

# Statistical Traffic Measurement

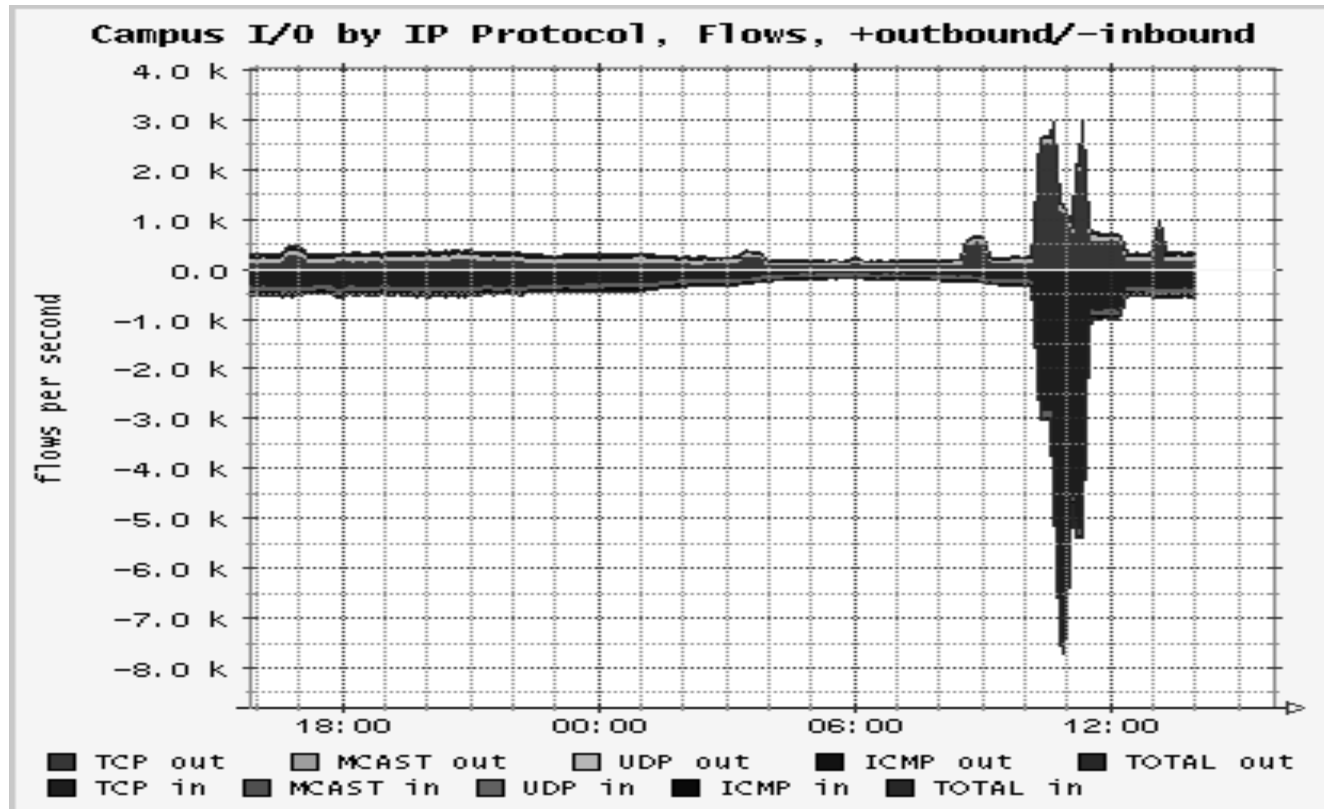
# Denial Of Service & Accounting

- DOS attacks consume resources.
- Looked at many approaches to account for resources.
- Use every available piece of information for anomaly detection
  - Volume of traffic
  - Number of flows
  - Address distribution
  - Port numbers
  - Protocol distribution

# Measurement

- How do you detect an anomaly?
- What is anomalous behavior?
- Use statistics and past distributions
  - So far, we looked at static thresholds
  - Flows above 1% of link bandwidth
  - Top 100 flows etc.
- How to get data for statistical measurements?

# FlowScan



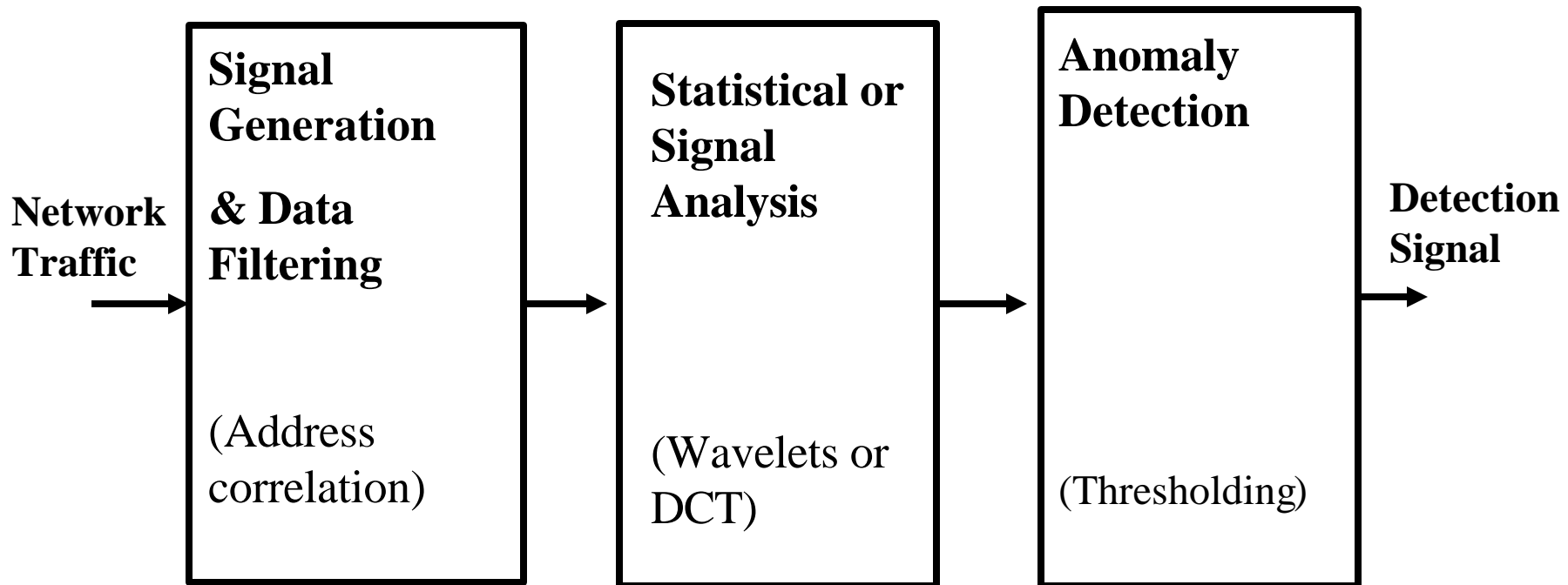
# False Alarms & False negatives

- Accurate anomaly detector requires
  - Few false alarms
  - Few false negatives
- Setting of thresholds requires careful analysis of data
- Today, a few case studies and a platform for statistics collection

# General Problem

- Collect information about a signal over the signal space each sample
  - Address space of  $2^{32}$
  - Port numbers of  $2^{16}$
- Collect information over many samples
- Does current sample look different?
- How to collect, analyze and conclude?
- Real-time versus Post-mortem

# Approach



# Signal Generation

- Traffic volume (bytes or packets)
  - Analyzed before
  - May not be a great signal when links are always congested (typical campus access links)
- Lot more information in packet headers
  - Source address
  - Destination address
  - Protocol number
  - Port numbers

# Signal Generation

- Per packet cost is important driver
- Update a counter for each packet header field
  - Too much memory to put in SRAM
- Break the field into multiple 8-bit fields
  - 32-bit address into four 8-bit fields
  - 1024 locations instead of  $2^{32}$  locations
  - In general,  $256^* (k/8)$  instead of  $2^k$
  - $k/8$  counter updates instead of 1

# Signal Generation

- What kind of signals can we generate with addresses, port numbers and protocol numbers?

