
- where F is the theoretical cumulative distribution of the distribution being tested which must be a continuous distribution (i.e., no discrete distributions such as the binomial or Poisson), and it must be fully specified (i.e., the location, scale, and shape parameters cannot be estimated from the data).

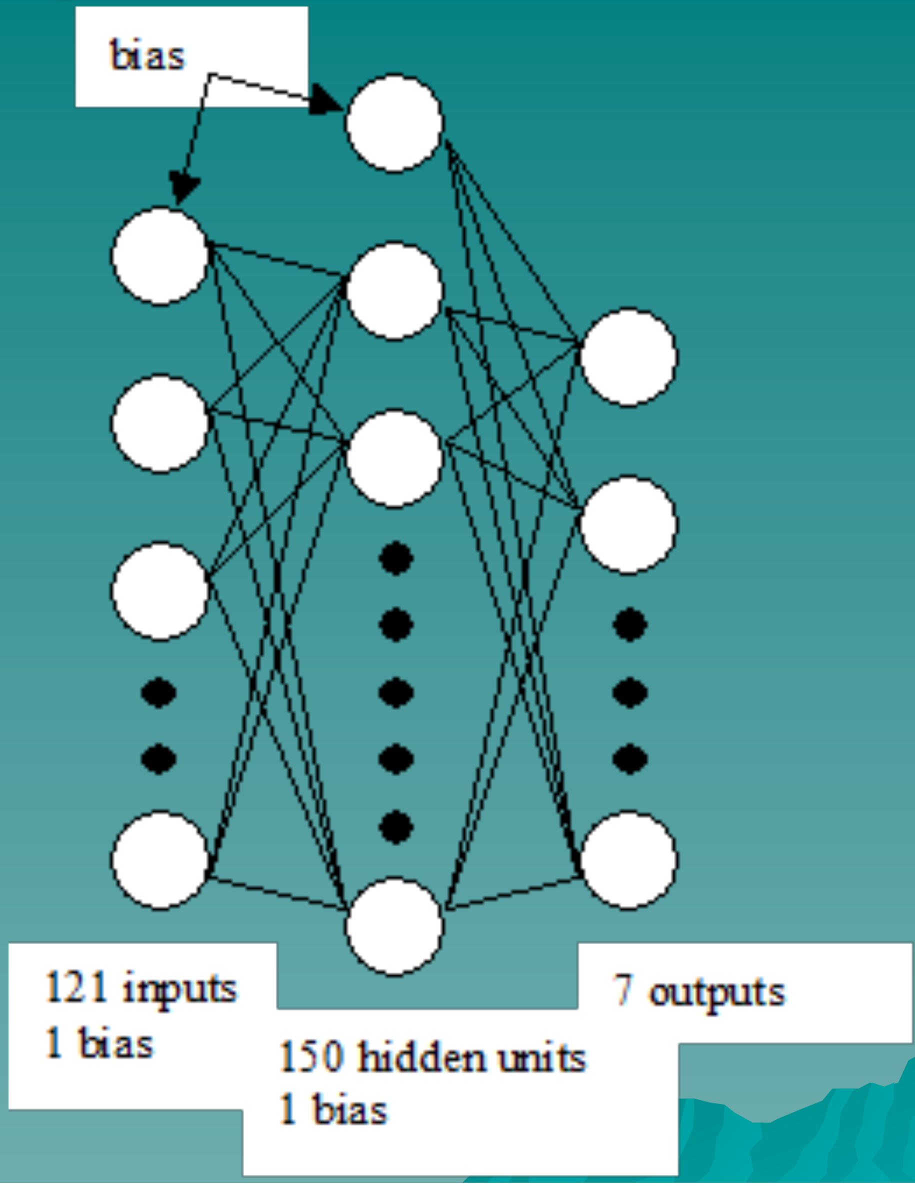
Using the KS Test



