

Network Traffic Measurements, Visualization and Modeling

Kavitha Chandra (PI)

Mital Parikh

Max Denis

Hark-Sang Kim

Jing Tsui

Gbenga Olowoeye

Jiraporn Pongsiri

Rajani Devineni

Prachee Sharma

Mira Raspopovic

Estella Pham

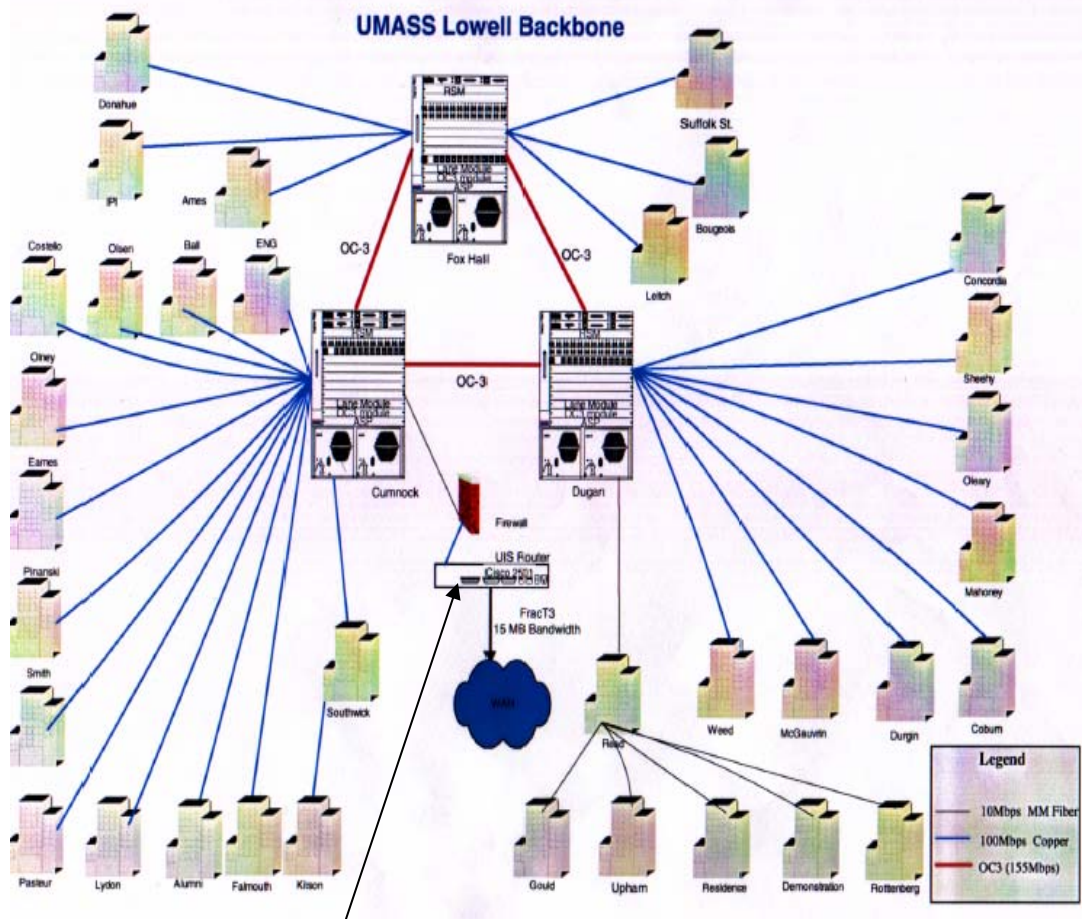
Chun You

Jimmie Davis



Center for Advanced Computation and
Telecommunications
Department of Electrical and Computer Engineering
University of Massachusetts Lowell
<http://morse.uml.edu>