# Addresses are correlated

- Most of us have habits
  - Access same web sites
- Large web sites get significant part of traffic
  - Google.com, hp.com, yahoo.com
- Large downloads correlate over time
  - ftp, video
- On an aggregate, addresses are correlated

# Address Correlation - attacks?

- Address correlation changes when traffic patterns change abruptly
  - Denial of service attacks
  - Flash crowds
  - Worms
- Results in differences in correlation
  - High --single attack victim
  - Low - lots of addresses --worm

# Address correlation signals

- Address correlation:
 
$$r(n) = \frac{\hat{a}_m(p_{mn-1} - \overline{p_{n-1}}) * (p_{mn} - \overline{p_n})}{\sqrt{\hat{a}_m(p_{mn-1} - \overline{p_{n-1}})^2} \sqrt{\hat{a}_m(p_{mn} - \overline{p_n})^2}}$$

- Simplified Address correlation:

$$C(n) = \sum_m p_{mn-1} * p_{mn} / \sum_m p_{mn}$$

# Signal Analysis

- Address correlation as a time series signal
- Employ known techniques to analyze time series signals
- Wavelets –one powerful technique
  - Allows analysis in both time and frequency domain
- Per-sample analysis has more flexibility
  - Not in forwarding path

# Analysis of address correlation

- What timescales should we consider?
- Sample to sample, 2/4/... samples?
- Wavelets allow analysis at multiple timescales
- Look at differences at multiple timescales

# Wavelets

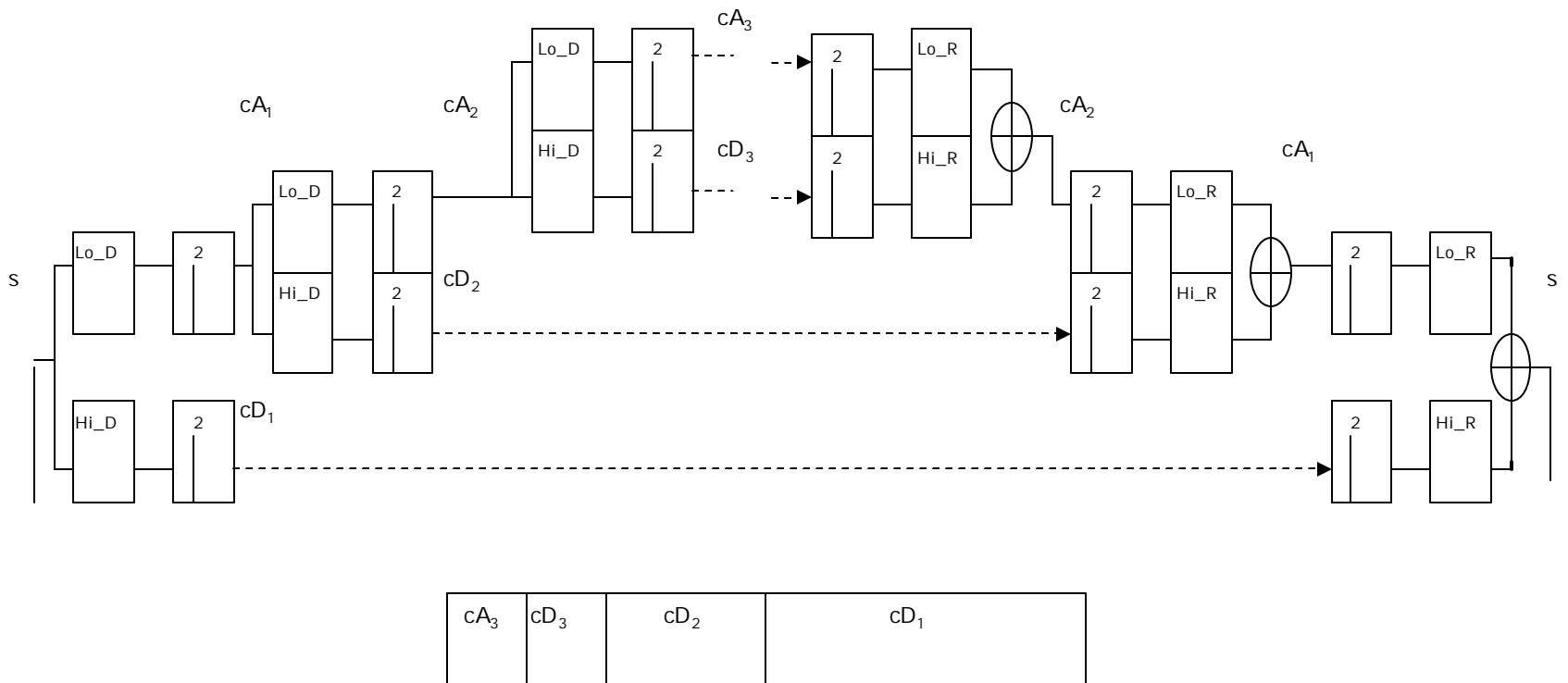
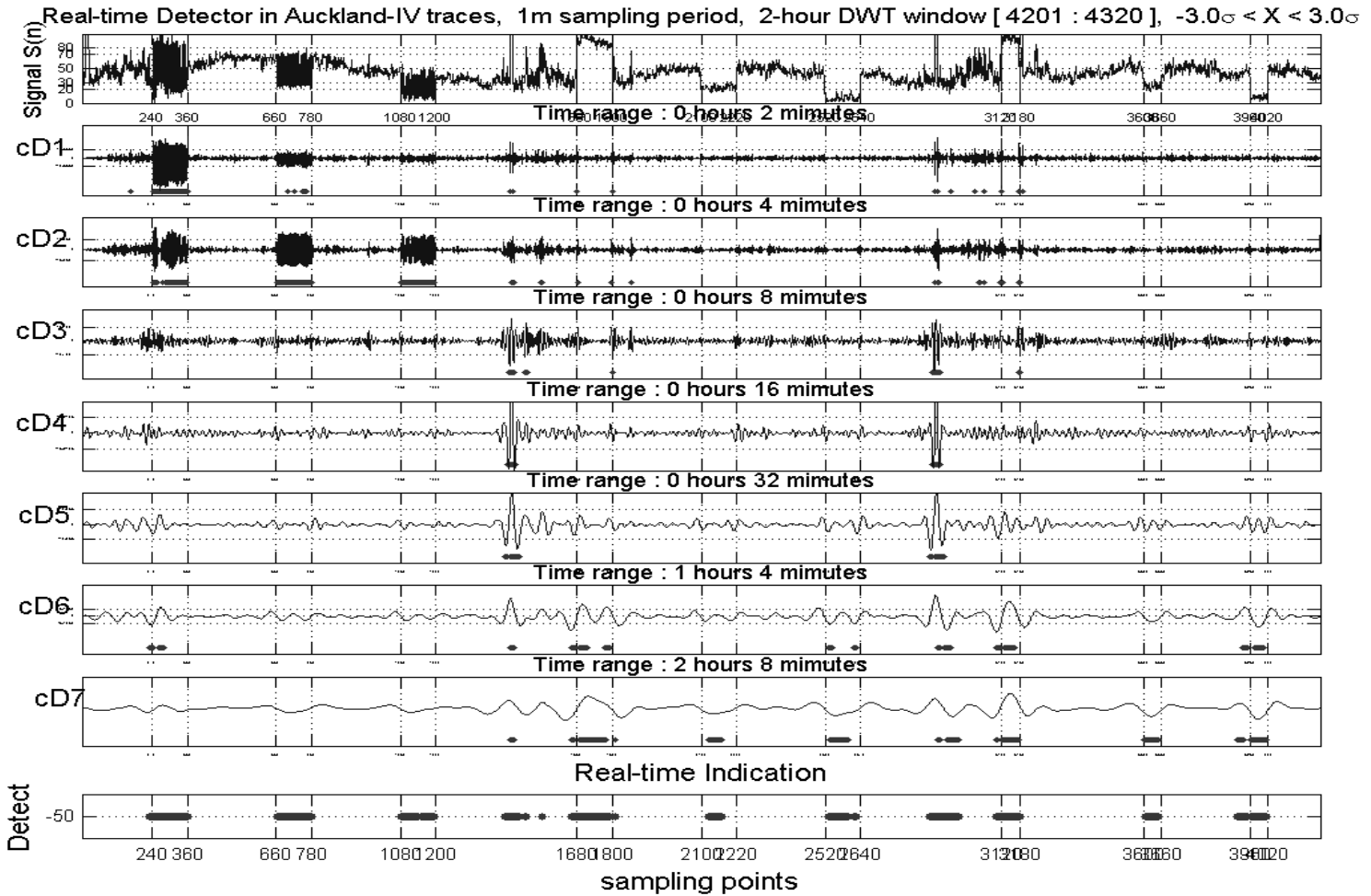
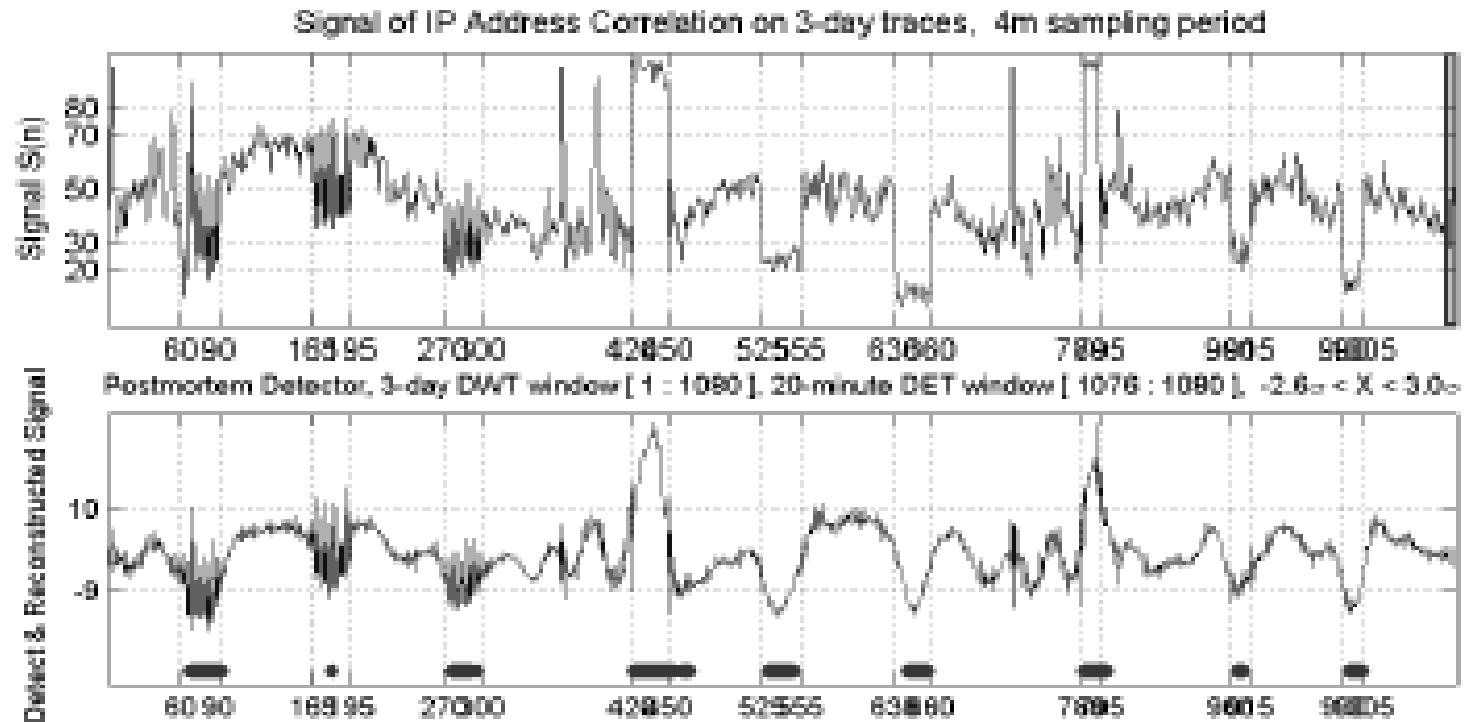