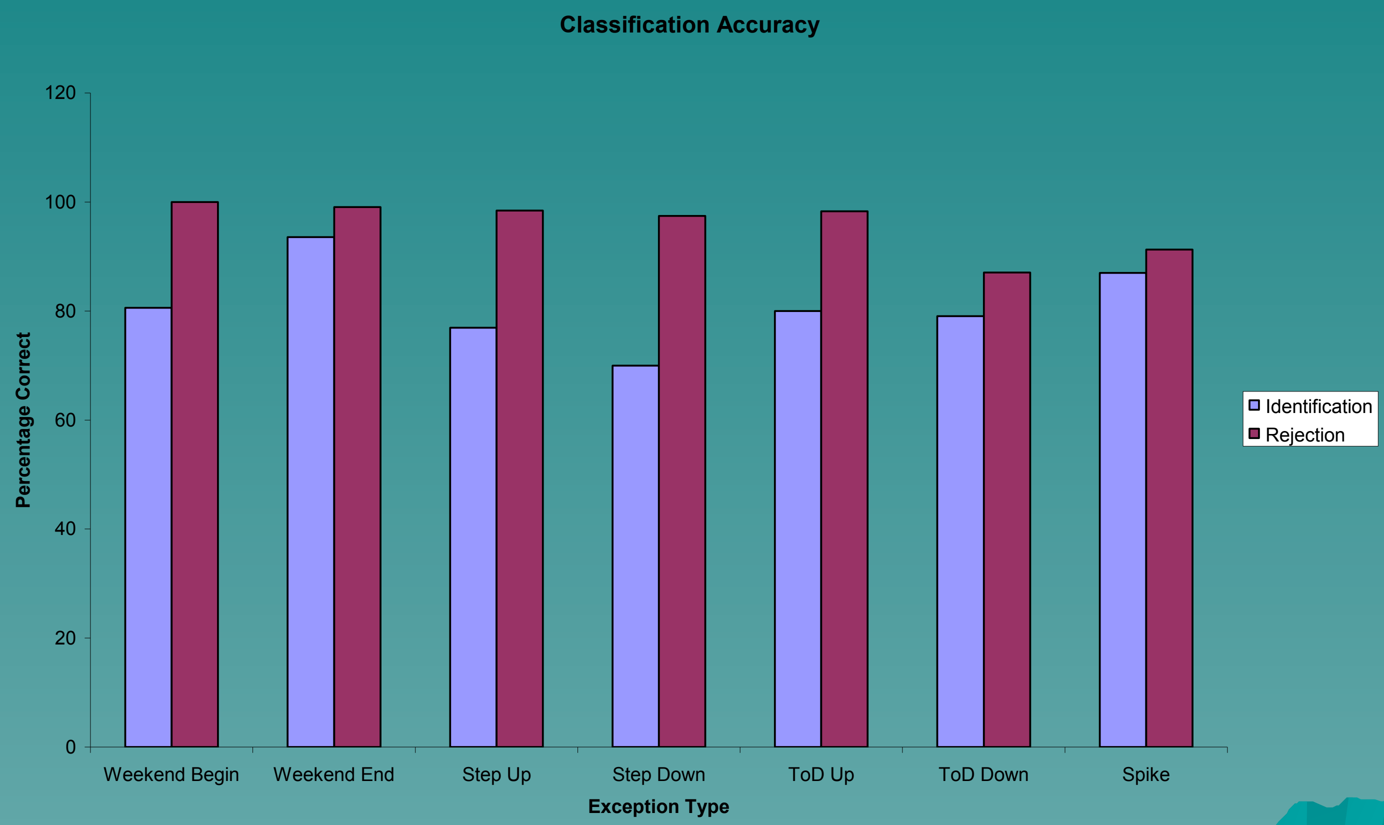
Classifing the Detection



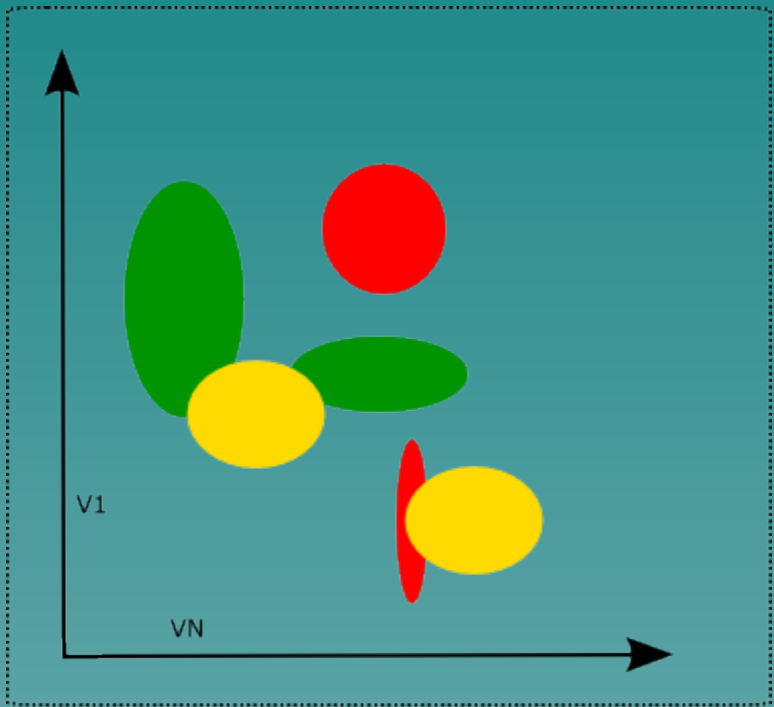
Using a Neural Network



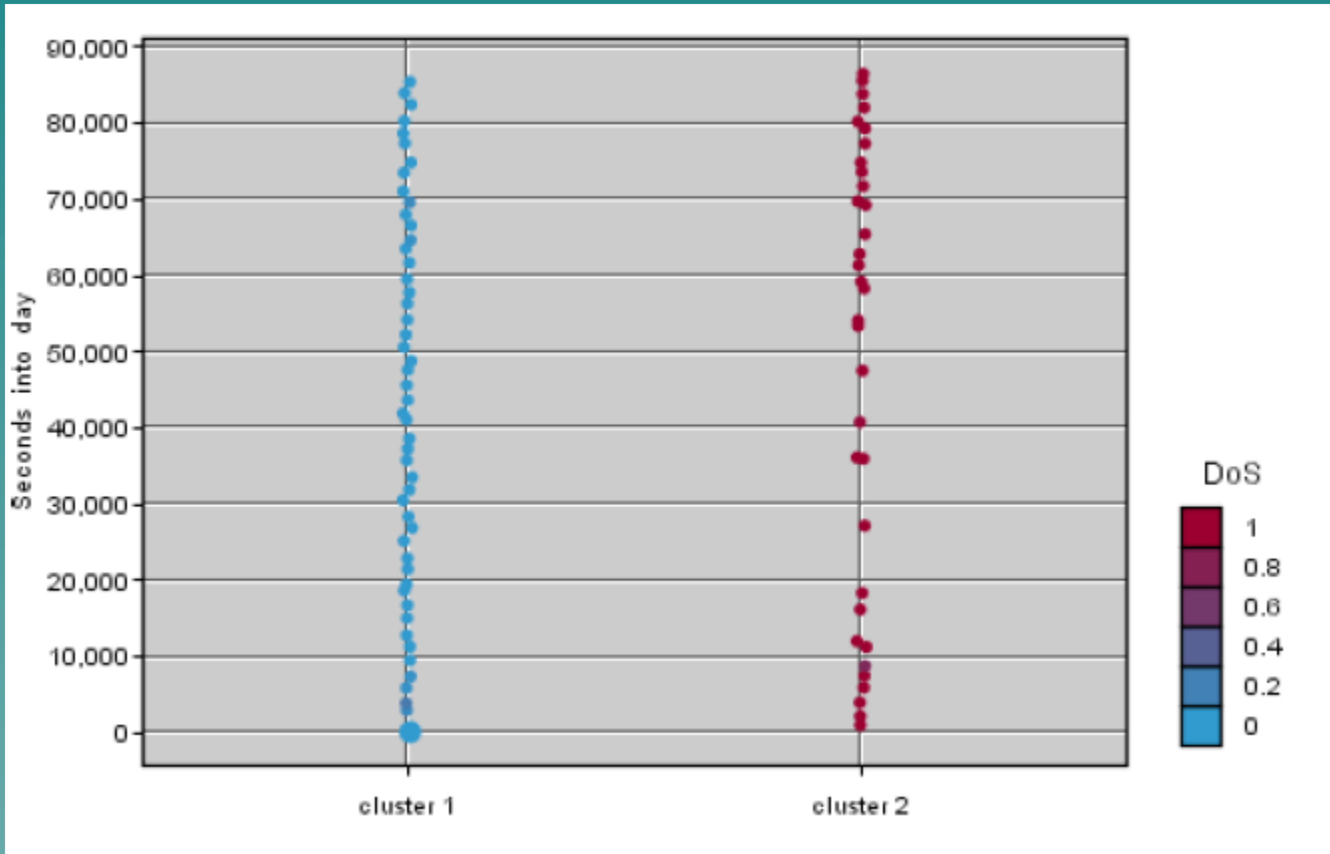
Using a Neural Network



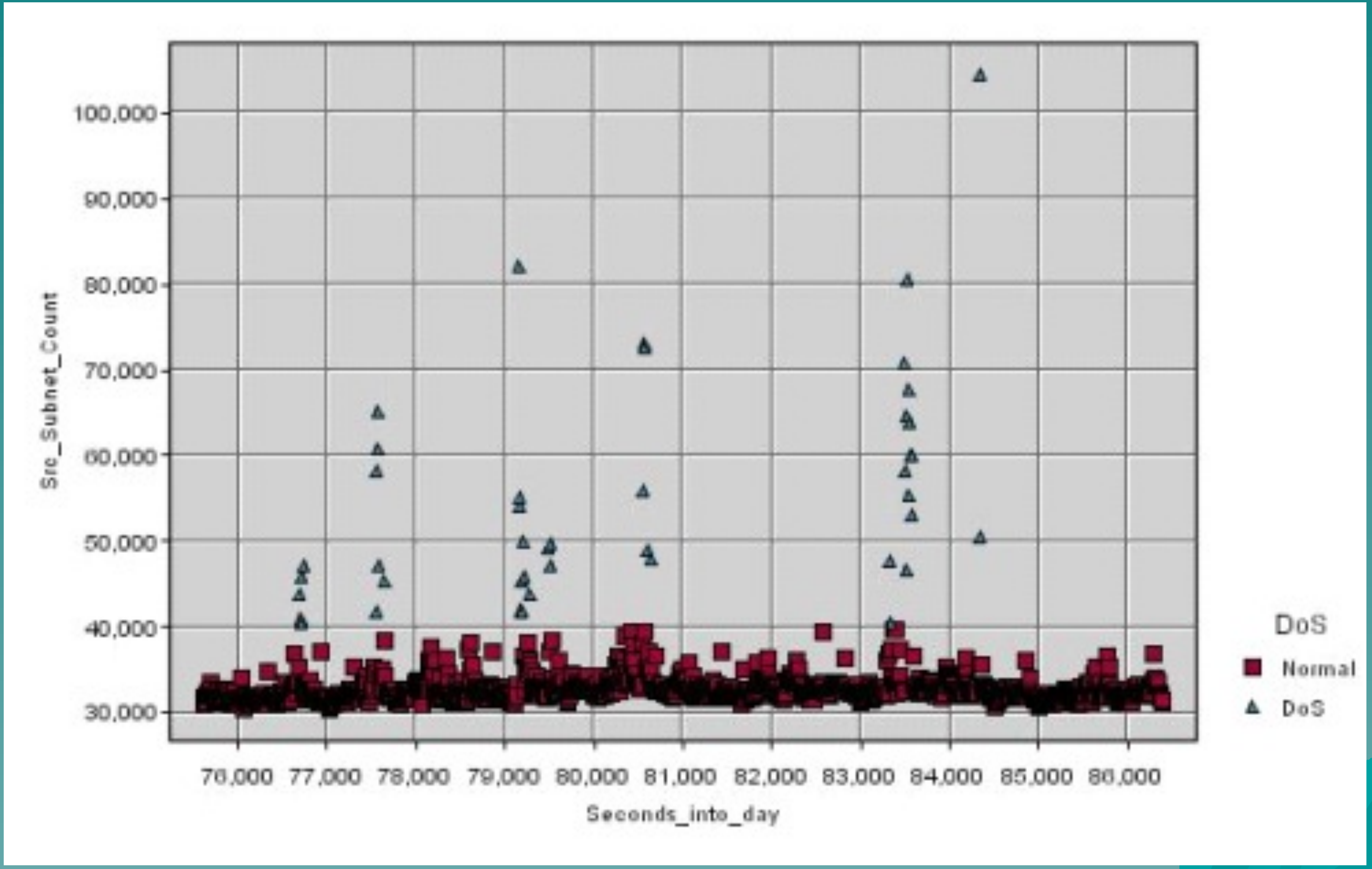
Anomaly Approach Using Data Mining



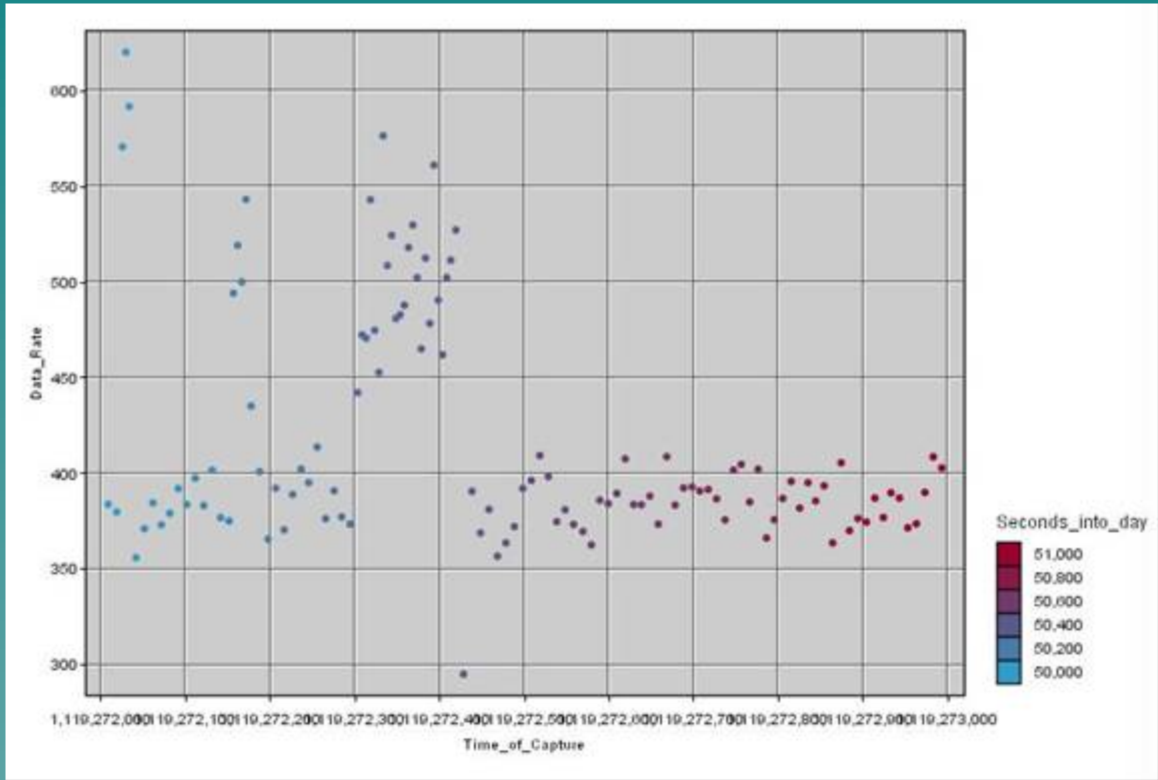
Clustering Algorithm for DoS



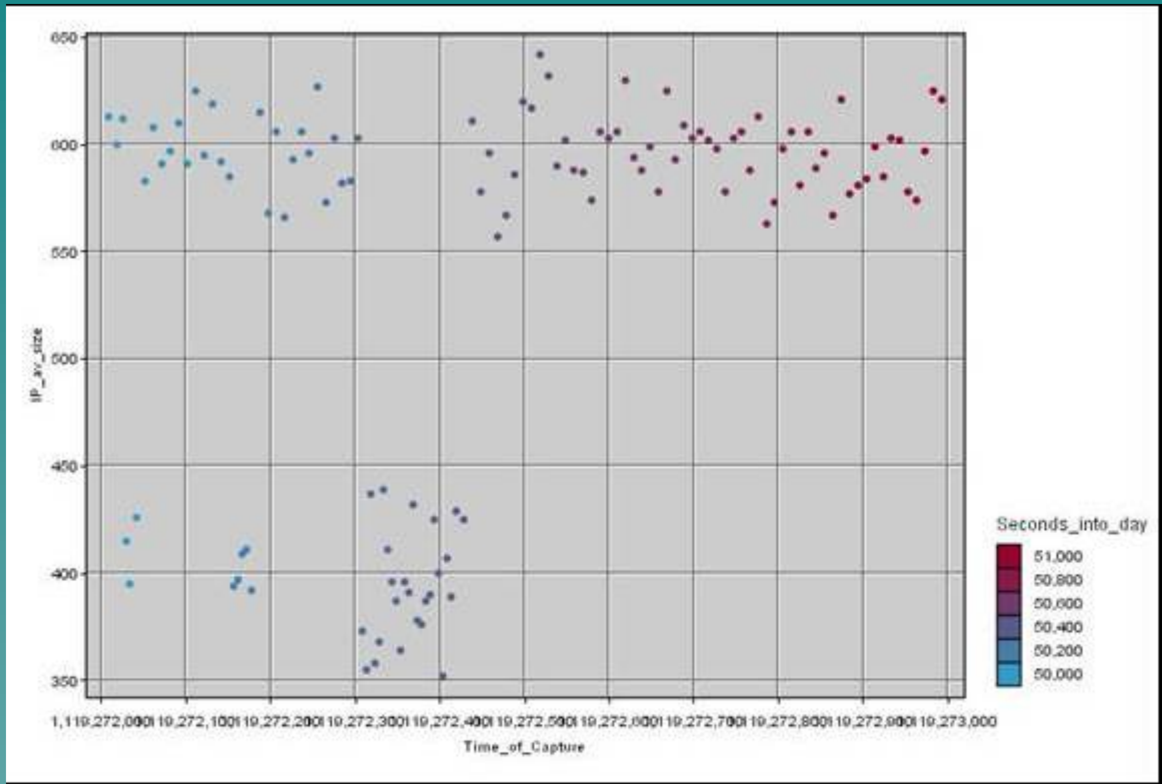