Measurement Scenario



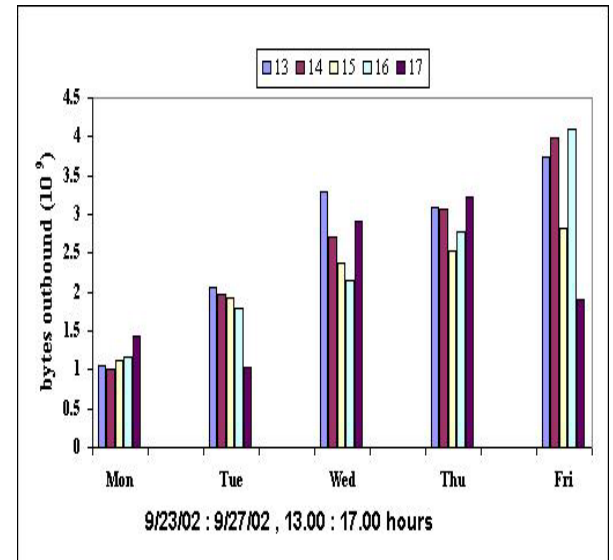
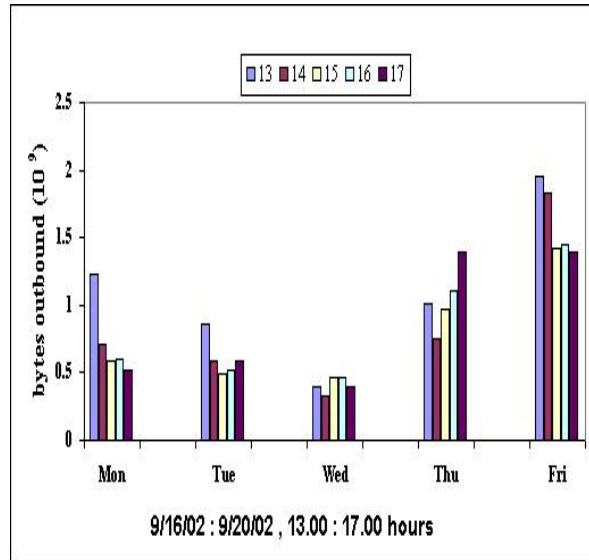
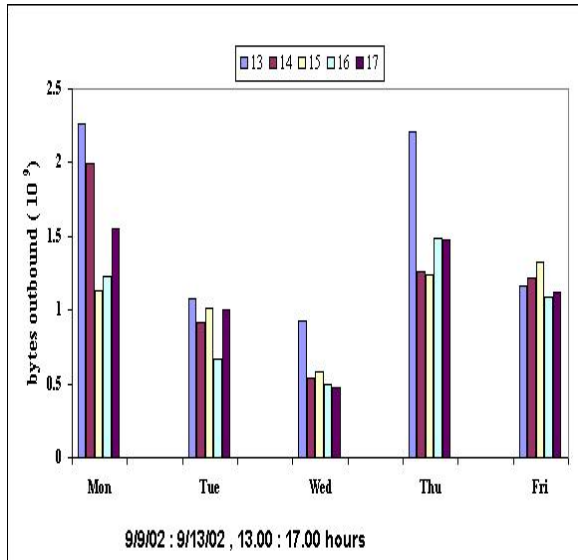
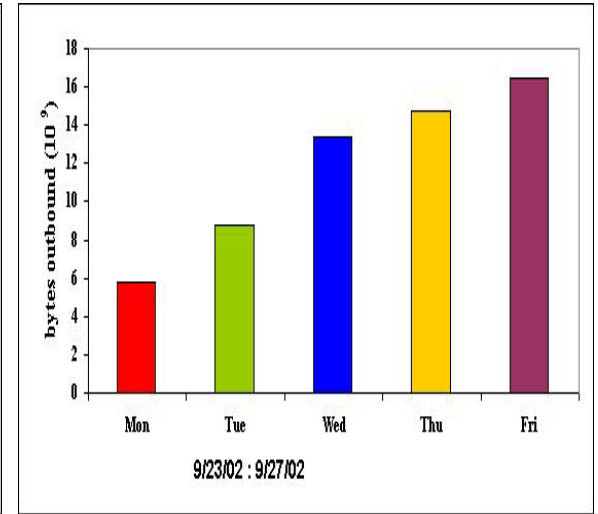
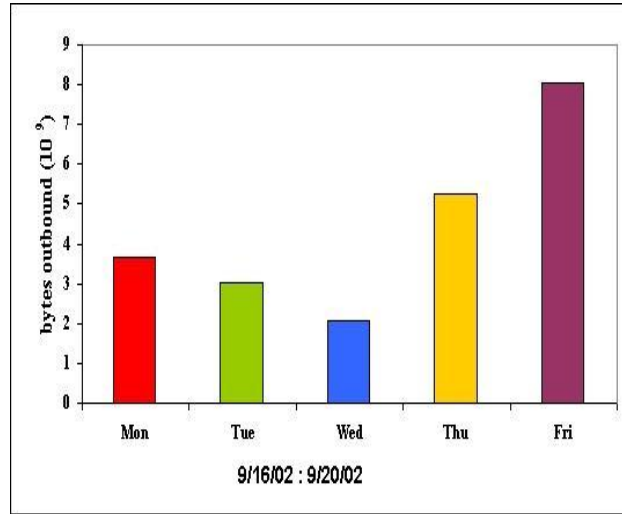
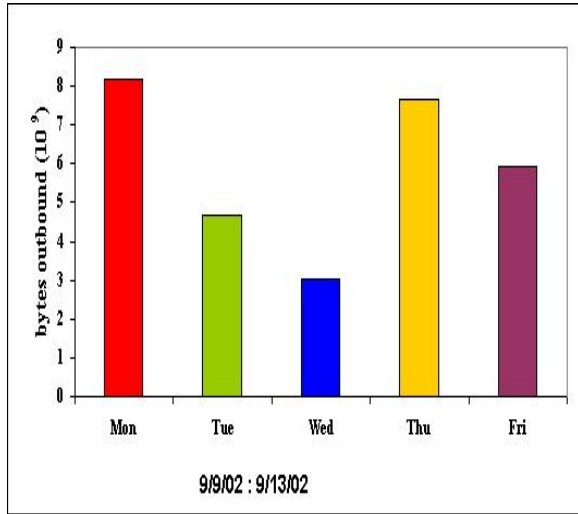
- Focus:**
- Characterize traffic at subnet, host and application level
 - Identify traffic invariants on the long time-scale
 - Identify flows that support multiplexing efficiency
 - Perform controlled traffic filtering and aggregation

Traffic Monitor: TCPDUMP packet traces collected daily at Internet router

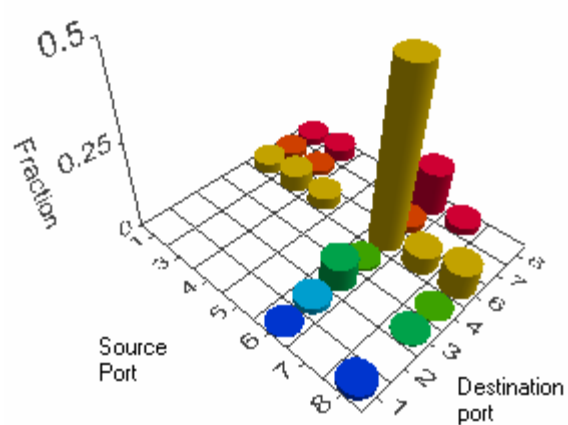
Data Form:

```
08:58:05.319735 129.63.153.137.4890 > 142.179.3.9.445: tcp 43  
08:58:05.319735 128.252.27.103.445 > 129.63.153.137.1050: tcp 0  
08:58:05.320712 209.249.123.51.80 > 129.63.73.10.49156: tcp 1460
```

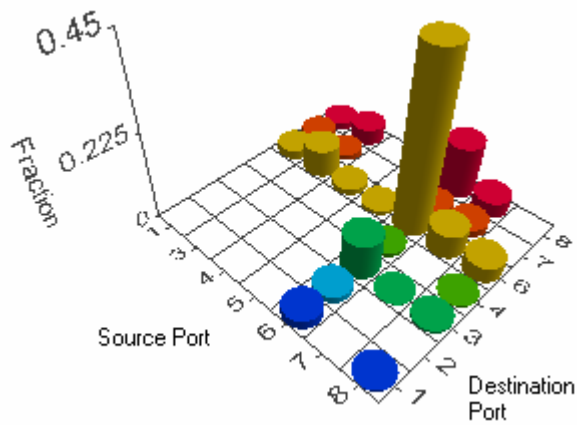
Traffic on weekly, daily & hourly time scale



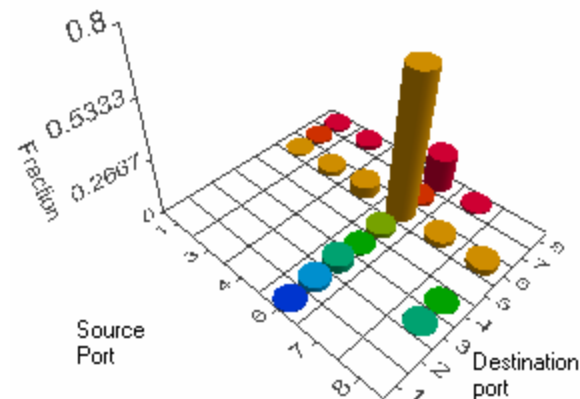
Outbound traffic distribution based on source-destination ports