Fig. 6. A Multilevel two-band wavelet decomposition and reconstruction

# Real-time analysis



# Does this work?



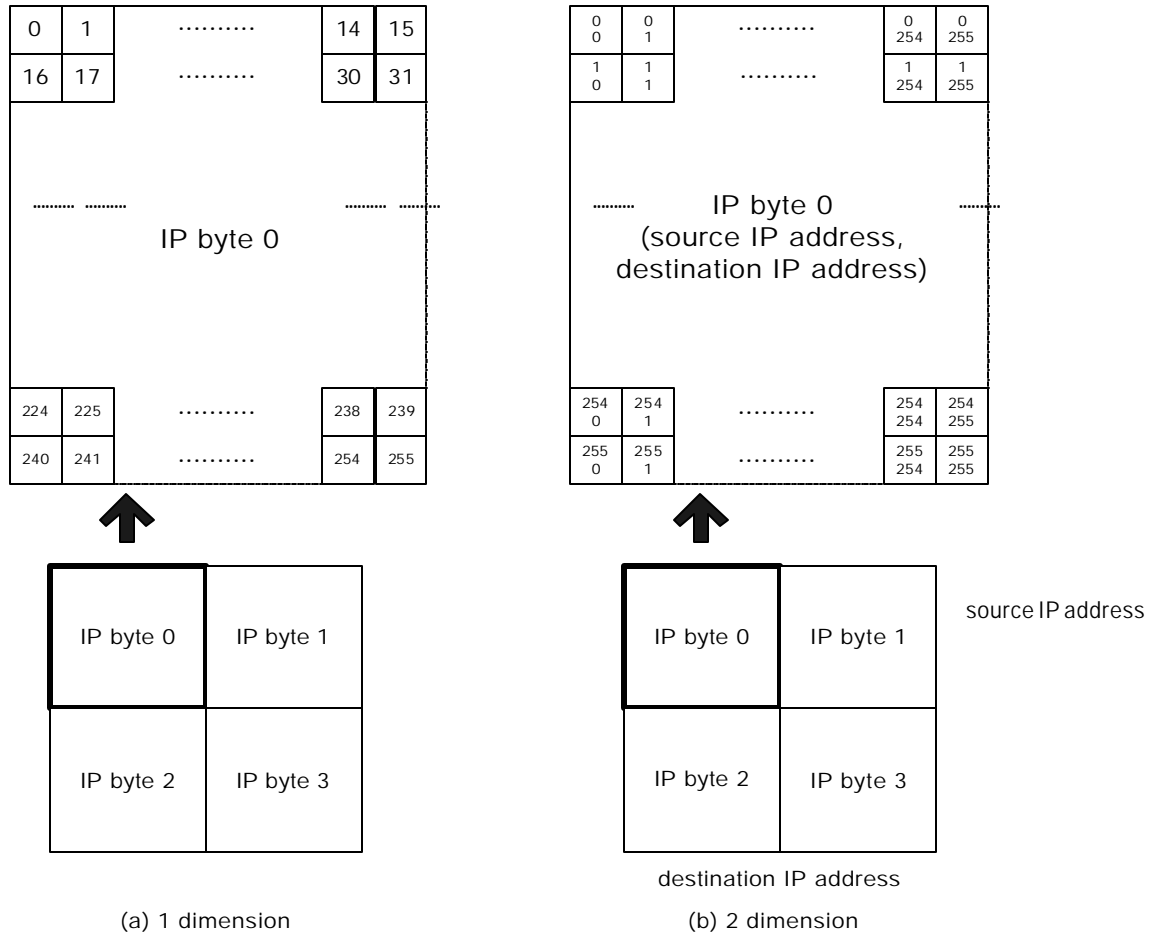
# Value of Wavelets

TABLE IV  
THE DETECTIONABILITY OF THE IP CORRELATION SIGNAL AND THE DWT SIGNAL

	<i>conf. level</i>	<i>DWT</i>	1	2	3	4	5	6	7	8	9	<i>false pos.<sup>a</sup></i>	<i>false neg.</i>
<i>2.5σ</i>	98.5 %	IP	c	x <sup>d</sup>	x	.	x	.	.	x	.	1	4
		DWT	.	.	.	.	.	.	.	.	.	2	0
<i>3.0σ</i>	99.7 %	IP	.	x	x	.	x	.	.	x	x	0	5
		DWT	.	.	.	.	.	.	.	.	.	0	0
<i>3.5σ</i>	99.95 %	IP	x	x	x	.	x	x	.	x	x	0	7
		DWT	.	.	x	.	.	.	.	x	.	0	2
<i>4.0σ</i>	99.99 %	IP	x	x	x	x	x	x	x	x	x	0	9
		DWT	.	x	x	.	x	.	.	x	.	0	4

- a. IP means the original IP address weighted correlation signal without applying the DWT
- b. DWT means the DWT transformed signal
- c. . means a detection
- d. x means a non-detection
- e. False positive is counted a series of relevant signal as 1