DDoS Abnormalities



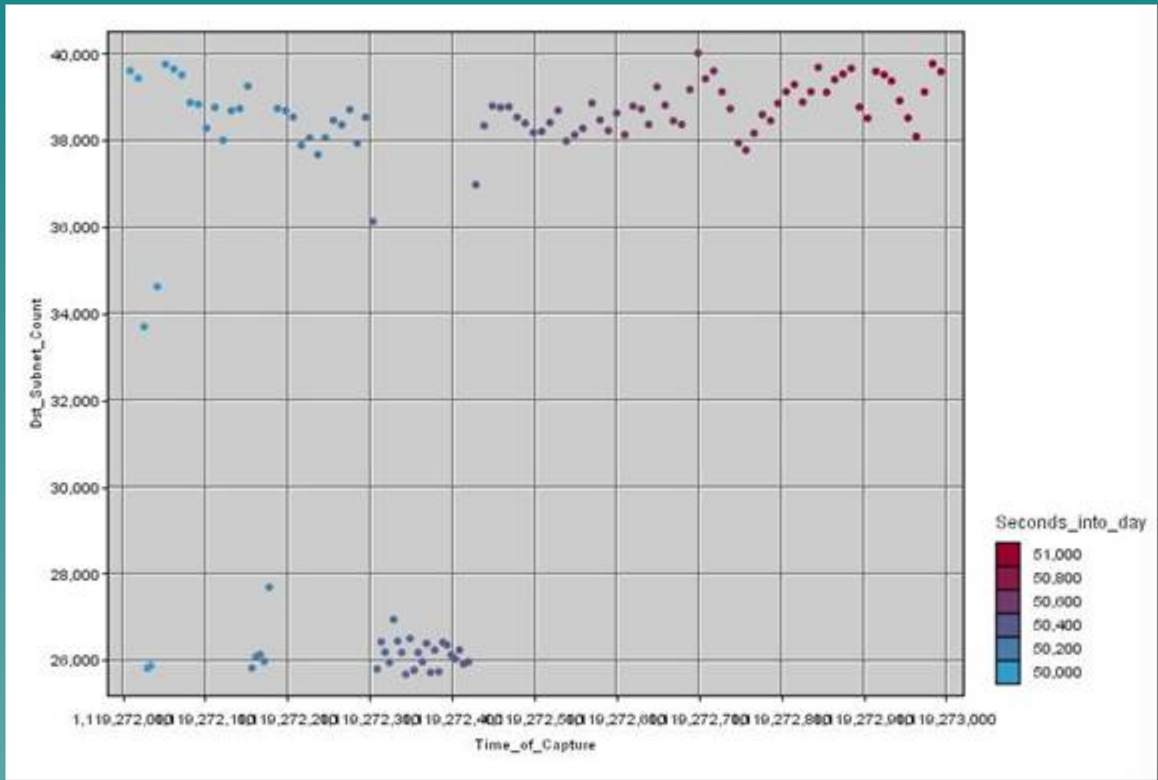
Anomaly Example – Data Rate



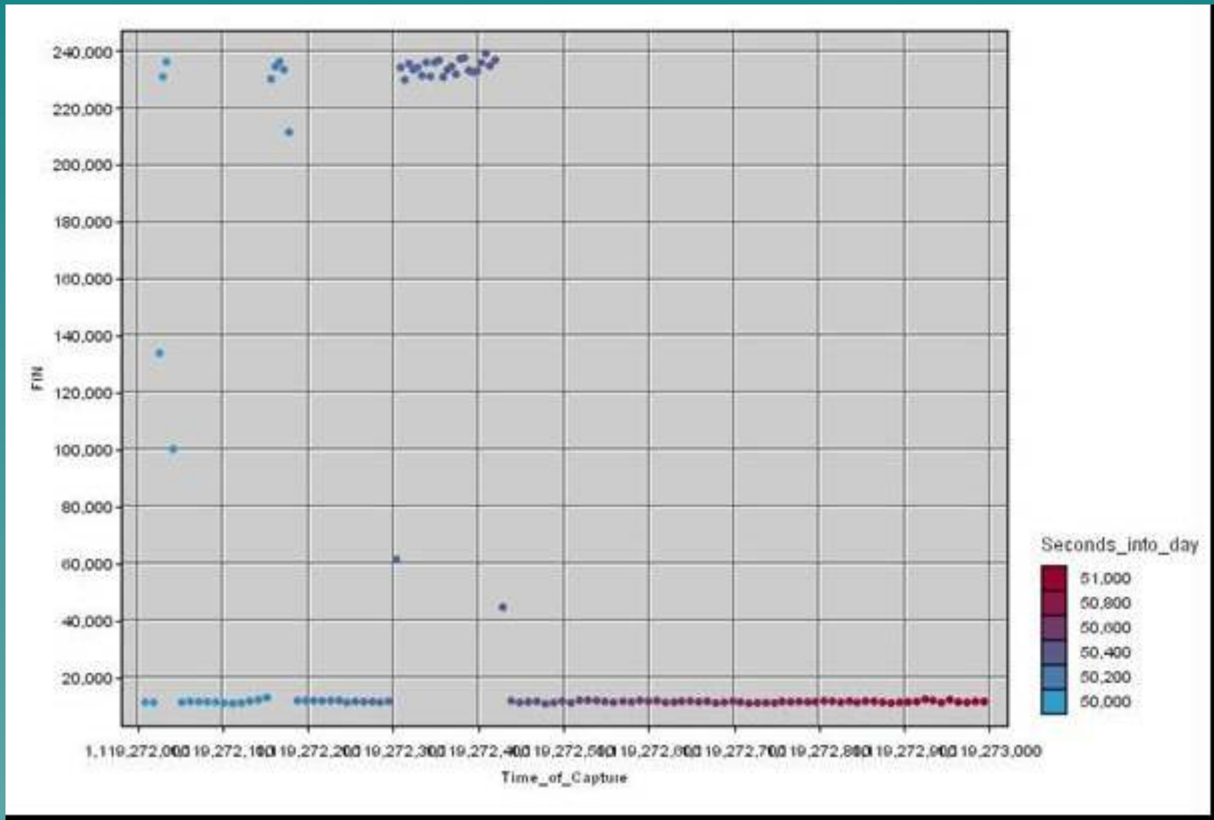
Anomaly Example – Average Packet Size



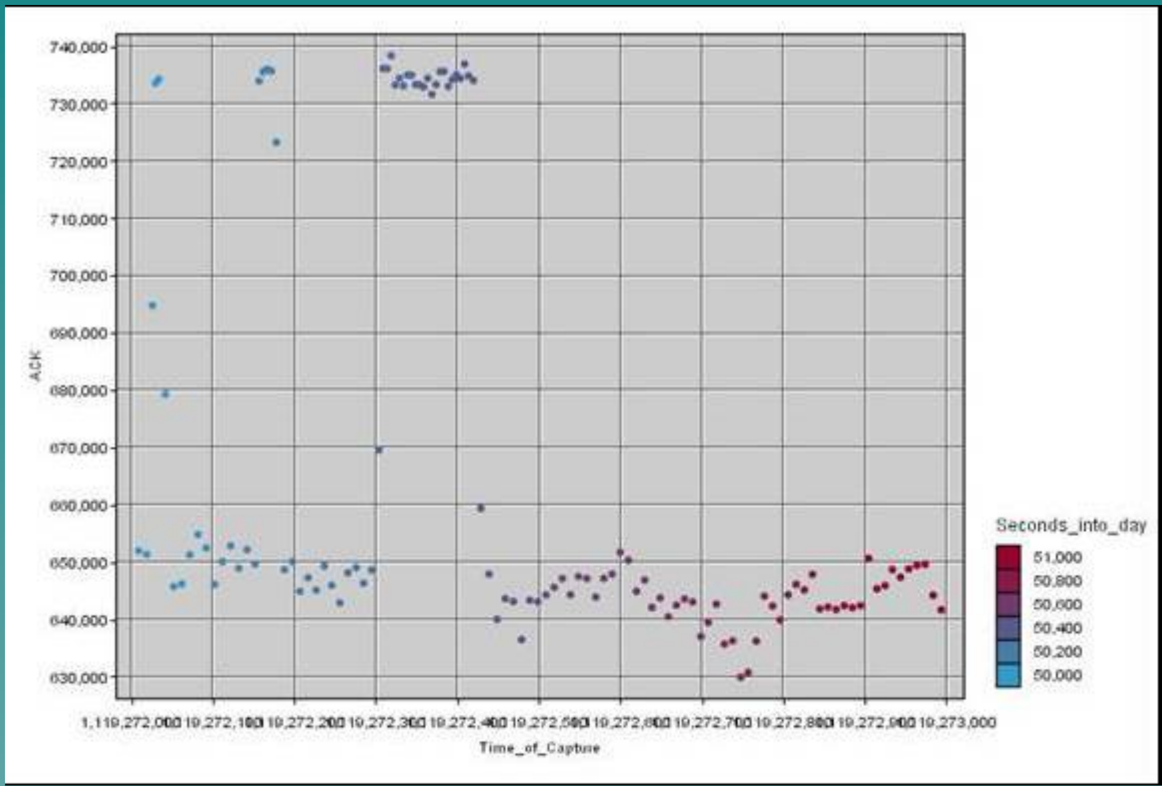
Anomaly Example – Destination Count



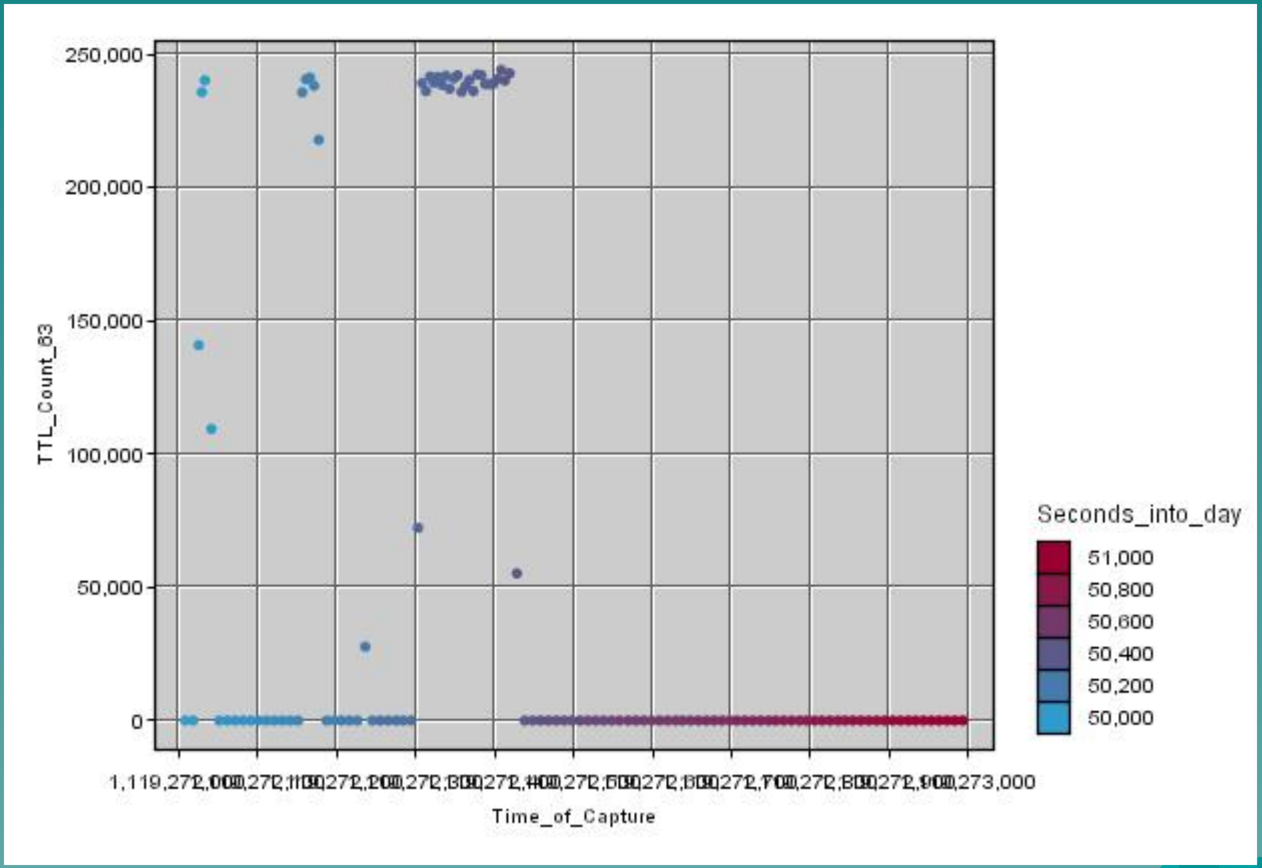
Anomaly Example – FIN Count



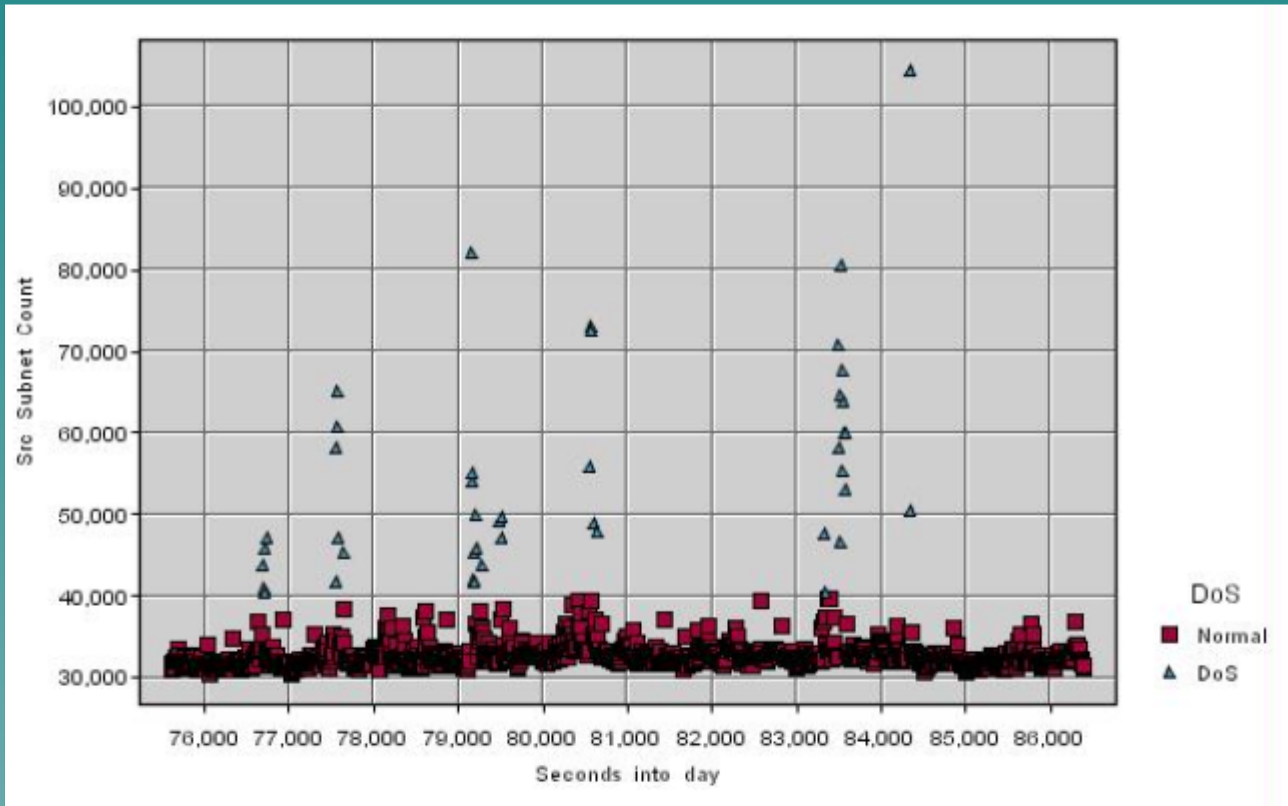
