A Software Tool for Network Intrusion Detection

4th Biennial Conference

Presented by: Christiaan van der Walt

Date:October 2012

our future through science

Presentation Outline

- Need for intrusion detection systems
- Overview of attacks
- Illustration of network traffic for various attacks
- Simulation of data
- Description of NetID Algorithm
- Illustration of NetID Software Tool
- Future Work

The Need for Network Intrusion Detection Systems

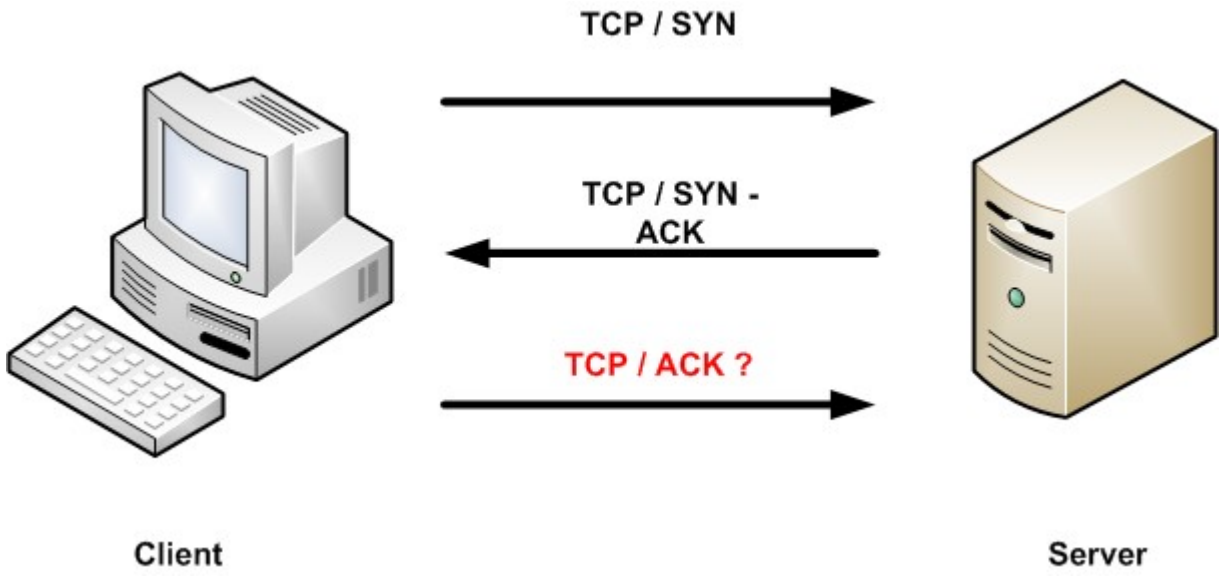
- Online services and security of data
- Serve content -> serve applications
- Online services include internet banking, e-commerce, video streaming, Gmail
- Data services include Dropbox, Google Docs, Google Drive
- Threats: hacking, Denial of Service (DoS) attacks
- Victims of DoS attacks include Yahoo, eBay, e-trade, CNN
- Distributed DoS attacks
- Why another software tool?

Types of DoS attacks

- Consumption of computational resources – bandwidth, disk space, processor time
- Disruption of configuration information – routing information
- Disruption of state information – unsolicited resetting of TCP connections
- Obstructing communication media – users and victim can't communicate adequately

Commonly used attacks

- TCP SYN (Neptune) flooding attack
  - More than 90% of DoS attacks use the TCP protocol
  - SYN flood is the most commonly-used TCP attack
  - Exploits the limitation of the three-way hand shake , that maintains half-open connections for a certain time period
  - Neptune - SYN flood denial of service on one or more ports



Commonly used attacks

- ICMP (Smurf) attack
  - Use spoofed broadcast ICMP echo (ping) messages
  - Sends spoofed ping messages (spoof ip address so that it seems the victim of the attack is sending them)
  - The network to which these ping requests are sent, then forwards these requests to all hosts in the network and each of them respor with an echo reply, thus multiplying the traffic by the number of hosts

- Teardrop attack
  - Exploits the flaw in the implementation of TCP/IP stacks that can not handle overlapping IP fragments
  - Sends mangled IP packets with overlapping IP fragments, and large payloads to victim of attack

What do DoS Attacks Look Like?