Sep 11

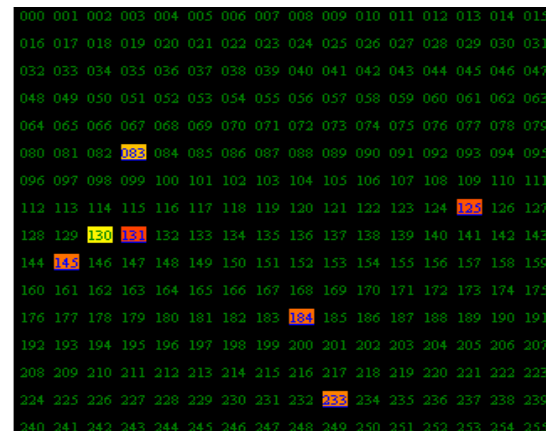
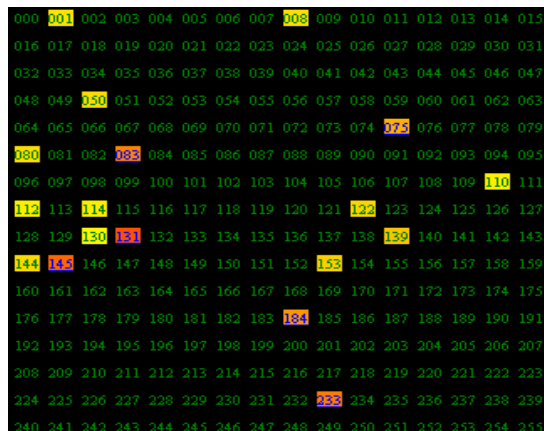
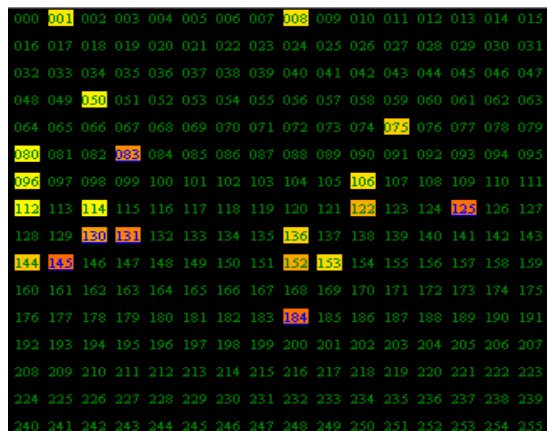


Sep 18



Sep 25

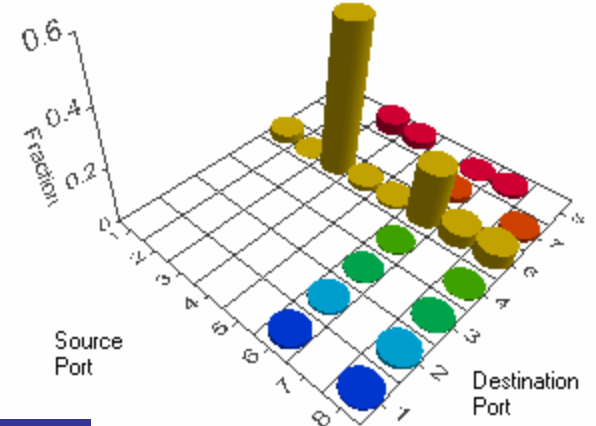
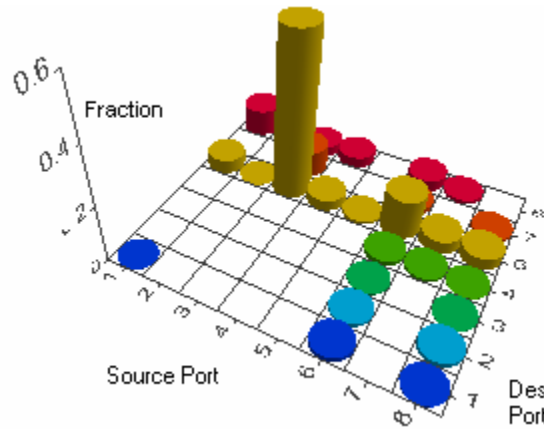
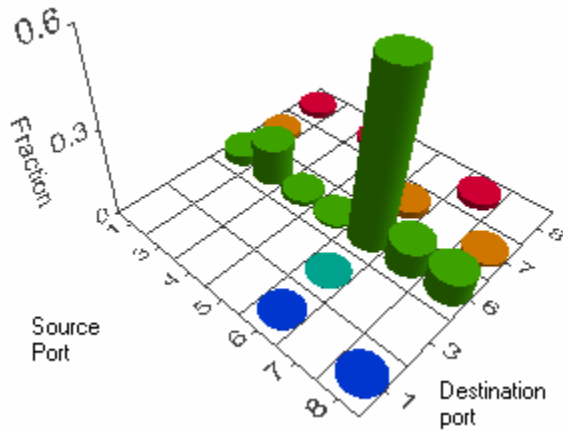
Outbound traffic distribution across subnets



1e-6

1 10 100

Inbound Traffic distribution based on source-destination ports



Inbound traffic distribution across subnets

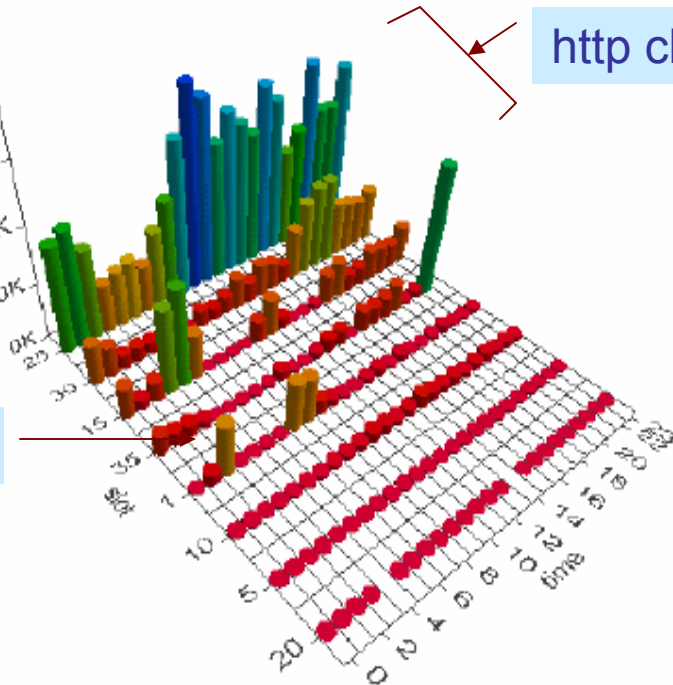
000	301	002	003	004	005	006	007	008	009	010	011	012	013	014	015
316	017	018	019	020	021	022	023	024	025	026	027	028	029	030	031
032	033	034	035	036	037	038	039	040	041	042	043	044	045	046	047
048	049	350	051	052	053	054	055	056	057	058	059	060	061	062	063
064	065	066	067	068	069	070	071	072	073	074	375	076	077	078	079
380	081	082	383	084	085	086	087	088	089	090	091	092	093	094	095
396	097	098	099	100	101	102	103	104	105	106	107	108	109	110	111
112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143
144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159
160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175
176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191
192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207
208	209	210	211	212	213	314	215	216	217	218	219	220	221	222	223
224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239
240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255