Anomaly Example – Ack Count



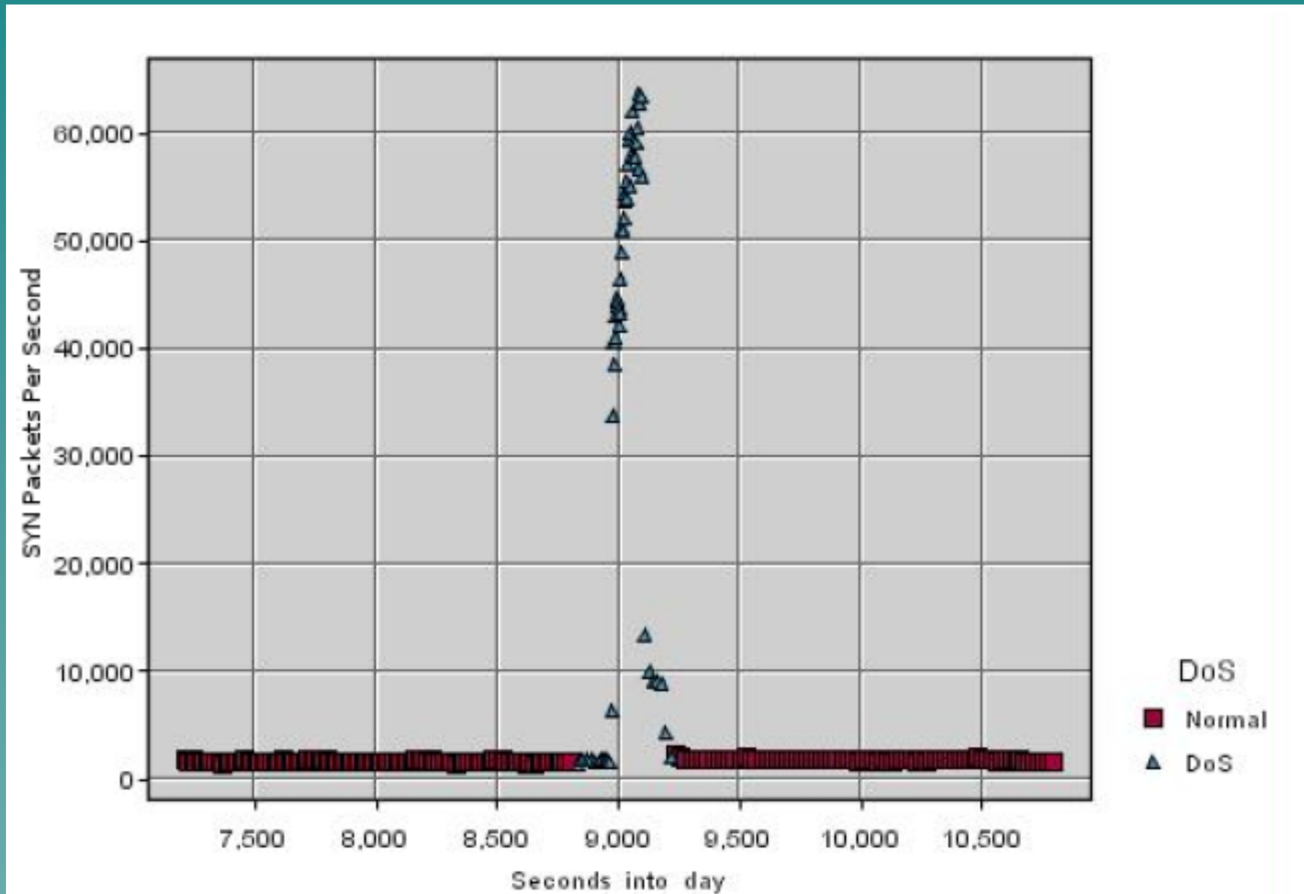
Anomaly TTL - 63



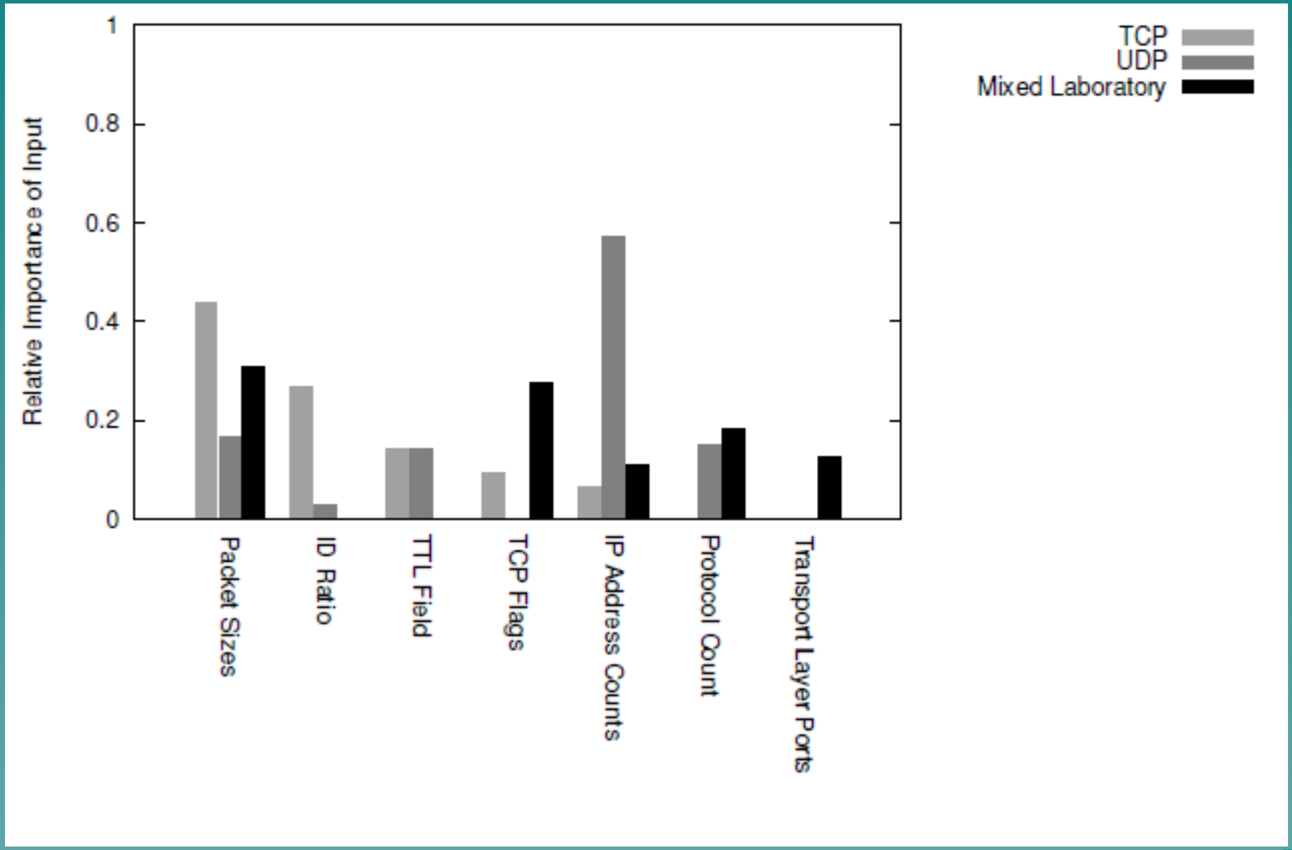
Example Detection Metric (IP Subnet Value)



2nd Example – TCP Syn Flags/Sec



Relative Importance of Detection Metrics



Loughborough University

Performance Assessment

- True Positive (TP) refers to one attack frame that has been correctly classified as malicious.