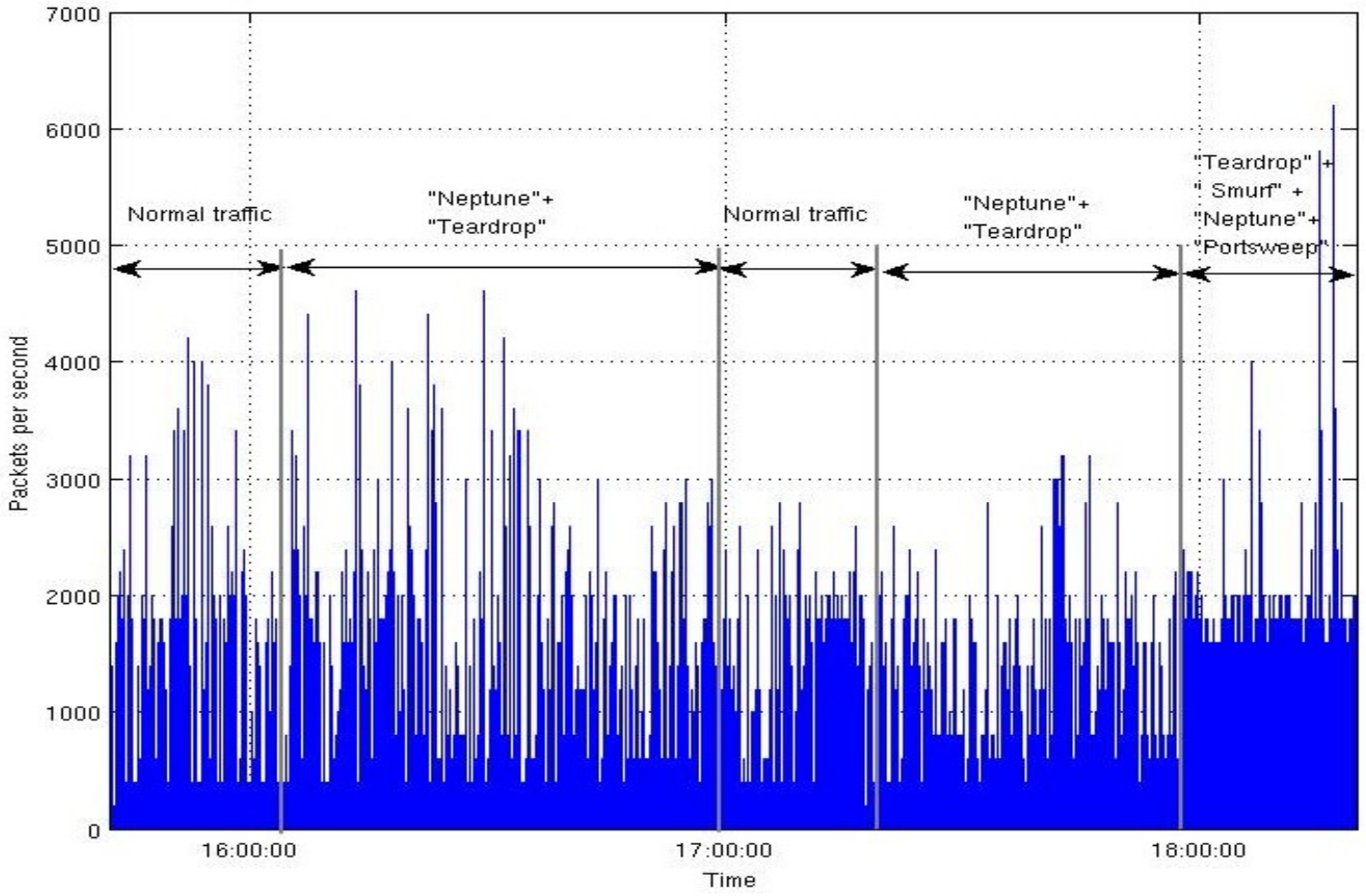


Figure: Network packet rate for different attacks

Approaches to detecting DoS flooding attacks

- Adaptive threshold algorithms
  - Monitor the traffic flow (number of packets per second), in case of SYN flood, they monitor the SYN packet rate
  - When packet rate exceeds a threshold a possible intrusion is flagged
  - Threshold is adapted to account for daily and weekly variations, typically make use of mean packet rate of recent traffic