000	301	002	003	004	005	006	007	008	009	010	011	012	013	014	015
316	017	018	019	020	021	022	023	024	025	026	027	028	029	030	031
032	033	034	035	036	037	038	039	040	041	042	043	044	045	046	047
048	049	350	051	052	053	054	055	056	057	058	059	060	061	062	063
064	065	066	067	068	069	070	071	072	073	074	375	076	077	078	079
380	081	082	383	084	085	086	087	088	089	090	091	092	093	094	095
396	097	098	099	100	101	102	103	104	105	106	107	108	109	110	111
112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143
144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159
160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175
176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191
192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207
208	209	210	211	212	213	314	215	216	217	218	219	220	221	222	223
224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239
240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255

000	301	002	003	004	005	006	007	008	009	010	011	012	013	014	015
316	017	018	019	020	021	022	023	024	025	026	027	028	029	030	031
032	033	034	035	036	037	038	039	040	041	042	043	044	045	046	047
048	049	350	051	052	053	054	055	056	057	058	059	060	061	062	063
064	065	066	067	068	069	070	071	072	073	074	375	076	077	078	079
380	081	082	383	084	085	086	087	388	089	090	091	092	093	094	095
396	097	098	099	100	101	102	103	104	105	106	107	108	109	110	111
112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143
144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159
160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175
176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191
192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207
208	209	210	211	212	213	314	215	216	217	218	219	220	221	222	223
224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239
240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255

2000K
1500K
1000K
500K
0K

FTP



http clients

Application based traffic in a day

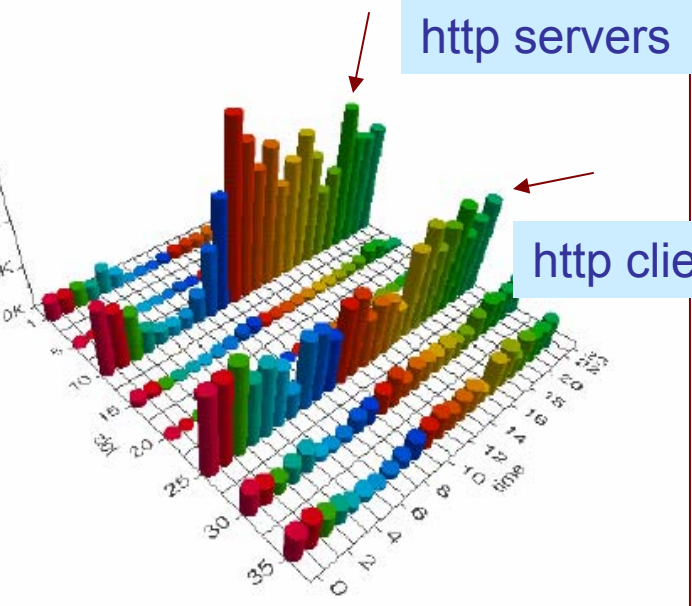
Outbound

Inbound

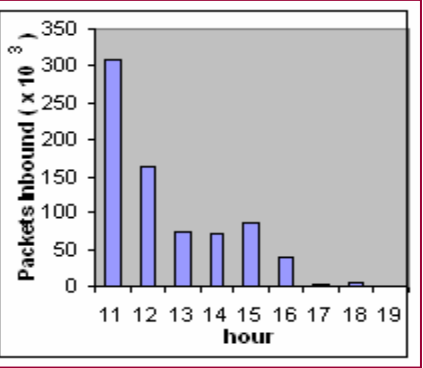
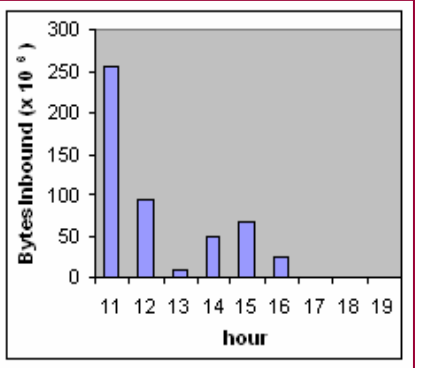
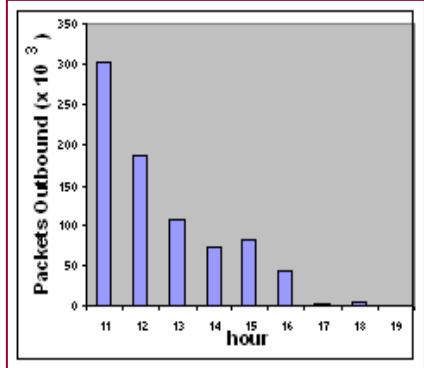
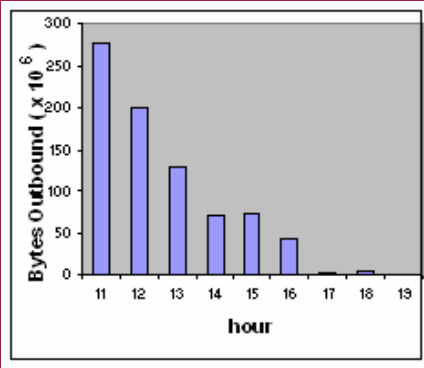
http servers