# Image generation



(a) 1 dimension

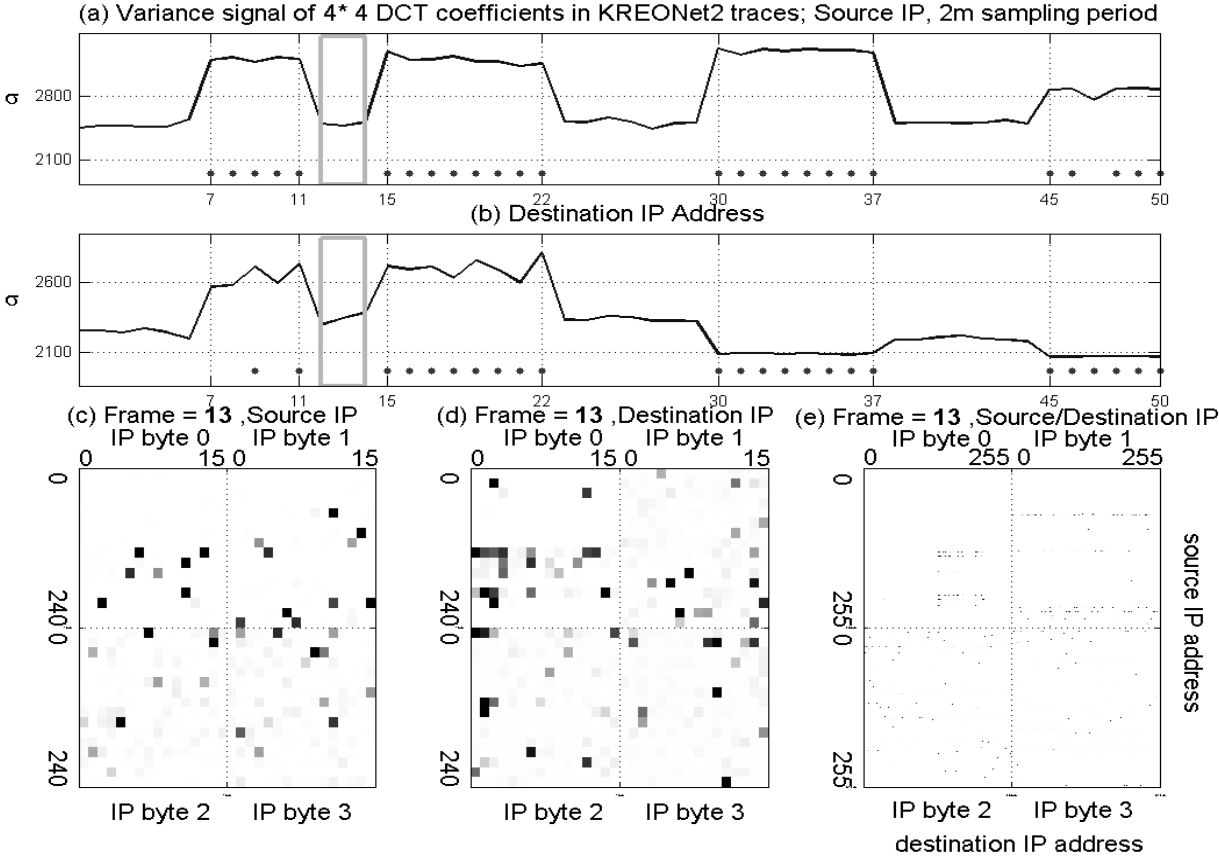
(b) 2 dimension

Figure 2. The visualization of network traffic signal in IP address

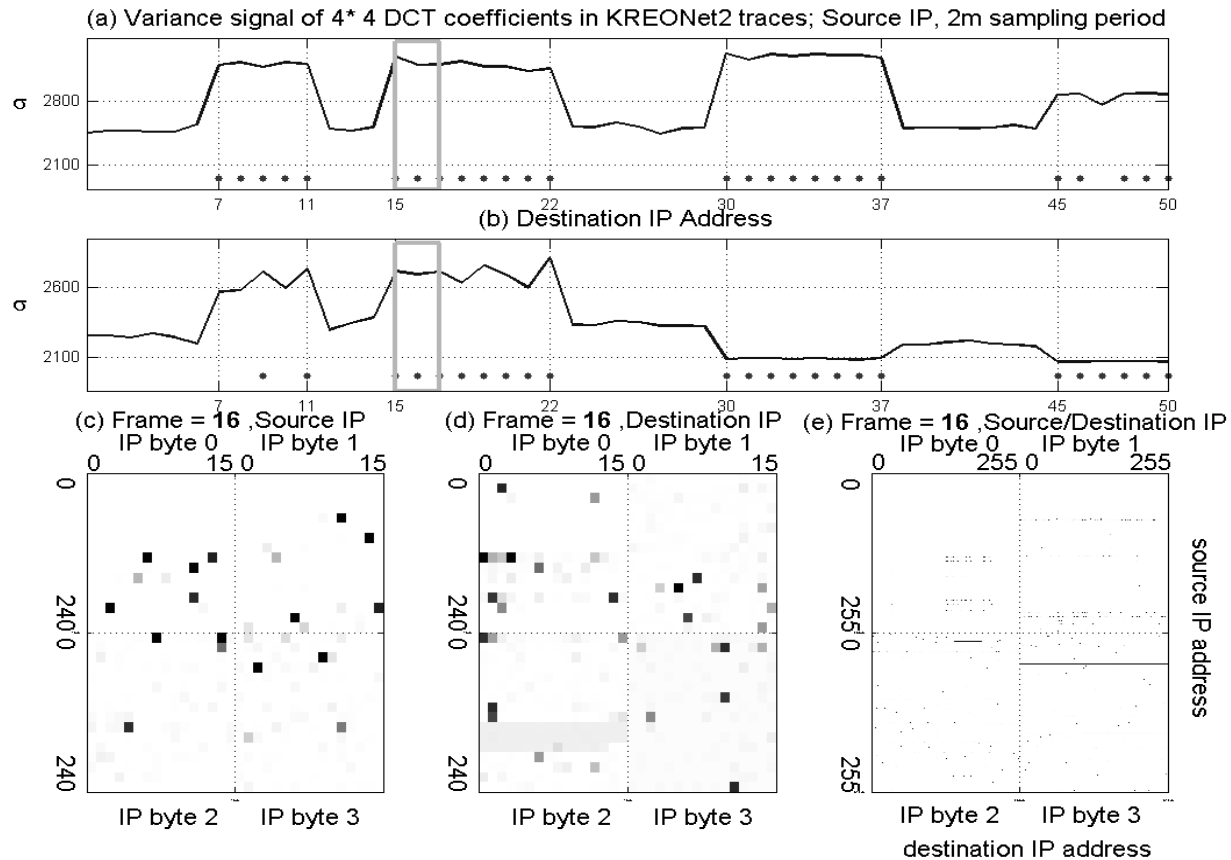
# Two dimensional images

- Horizontal/vertical lines indicate anomalies
  - Infected machine contacting multiple destinations (worm propagation)