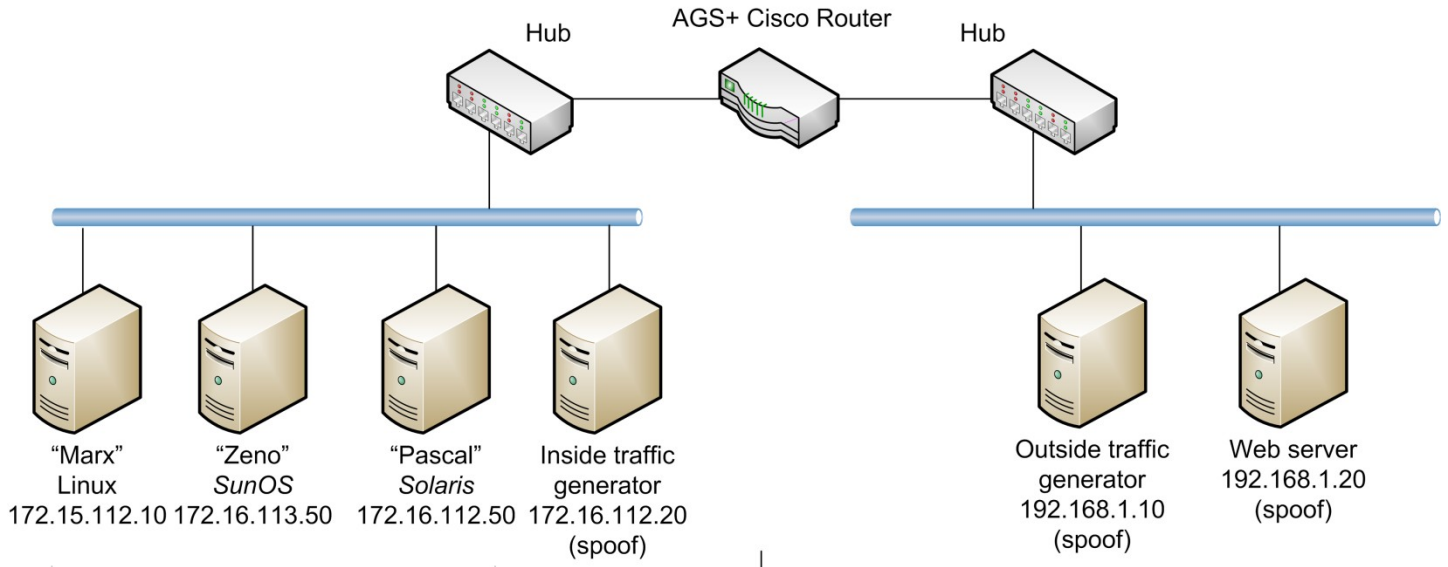
- Change-point detection algorithms
  - Based on hypothesis testing for iid data
  - Continually estimate a statistical distribution of network traffic, and test whether the change in distribution is statistically significant

Algorithm Development

- Make use DARPA Intrusion Detection Evaluation Data generated by MIT
- The simulated the following DoS attacks