- True Negative (TN) refers to one non-attack frame that has been correctly classified as legal frames.
- False Positive (FP) refers to one non-attack frame that has been misclassified as malicious.
- False Negative (FN) refers to one attack frame that has been misclassified as legal frames.

- Detection Rate (DR) is the proportion of attack frames correctly classified as malicious, among all the attack frames.
- $DR\ (\%) = TP / FN + TP$
- False Positive Rate ($FP \downarrow Rate$) is the proportion of non-attack frames misclassified as malicious, among all the evaluated frames.
- $FP \downarrow Rate\ (\%) = FP / TP + FP + TN + FN$
- False Negative Rate ($FN \downarrow Rate$) is the proportion of attack frames misclassified as legal, among all the attack frames.

Loughborough University

- Overall Success Rate (*OSR*) or *Accuracy* is the proportion of the total number of frames correctly classified, among all the evaluated frames.

- *OSR (%)=TN+TP/TP+FP+TN+FN*

- *Precision* or *Recall* is the proportion of attack frames correctly classified as malicious, among all the alarms generated.

- *Precision (%)=TP/TP+FP*

- *F-Score* or *F-Measure* is a tradeoff between Precision and DR. The

Summary and Conclusions

Review Questions

1. Which AI approach may be best for the following scenarios?

- Determining which, of a number of groups, a particular pattern of an attack belongs to.
- Combining the outputs of a number of different IDSs into a single result.