  - Multiple source machines targeting a single destination (DDOS)

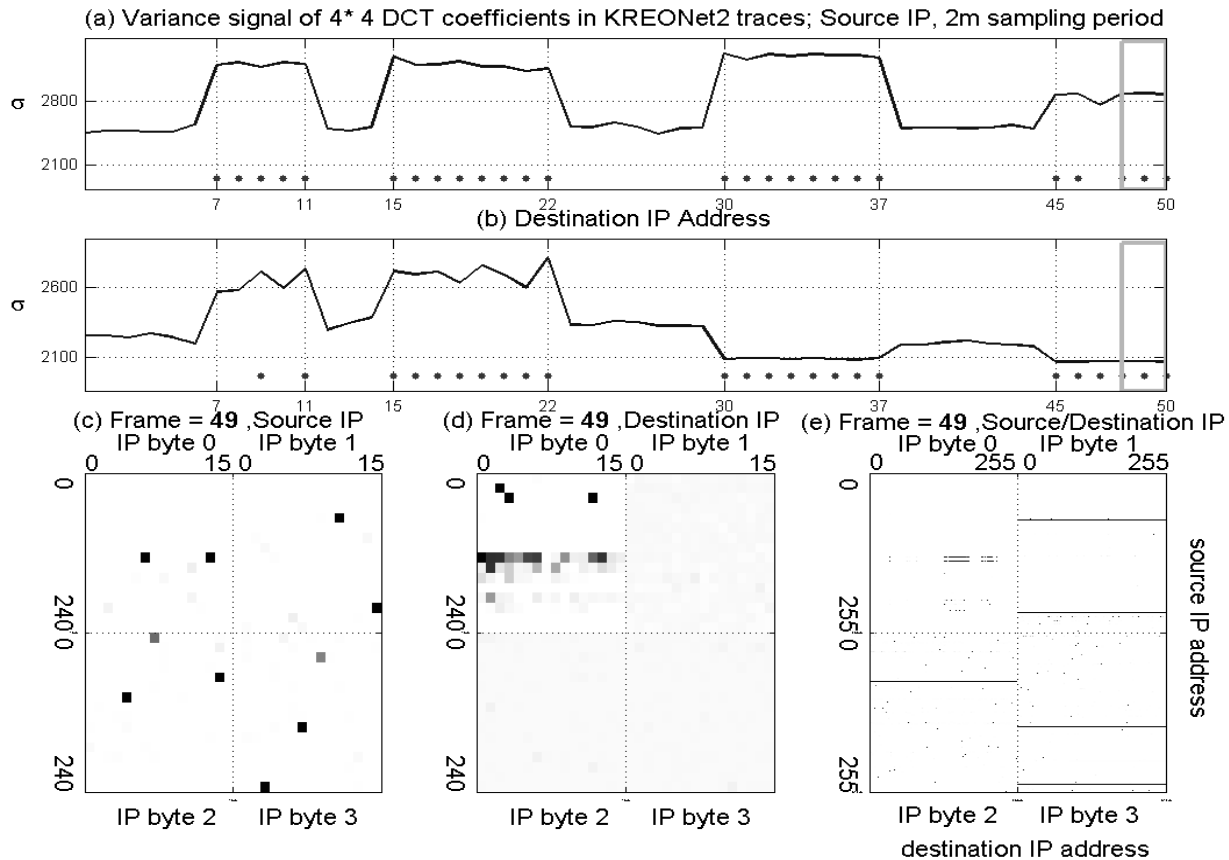
# DCT analysis of addresses



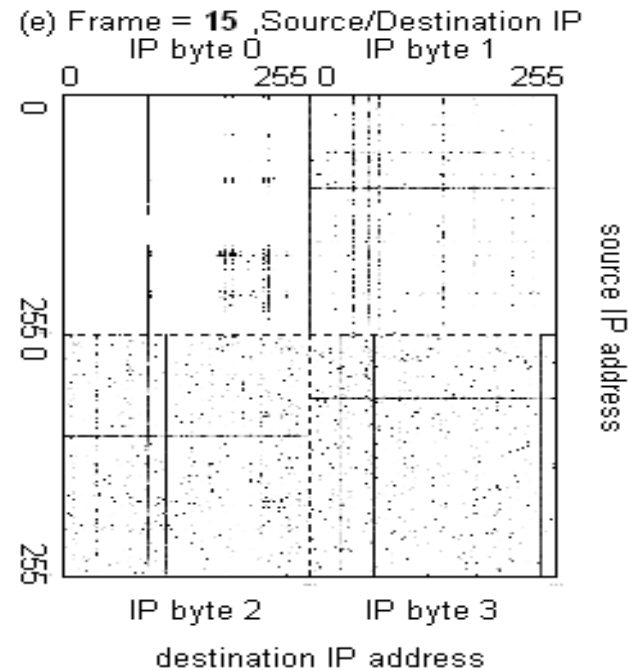
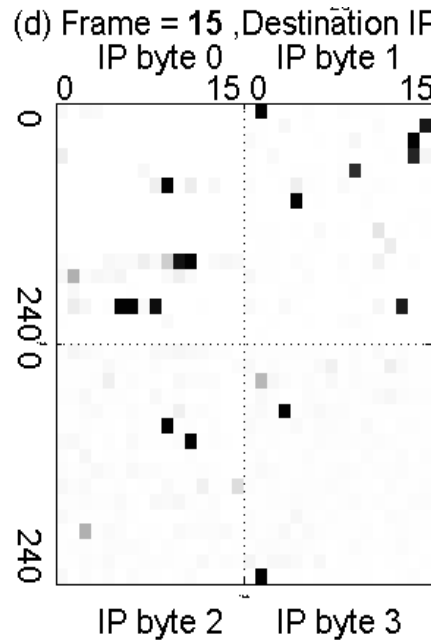
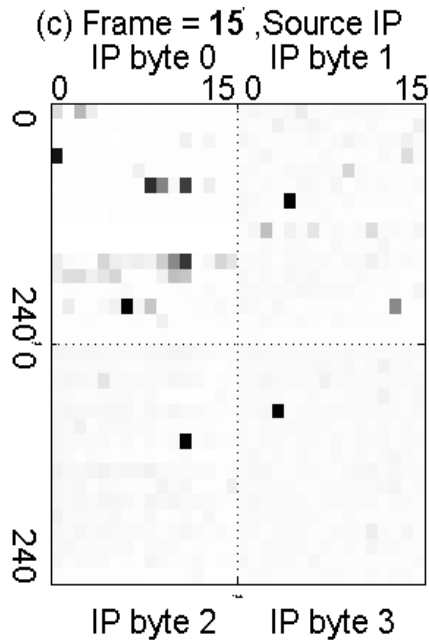
# Semi-random attacks