http clients

1600K
1200K
800K
400K
0K



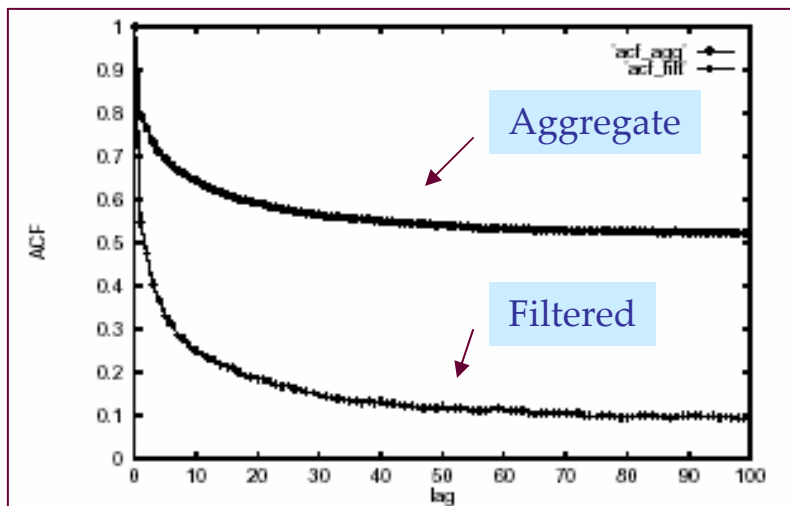
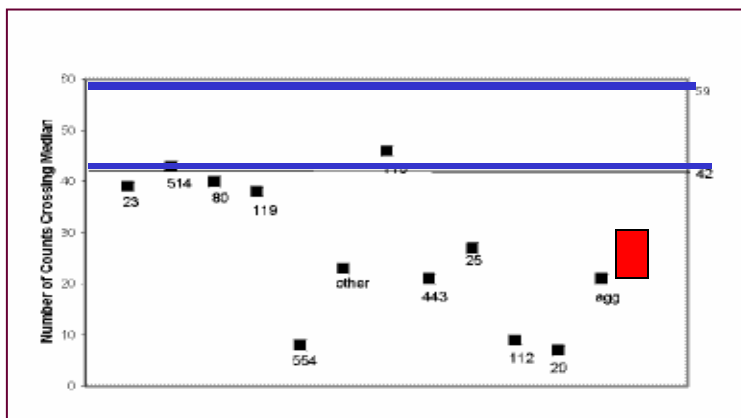
Subnet Level Statistics