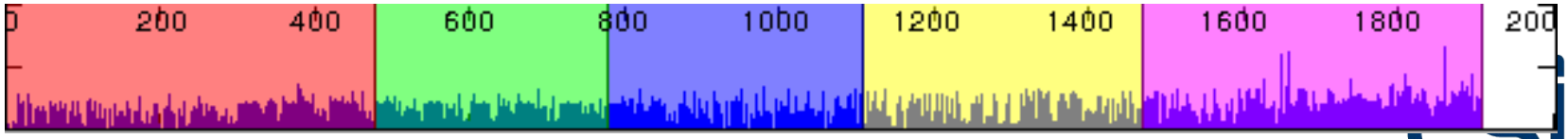
Name	Service	Vulnerable Platforms	Mechanism	Time to Implement	Effect
Apache2	http	Any Apache	Abuse	Short	Crash httpd
Back	http	Any Apache	Abuse/Bug	Short	Slow server response
Land	N/A	SunOS	Bug	Short	Freeze machine
Mailbomb	smtp	All	Abuse	Short	Annoyance
SYN Flood	Any TCP	All	Abuse	Short	Deny service on one or more ports for minutes
Ping of Death	icmp	None	Bug	Short	None
Process Table	Any TCP	All	Abuse	Moderate	Deny new processes
Smurf	icmp	All	Abuse	Moderate/ Long	Network Slowdown
Syslogd	syslog	Solaris	Bug	Short	Kill Syslogd
Teardrop	N/A	Linux	Bug	Short	Reboot machine
Udpstorm	echo/ chargen	All	Abuse	Short	Network Slowdown

Data Simulation Setup



"Inside"
172.16.* eyrie.af.mil

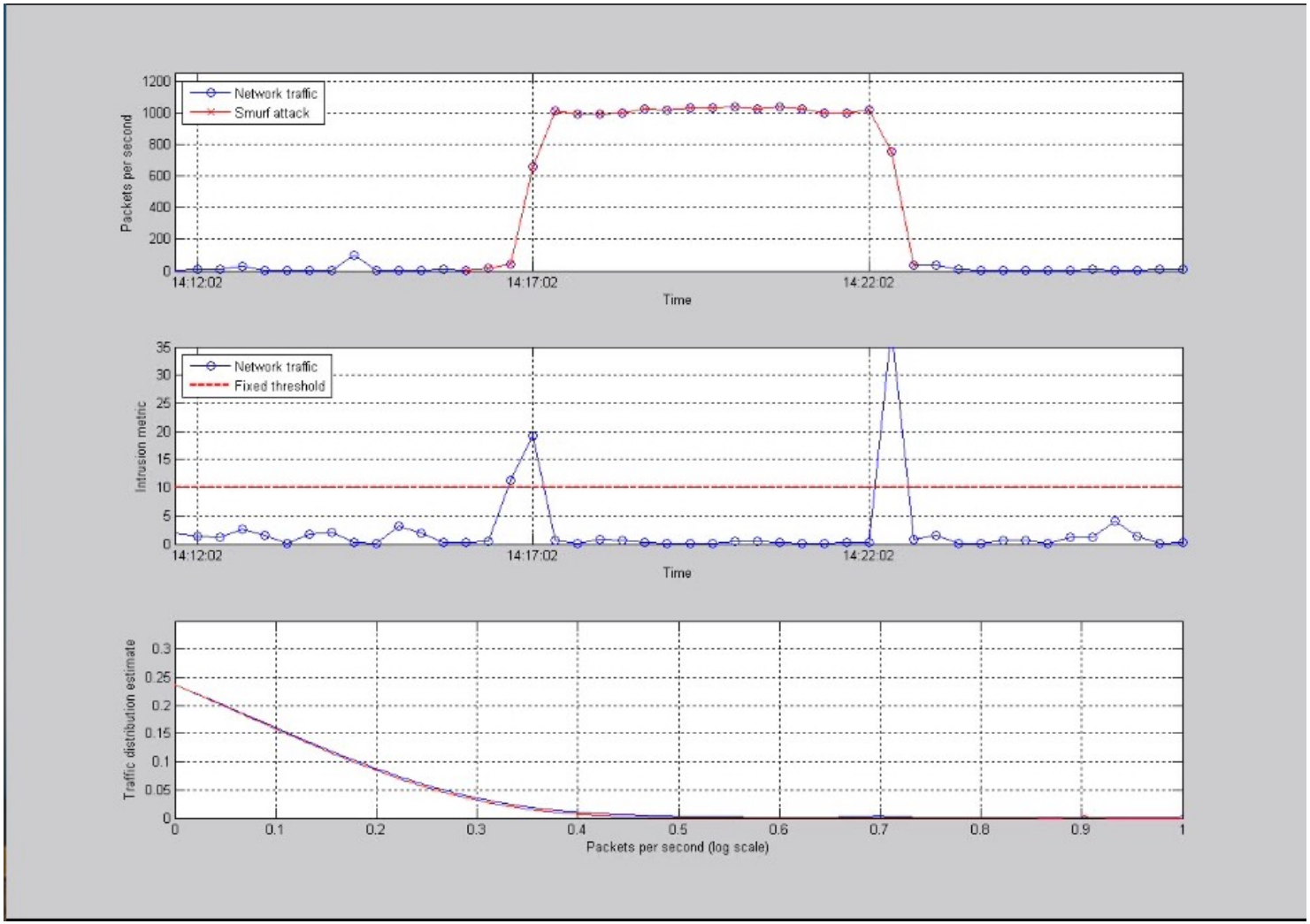
"Outside"
192.168.1.* world.net
194.27.251.* plum.net
197.218.177.* grape.mil