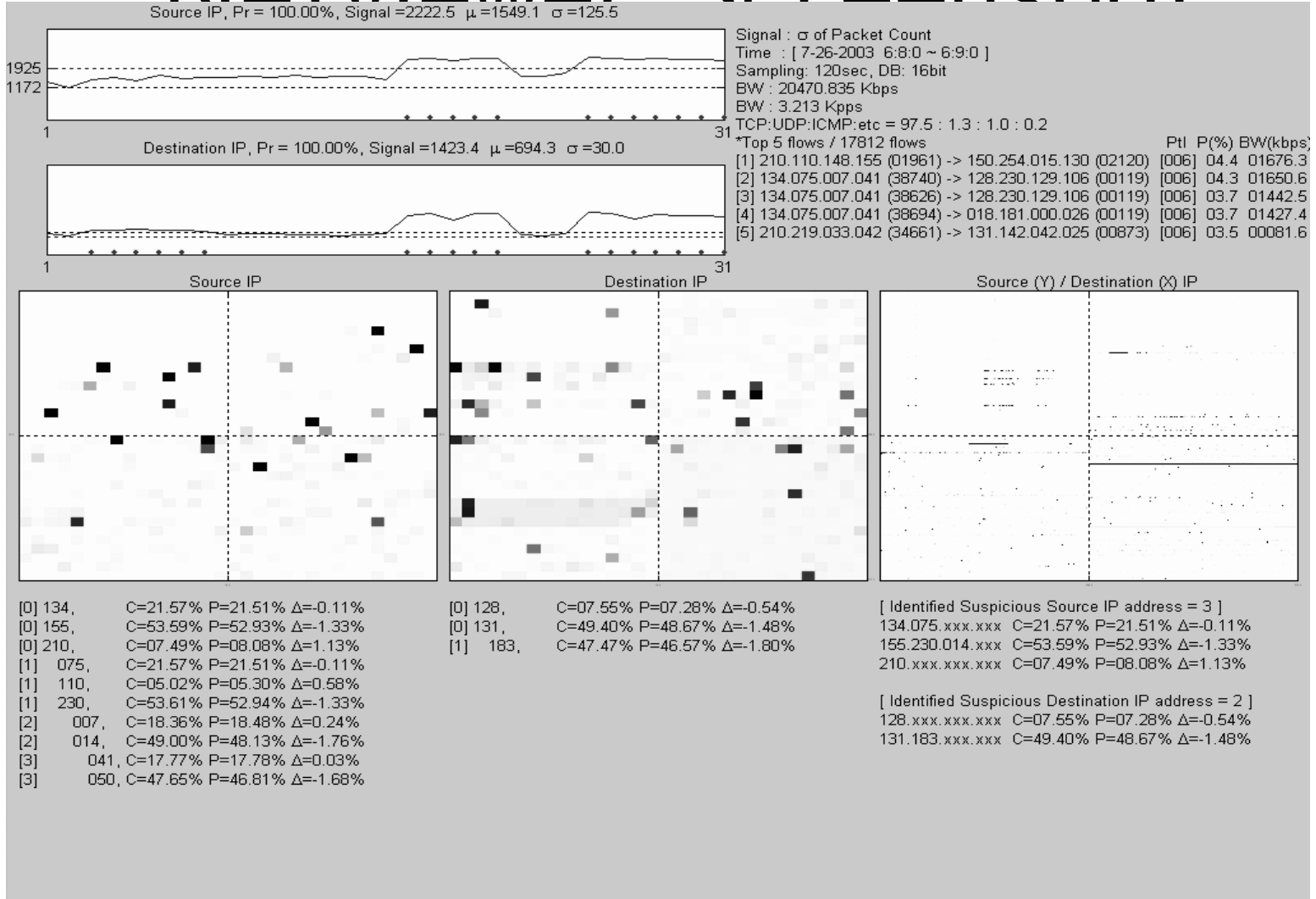
# Random attacks



# Complex attacks



# Netviewer Screenshot



# Anomaly Detection 1

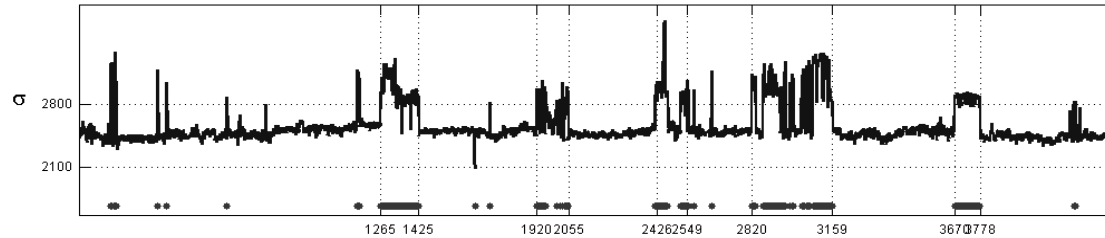
- Compute the variance of all pixels
- Compare this variance with historical norms
- If the current variance is above/below  $\text{mean} \pm 3 * \text{sigma}$ , declare anomaly
- Mean, sigma computed over a moving window.

# Anomaly Detection 2

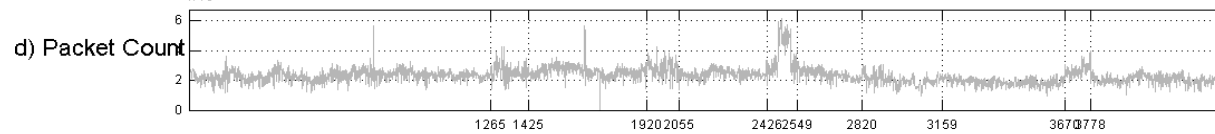
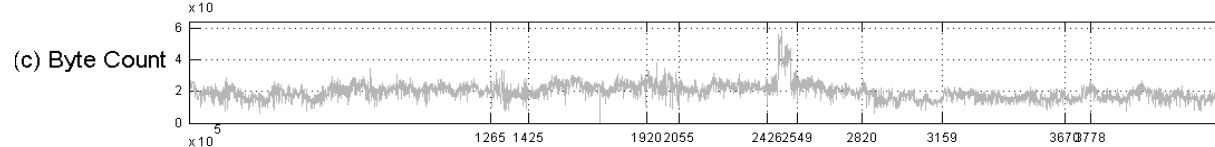
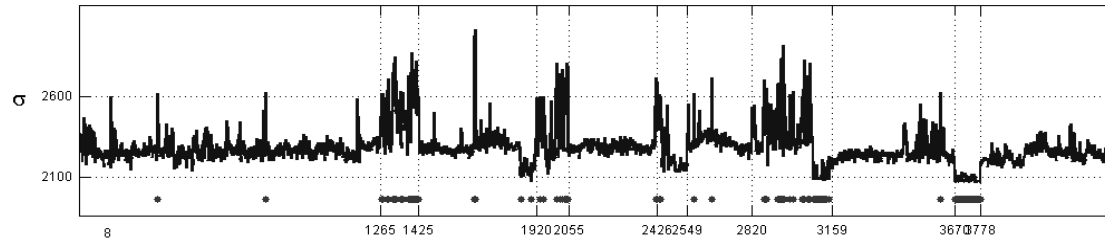
- Compute the DCT of 16x16 blocks
- Keep one coefficient from each block
- Compute the variance of the 256 saved coefficients
- Use this as a signal
- Allows compressed view of traffic to be saved for later use.