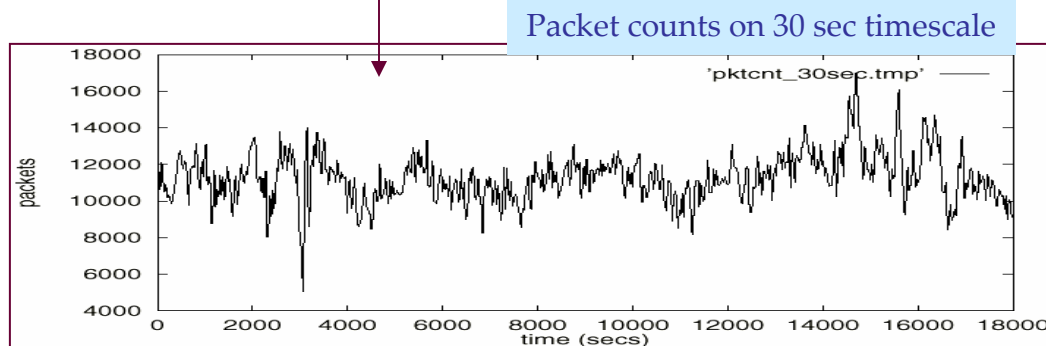
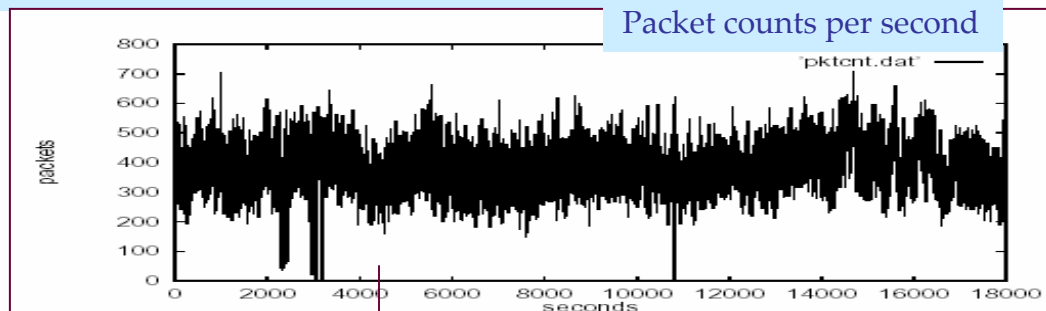
1,1 1,2 1,3 1,4 1,5 1,6 1,7 1,8 2,1 2,2 2,3 2,4 2,5 2,6 2,7 2,8 3,1 3,2 3,3 3,4 3,5 3,6 3,7 3,8 4,1 4,2 4,3 4,4 4,5 4,6 4,7 4,8 5,1 5,2 5,3 5,4 5,5 5,6 5,7 5,8 6,1 6,2 6,3 6,4 6,5 6,6 6,7 6,8 7,1 7,2 7,3 7,4 7,5 7,6 7,7 7,8 8,1 8,2 8,3 8,4 8,5 8,6 8,7 8,8	1,1 1,2 1,3 1,4 1,5 1,6 1,7 1,8 2,1 2,2 2,3 2,4 2,5 2,6 2,7 2,8 3,1 3,2 3,3 3,4 3,5 3,6 3,7 3,8 4,1 4,2 4,3 4,4 4,5 4,6 4,7 4,8 5,1 5,2 5,3 5,4 5,5 5,6 5,7 5,8 6,1 6,2 6,3 6,4 6,5 6,6 6,7 6,8 7,1 7,2 7,3 7,4 7,5 7,6 7,7 7,8 8,1 8,2 8,3 8,4 8,5 8,6 8,7 8,8	1,1 1,2 1,3 1,4 1,5 1,6 1,7 1,8 2,1 2,2 2,3 2,4 2,5 2,6 2,7 2,8 3,1 3,2 3,3 3,4 3,5 3,6 3,7 3,8 4,1 4,2 4,3 4,4 4,5 4,6 4,7 4,8 5,1 5,2 5,3 5,4 5,5 5,6 5,7 5,8 6,1 6,2 6,3 6,4 6,5 6,6 6,7 6,8 7,1 7,2 7,3 7,4 7,5 7,6 7,7 7,8 8,1 8,2 8,3 8,4 8,5 8,6 8,7 8,8	1,1 1,2 1,3 1,4 1,5 1,6 1,7 1,8 2,1 2,2 2,3 2,4 2,5 2,6 2,7 2,8 3,1 3,2 3,3 3,4 3,5 3,6 3,7 3,8 4,1 4,2 4,3 4,4 4,5 4,6 4,7 4,8 5,1 5,2 5,3 5,4 5,5 5,6 5,7 5,8 6,1 6,2 6,3 6,4 6,5 6,6 6,7 6,8 7,1 7,2 7,3 7,4 7,5 7,6 7,7 7,8 8,1 8,2 8,3 8,4 8,5 8,6 8,7 8,8	1,1 1,2 1,3 1,4 1,5 1,6 1,7 1,8 2,1 2,2 2,3 2,4 2,5 2,6 2,7 2,8 3,1 3,2 3,3 3,4 3,5 3,6 3,7 3,8 4,1 4,2 4,3 4,4 4,5 4,6 4,7 4,8 5,1 5,2 5,3 5,4 5,5 5,6 5,7 5,8 6,1 6,2 6,3 6,4 6,5 6,6 6,7 6,8 7,1 7,2 7,3 7,4 7,5 7,6 7,7 7,8 8,1 8,2 8,3 8,4 8,5 8,6 8,7 8,8																																																																																																				
10am	11am	12pm	1pm	2pm																																																																																																				
1,1 1,2 1,3 1,4 1,5 1,6 1,7 1,8 2,1 2,2 2,3 2,4 2,5 2,6 2,7 2,8 3,1 3,2 3,3 3,4 3,5 3,6 3,7 3,8 4,1 4,2 4,3 4,4 4,5 4,6 4,7 4,8 5,1 5,2 5,3 5,4 5,5 5,6 5,7 5,8 6,1 6,2 6,3 6,4 6,5 6,6 6,7 6,8 7,1 7,2 7,3 7,4 7,5 7,6 7,7 7,8 8,1 8,2 8,3 8,4 8,5 8,6 8,7 8,8	1,1 1,2 1,3 1,4 1,5 1,6 1,7 1,8 2,1 2,2 2,3 2,4 2,5 2,6 2,7 2,8 3,1 3,2 3,3 3,4 3,5 3,6 3,7 3,8 4,1 4,2 4,3 4,4 4,5 4,6 4,7 4,8 5,1 5,2 5,3 5,4 5,5 5,6 5,7 5,8 6,1 6,2 6,3 6,4 6,5 6,6 6,7 6,8 7,1 7,2 7,3 7,4 7,5 7,6 7,7 7,8 8,1 8,2 8,3 8,4 8,5 8,6 8,7 8,8	1,1 1,2 1,3 1,4 1,5 1,6 1,7 1,8 2,1 2,2 2,3 2,4 2,5 2,6 2,7 2,8 3,1 3,2 3,3 3,4 3,5 3,6 3,7 3,8 4,1 4,2 4,3 4,4 4,5 4,6 4,7 4,8 5,1 5,2 5,3 5,4 5,5 5,6 5,7 5,8 6,1 6,2 6,3 6,4 6,5 6,6 6,7 6,8 7,1 7,2 7,3 7,4 7,5 7,6 7,7 7,8 8,1 8,2 8,3 8,4 8,5 8,6 8,7 8,8	<table border="1"> <thead> <tr> <th colspan="2"></th> <th colspan="8">Destination ports</th> </tr> <tr> <th rowspan="2">Source ports</th> <th>port numbers</th> <th>1</th> <th>2</th> <th>3</th> <th>4</th> <th>5</th> <th>6</th> <th>7</th> <th>8</th> </tr> </thead> <tbody> <tr> <td>0-24</td> <td>1</td> <td>1,1</td> <td>2,1</td> <td>3,1</td> <td>4,1</td> <td>5,1</td> <td>6,1</td> <td>7,1</td> <td>8,1</td> </tr> <tr> <td>25-50</td> <td>2</td> <td>1,2</td> <td>2,2</td> <td>3,2</td> <td>4,2</td> <td>5,2</td> <td>6,2</td> <td>7,2</td> <td>8,2</td> </tr> <tr> <td>51-100</td> <td>3</td> <td>1,3</td> <td>2,3</td> <td>3,3</td> <td>4,3</td> <td>5,3</td> <td>6,3</td> <td>7,3</td> <td>8,3</td> </tr> <tr> <td>101-500</td> <td>4</td> <td>1,4</td> <td>2,4</td> <td>3,4</td> <td>4,4</td> <td>5,4</td> <td>6,4</td> <td>7,4</td> <td>8,4</td> </tr> <tr> <td>501-1000</td> <td>5</td> <td>1,5</td> <td>2,5</td> <td>3,5</td> <td>4,5</td> <td>5,5</td> <td>6,5</td> <td>7,5</td> <td>8,5</td> </tr> <tr> <td>1001-5000</td> <td>6</td> <td>1,6</td> <td>2,6</td> <td>3,6</td> <td>4,6</td> <td>5,6</td> <td>6,6</td> <td>7,6</td> <td>8,6</td> </tr> <tr> <td>5001-10000</td> <td>7</td> <td>1,7</td> <td>2,7</td> <td>3,7</td> <td>4,7</td> <td>5,7</td> <td>6,7</td> <td>7,7</td> <td>8,7</td> </tr> <tr> <td>10000+</td> <td>8</td> <td>1,8</td> <td>2,8</td> <td>3,8</td> <td>4,8</td> <td>5,8</td> <td>6,8</td> <td>7,8</td> <td>8,8</td> </tr> </tbody> </table>				Destination ports								Source ports	port numbers	1	2	3	4	5	6	7	8	0-24	1	1,1	2,1	3,1	4,1	5,1	6,1	7,1	8,1	25-50	2	1,2	2,2	3,2	4,2	5,2	6,2	7,2	8,2	51-100	3	1,3	2,3	3,3	4,3	5,3	6,3	7,3	8,3	101-500	4	1,4	2,4	3,4	4,4	5,4	6,4	7,4	8,4	501-1000	5	1,5	2,5	3,5	4,5	5,5	6,5	7,5	8,5	1001-5000	6	1,6	2,6	3,6	4,6	5,6	6,6	7,6	8,6	5001-10000	7	1,7	2,7	3,7	4,7	5,7	6,7	7,7	8,7	10000+	8	1,8	2,8	3,8	4,8	5,8	6,8	7,8	8,8
		Destination ports																																																																																																						
Source ports	port numbers	1	2	3	4	5	6	7	8																																																																																															
	0-24	1	1,1	2,1	3,1	4,1	5,1	6,1	7,1	8,1																																																																																														
25-50	2	1,2	2,2	3,2	4,2	5,2	6,2	7,2	8,2																																																																																															
51-100	3	1,3	2,3	3,3	4,3	5,3	6,3	7,3	8,3																																																																																															
101-500	4	1,4	2,4	3,4	4,4	5,4	6,4	7,4	8,4																																																																																															
501-1000	5	1,5	2,5	3,5	4,5	5,5	6,5	7,5	8,5																																																																																															
1001-5000	6	1,6	2,6	3,6	4,6	5,6	6,6	7,6	8,6																																																																																															
5001-10000	7	1,7	2,7	3,7	4,7	5,7	6,7	7,7	8,7																																																																																															
10000+	8	1,8	2,8	3,8	4,8	5,8	6,8	7,8	8,8																																																																																															
3pm	4pm	5pm																																																																																																						