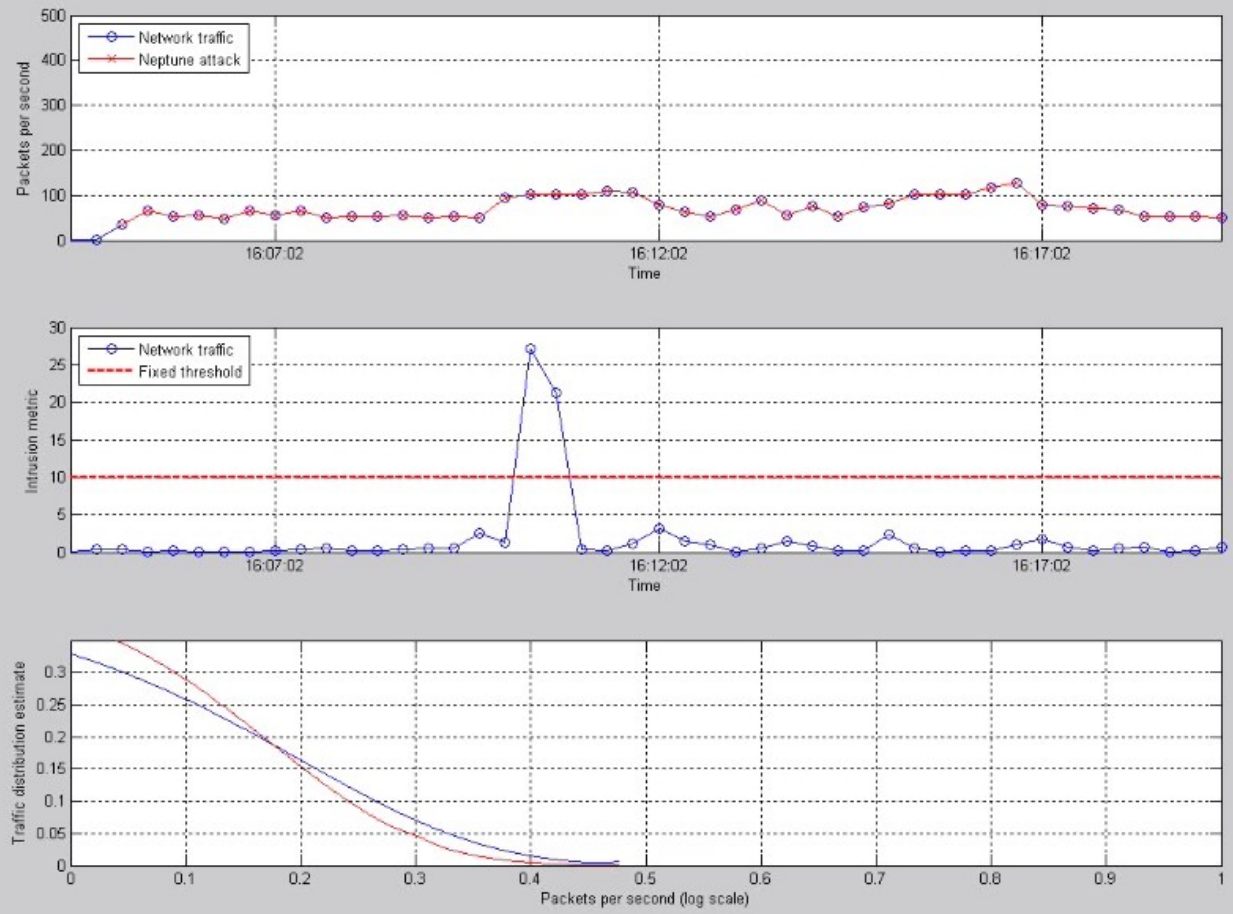
NetID Online Detection Algorithm

- Detect attacks in real-time (is capable of scanning 4 hours of data in a few minutes)
- High detection accuracy and fast detection time (< 5 seconds)
- Performs change detection via an advanced statistics adaptive threshold algorithm
- Algorithm
    - Specify sampling rate (typically 5ms)
    - Arrival times of network packets are converted to packet rate (packets per sampling rate)
    - Specify window length (typically 80s)
    - Estimate the probability density function (PDF) of the data in the time window starting at time t
    - Specify a window step size (typically 2.5s)
    - Move the samples in the window to time t + step_size
    - Estimate the PDF of window t + step_size
    - Calculate the change in distribution
    - Test if change > threshold