# Better than volume analysis

(a) Variance signal of 4\*4 DCT coefficients in KREONet2 traces; Source IP, 2m sampling period



(b) Destination IP Address



# Evaluation

- True Positive Rate
- False Alarm Rate or False Positive Rate
- True Negative Rate, False Negative Rate
- $LR = \frac{\text{true + rate}}{\text{false + rate}}$
- $NLR = \frac{\text{false -ve rate}}{\text{true -ve rate}}$
- Ideally,  $LR = \text{infinity}$ ,  $NLR = 0$

# Neyman-Pearson Test

- Used to detect signals in communication theory -optimal.
- In our case, normal traffic == noise, anomalous traffic == signal
- Need classified traffic: normal, anomalous to train the detector
- Test on the remaining attacks in the trace.

# Comparison of Scalar signals

Signals	T.P. $\beta^1$	F.P. $\alpha^2$	<i>NP</i> $\beta^3$	<i>NP</i> $\alpha^4$	LR $^5$	NLR $^6$
Byte count	8.2% 64/782	0.11% 4/3563	<i>13.1%</i>	<i>0.22%</i>	72.9/ 59.9	0.92/ 0.87
Packet count	11.9% 93/782	0.25% 9/3563	<i>20.3%</i>	<i>0.15%</i>	47.1/ 134.8	0.88/ 0.80
Flow number	95.8% 749/782	0.73% 26/3563	<i>89.9%</i>	<i>0.23%</i>	131.3/ 397.0	0.04/ 0.10

1. True Positive rate
2. False Positive rate

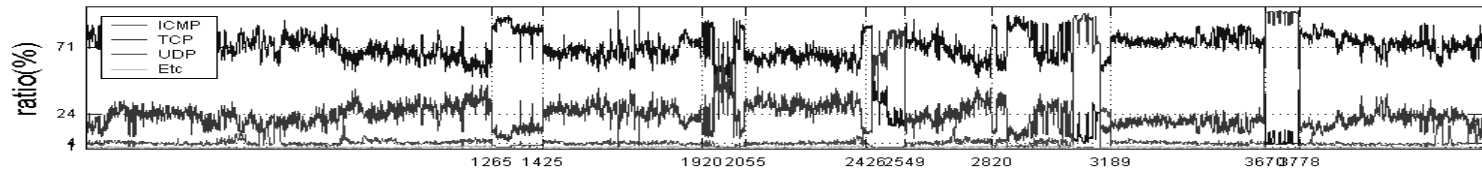
# Protocol Composition

- During attack, attack protocol volume will be higher
  - Observation of changes can lead to detection

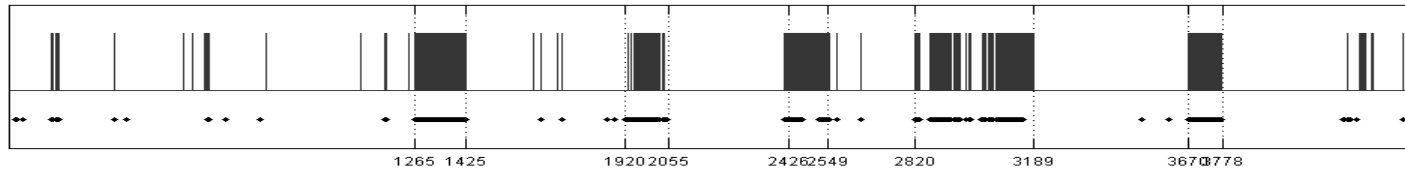
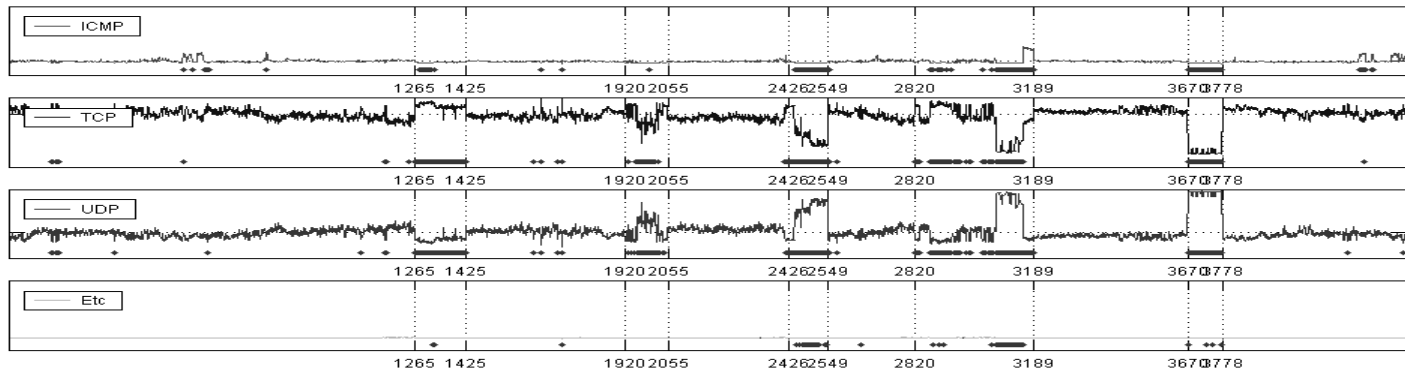
Signals	T.P. $\beta$	F.P. $\alpha$	$NP \beta$	$NP \alpha$	LR	NLR
Protocol composition	89.8% 702/782	2.30% 82/3563	- <sup>1</sup>	-	39.0	0.10

# Protocol Composition

(a) Input traffic Proportion in "Access Link" traces based on Protocols, 2m sampling period