Traffic Stationarity

- Stationarity test based on run length counts show that aggregate traffic departs strongly from stationary hypothesis

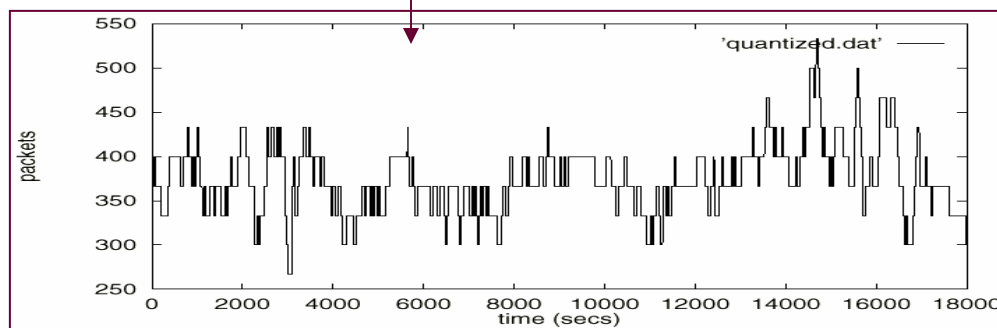


- Traffic filtering and smoothing to estimate time varying mean



Smooth, Quantize & Scale

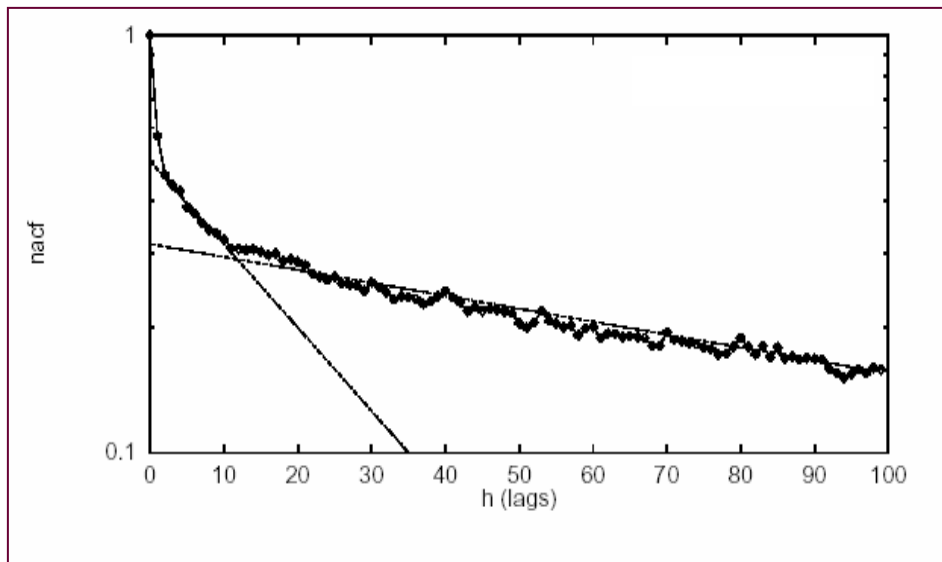
Mean count on 1 sec timescale



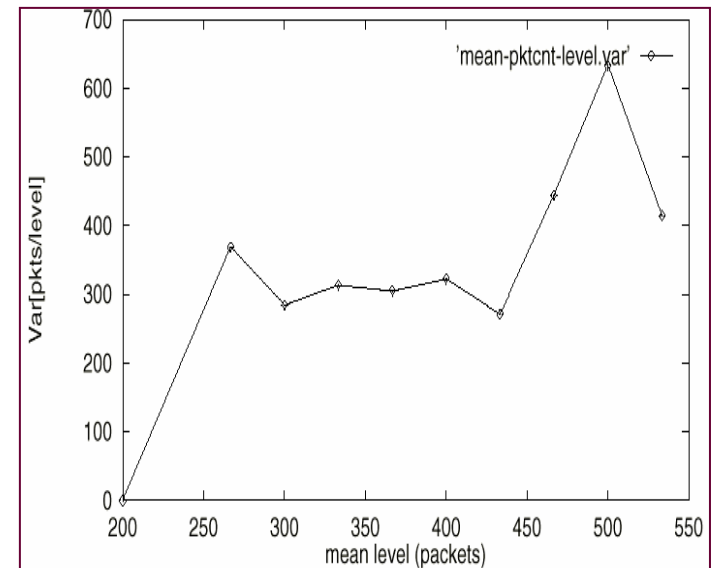
Http Client Traffic

- Characteristic Features

- Slowly varying mean component gives rise to long range correlation
- Variance changes as a function of mean level
 - Introduces non-linear features: Amplitude dependent dynamics
- Faster packet-level variations are function of server and network-response times



NACF of http packet counts (One lag = 1 second)



Level dependent variance

Http Traffic Model : Nonlinear Time Series

Packet counts / second

$y(n)$

Additive Gaussian noise: $g(n): N(0, 1)$

Process Mean: DTMC Model

$\mu(n)$

Traffic Model

$$y(n) = \mu(n) + f_1[\underline{y}(n-1), \underline{\mu}(n-1)] + f_2[\mu(n), g(n)]$$

$\underline{y}(n-1)$ and $\underline{\mu}(n-1)$:

Vectors of past observations

$$f_1[\underline{y}(n-1), \underline{\mu}(n-1)] = \sum_{i=1}^p \beta_i [y(n-i) - \mu(n-i)]$$

$\beta_i \ i = 1, 2, \dots, p$:

AR Coefficients

$$f_2[\mu(n), g(n)] = g_\mu(n) = \gamma \mu(n) g(n)$$

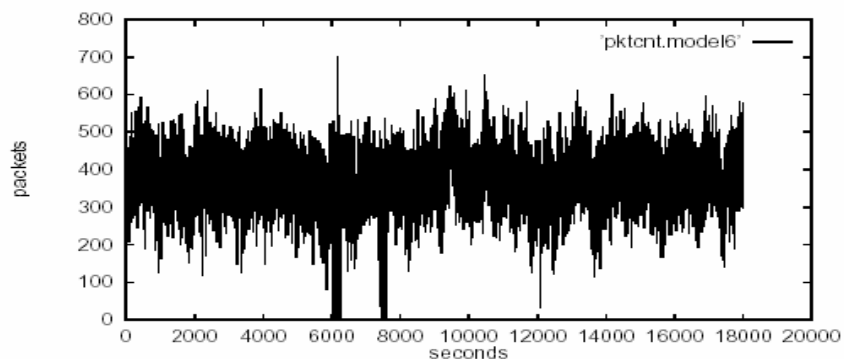
State dependent variance

$$y(n) = \mu(n) + \sum_{i=1}^p \beta_i (y(n-i) - \mu(n-i)) + g_\mu(n)$$

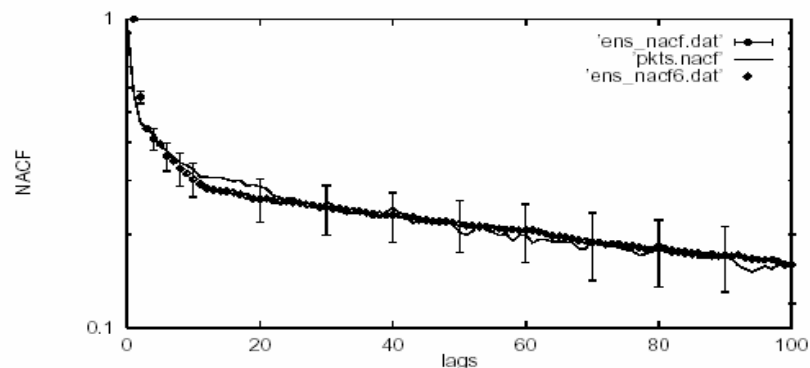
Estimate parameters: β and γ

Http Traffic Model Evaluation

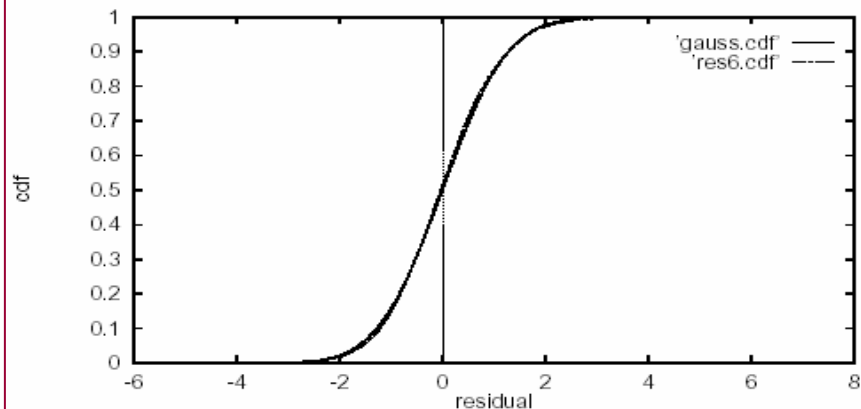
Model generated Http Packet Arrivals



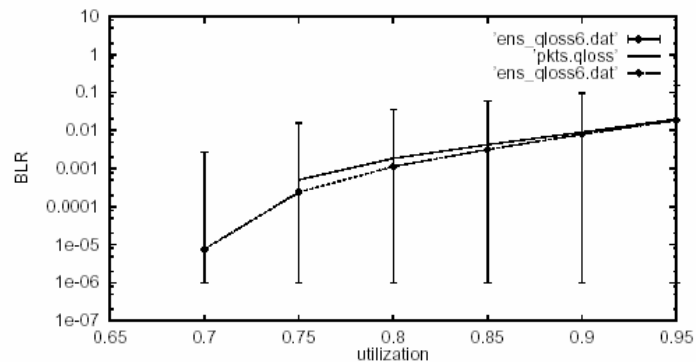
Matching Dependence Features



Model Residuals are Gaussian



Performance in Queues



Summary

Internet traffic generated by UML campus network over a duration of two years show many invariant features on the daily and hourly time scale.

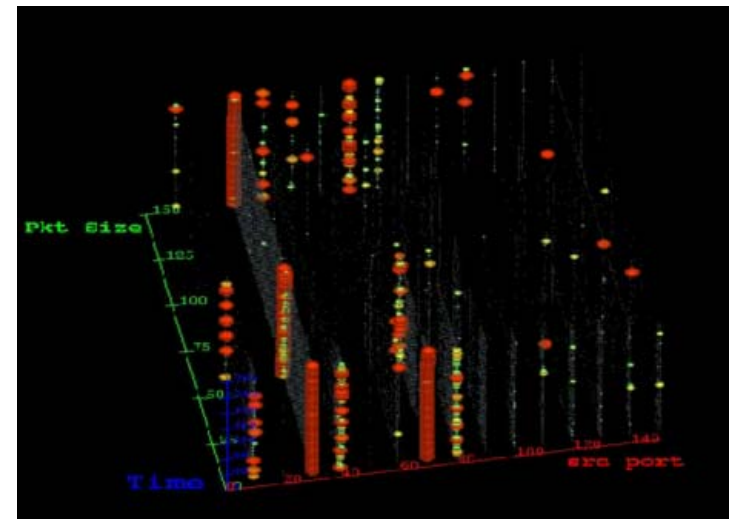
- Typically less than 20% of the active subnets contribute to over 90% of the aggregate traffic
- Less than 10% of active hosts are responsible for over 95% of the subnet traffic
- Dominant outbound traffic flows : Client access traffic
- Dominant inbound traffic flows : Http Server traffic

Network access patterns, packet sizes and packet interarrival times are application dependent

- Many application dependent traffic flows exhibit non-stationary and deterministic features on the connection time scale
- Filtering non-stationary flows leads to a significant reduction in temporal correlation.

Traffic amplitude dependent features induce non-linearity in traffic patterns

- Amplitudes above and below a threshold exhibit different correlation structures
- Suggests that traffic features in a state leading to congestion may be differentiated from that of normal operating conditions
- Non-linear time series models that capture these features shown to provide observed traffic features.



9/11/01 - 9/11/02