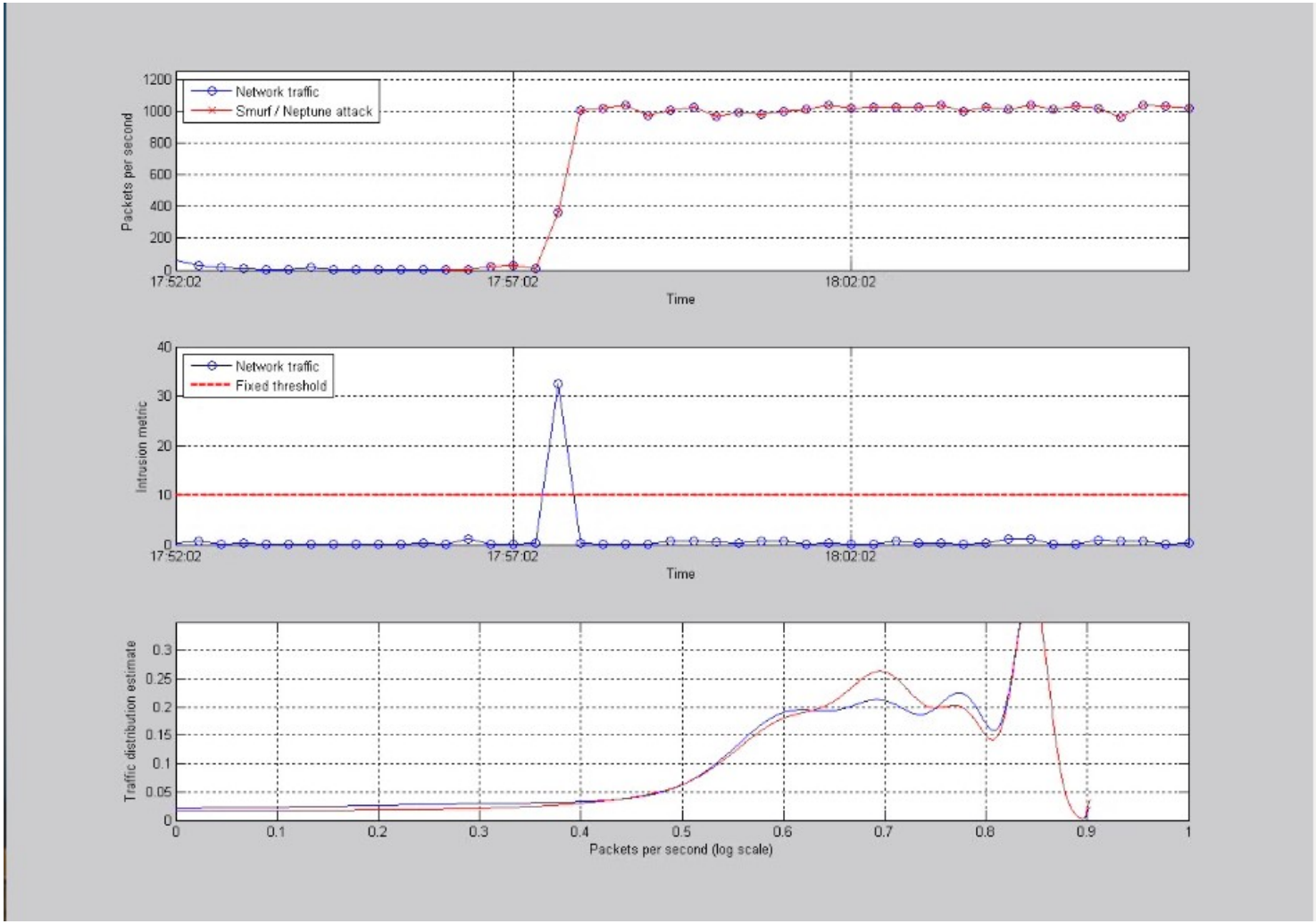
Simulation results – Smurf Attack 1



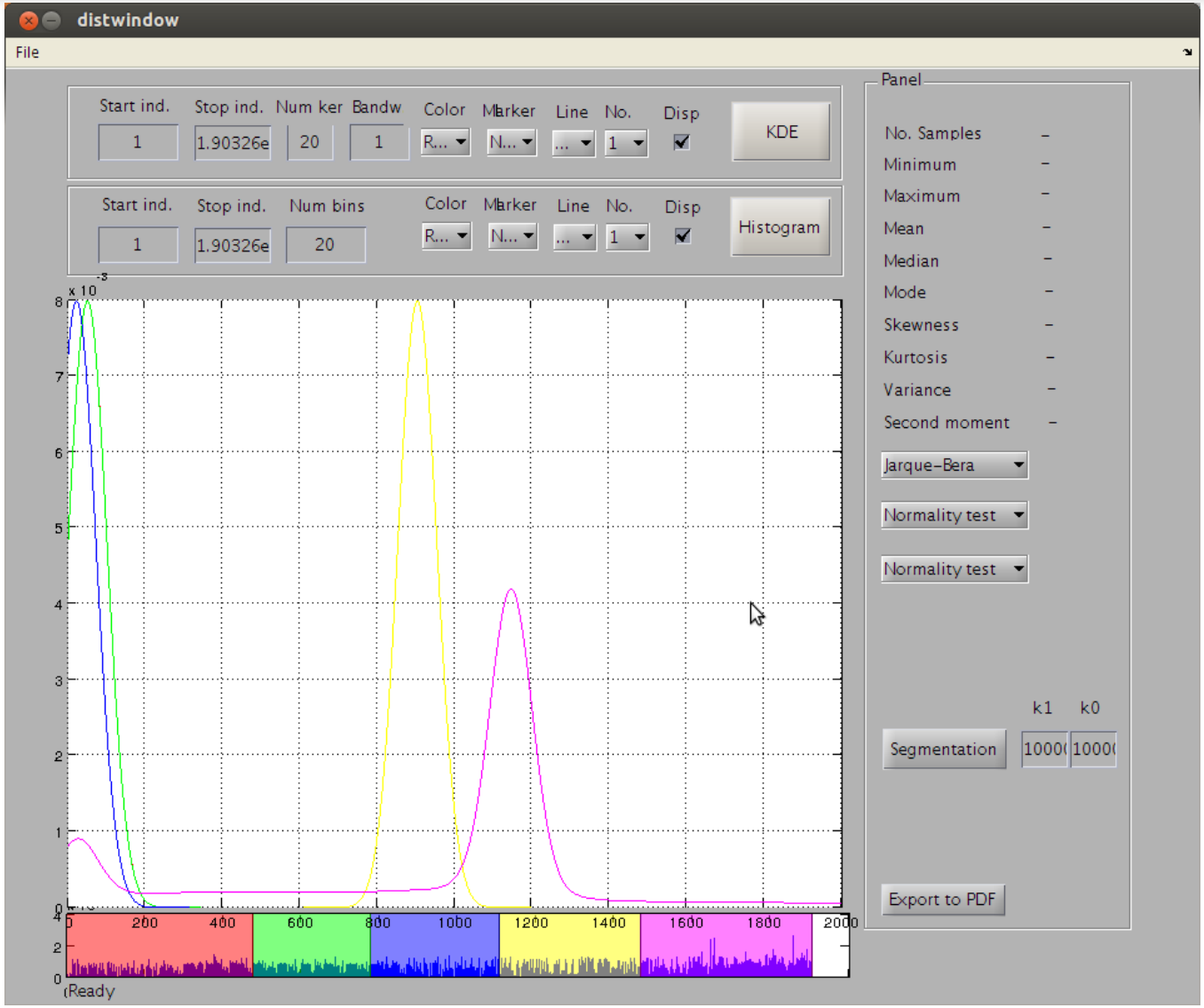
Simulation results – Neptune Attack 1



Simulation results – Smurf Attack 2