(e) detect & ratio (c) detect & ratio (c) detect & ratio (c) detect & ratio



(f) Anomaly Detection Signal

# Address based signals

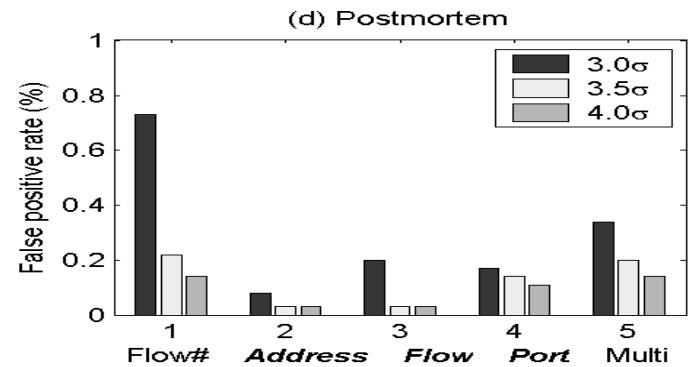
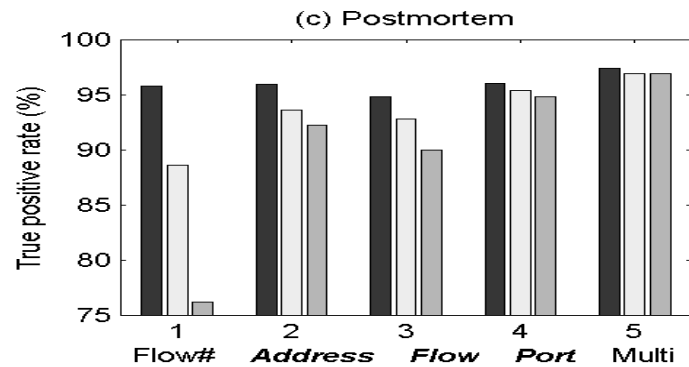
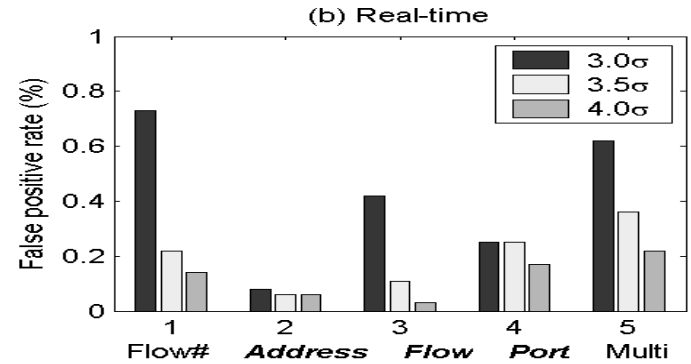
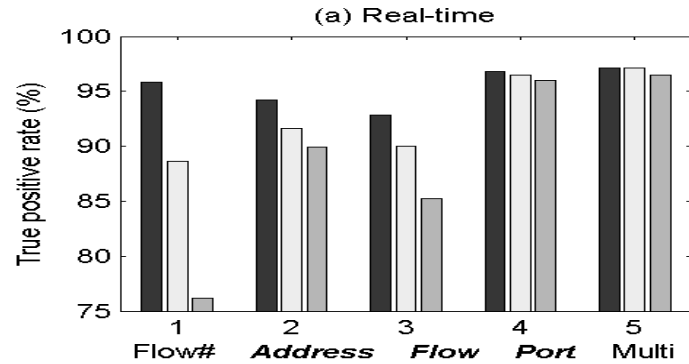
<b>Time</b>	<b>D.</b>	<b>TP <math>\beta</math></b>	<b>FP <math>\alpha</math></b>	<b>NP <math>\beta</math></b>	<b>NP <math>\alpha</math></b>	<b>LR</b>	<b>NLR</b>
Real-time	SA <sup>2</sup>	81.5% (637)	0.00% (0)	72.5%	0.15%	$\infty$ / 483.3	0.19/ 0.28
	DA <sup>3</sup>	87.1% (681)	0.08% (3)	86.5%	0.15%	1034/ 576.7	0.13/ 0.14
	(SA, DA) <sup>4</sup>	94.2% (737)	0.08% (3)	–	–	1119	0.06
Post mortem	SA	88.6% (693)	0.03% (1)	92.9%	0.15%	3157/ 619.3	0.11/ 0.07
	DA	80.2% (627)	0.06% (2)	84.0%	0.58%	1428/ 144.8	0.20/ 0.16
	(SA, DA)	95.9% (750)	0.08% (3)	–	–	1139	0.04

<sup>1</sup> *Address based signals* <sup>2</sup> *SA* <sup>3</sup> *DA* <sup>4</sup> *(SA, DA)*

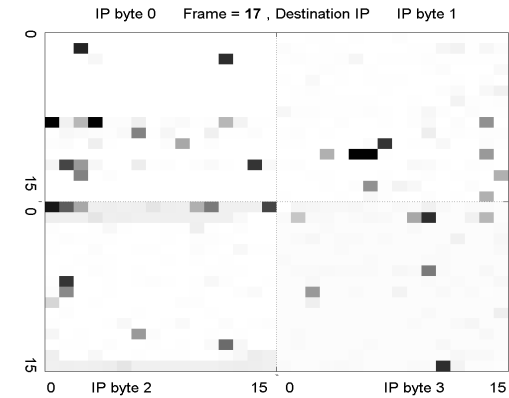
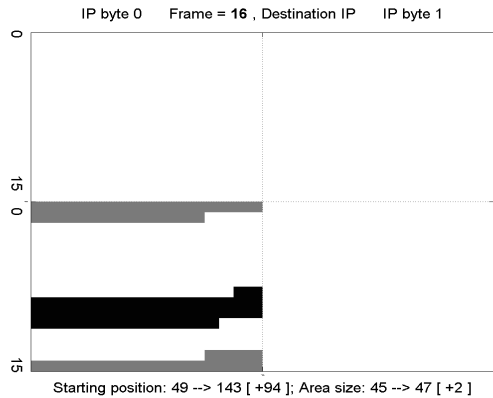
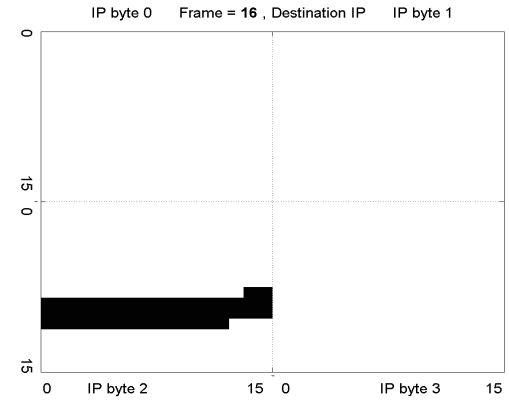
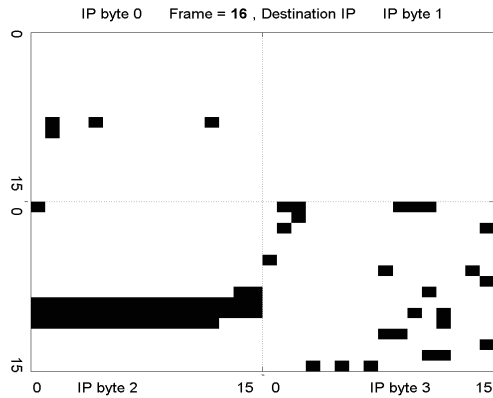
# Port Number Domain

<b>Time</b>	<b>D.</b>	<b>TP <math>\beta</math></b>	<b>FP <math>\alpha</math></b>	<b>NP <math>\beta</math></b>	<b>NP <math>\alpha</math></b>	<b>LR</b>	<b>NLR</b>
Real-time	SP <sup>1</sup>	83.4% (652)	0.14% (5)	95.5%	0.26%	594.1/ 371.5	0.17/ 0.05
	DP <sup>2</sup>	96.2% (752)	0.17% (6)	91.8%	0.55%	571.1/ 167.5	0.04/ 0.08
	(SP, DP) <sup>3</sup>	96.8% (757)	0.25% (9)	–	–	383.2	0.03
Post mortem	SP	93.9% (734)	0.11% (4)	92.3%	0.22%	836.1/ 415.5	0.06/ 0.08
	DP	95.7% (748)	0.14% (5)	87.9%	0.40%	681.6/ 222.3	0.04/ 0.12
	(SP, DP)	96.0% (751)	0.17% (6)	–	–	570.3	0.04

# Thresholds vs. Detection



# Motion prediction



# Summary of Image signals

- Distributions of signals over different domains (Addresses, port numbers, protocols) more powerful than static volume signals
- Lots of useful information in packet headers
- Possible to detect attacks in real-time.

# Advantages

- Not looking for specific known attacks
- Generic mechanism
- Works in real-time
  - Latencies of a few samples
  - Simple enough to be implemented inline

# References

- [1] Seong Soo Kim and A. L. N. Reddy, "A study of analyzing network traffic as images in real-time", Infocom 2005
- [2] --- "Detecting traffic anomalies through aggregate analysis of packet header data" Networking 2004