NetID Software Tool (Illustration)



Operator Controls

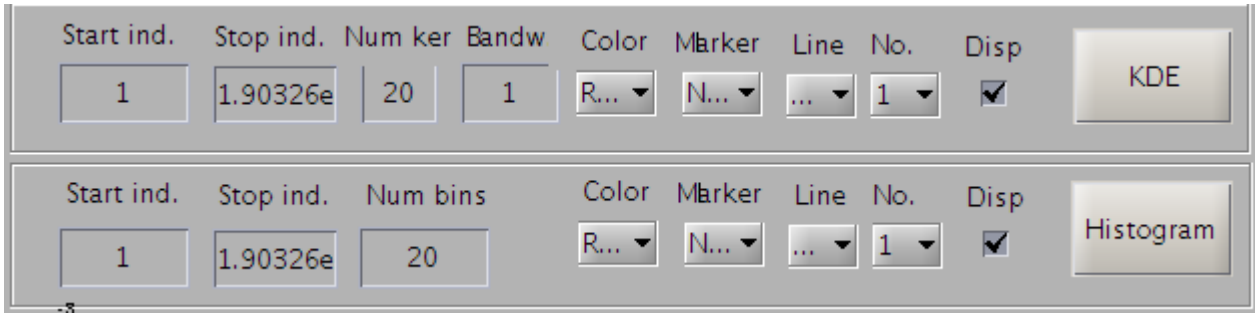


Figure: Operator Tools

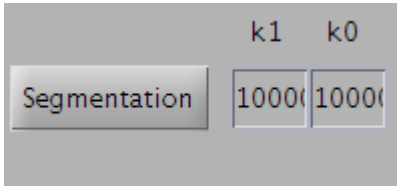


Figure: Parameter settings

Future Work

- Add more intrusion detection algorithms to NetID Software
- Investigate more attacks and their detection performance
- Simulate our own attacks (possibly from within NetID Software)
- Further develop the analysis tools for NetID

Thank you