Time Series Models and its Relevance to Modeling TCP SYN based DoS attacks

Cyriac James, Hema A. Murthy
Department of Computer Science & Engineering
Indian Institute of Technology Madras, India

June 23, 2011

Background: TCP SYN Attack

- A common DoS attack: TCP SYN Attack
- Limited backlog queue
  
  \[(\text{sysctl} \ - \ a \ | \ \text{grep} \ \text{ipv4.tcp.max_syn_backlog})\]

- Time out: 3, 6, 12, 24 and 48 seconds\(^1\)

\(^1\)V. Paxson and M. Allman, “RFC 2988 - Computing TCPs Retransmission Timer;”
Related Work

- Popular statistical work based on CUSUM algorithm by H. Wang et al - for the edge routers
  - SYN - FIN
  - SYN - SYN/ACK
- Drawbacks
  - Series assumed to be i.i.d
- Traffic burstiness and non-stationarity: Local-Area Network and Wide-Area Network

Related Work

Later, there were quite a few work based on *Box-Jenkins* Time Series Models - solution at the victim server

- Modeling the outstanding TCP requests\(^1\)
- Modeling the service rate\(^2\)
- Based on modeling the flow level features\(^3\)
- Modeling the web traffic\(^4\)

\(^1\)D. M. Divakaran, H. A. Murthy, and T. A. Gonsalves, "Detection of SYN flooding attacks using linear prediction analysis," ICON, 2006

Motivation for the Work

Some of the major drawbacks of these work are:

- Assumptions of time invariance and stability of the process
  - Window sizes of the order of seconds or lesser
  - Can we have a model valid for a longer period?
- Lacks description on:
  - Model identification
  - Model validation
- Relevance of linear time series models?
Network Trace

Traces collected at the edge router using tcpdump
Feature: SYN - SYN/ACK, also called half-open count
Sampling Interval: 10 seconds
- Data Set-1: 26th July 2010 to 30th July 2010
- Data Set-2: 23rd August 2010 to 27th August 2010
- Data Set-3: 20th September 2010 to 24th September 2010
Representing Network Traffic as a Discrete Time Signal

Discrete Time Signal

No access to input signals
Consider the series as a sequence of impulse responses $\mu_t$, for time $t \geq 0$

Stability of the System

- For a linear system, 
  \[ \text{Total Response} = \text{Zero-State Response} + \text{Zero-Input Response} \]
- External Stability: Zero-State Response
- Internal Stability: Zero-Input Response
- Internal Stability $\Rightarrow$ External Stability
- For internal stability, Impulse response must die-off

$$\sum_{j=0}^{\infty} |\mu_j| < \infty \quad (1)$$

$\mu_j$: Impulse response at $j^{th}$ time lag

---

Idea from the observations of Yule \(^1\)

\[
x_t = a_t + \alpha_1 a_{t-1} + \alpha_2 a_{t-2} + \ldots \tag{2}
\]

- \(x_t\): Output Signal at time \(t\)
- \(a_t, a_{t-1}, \ldots\): Random shocks or white noise process
- \(\alpha_1, \alpha_2, \ldots\): Model coefficients
- Also called Linear Filter Model
- Stationarity: First and Second order moments finite and independent of time\(^2\)
- LTI and Stability ⇔ Stationarity
- Can be used to build models for prediction


**Auto-Regressive (AR) Model**

An AR model can be written as

$$x_t = \alpha_1 x_{t-1} + \alpha_2 x_{t-2} + \ldots + \alpha_p x_{t-p} + a_t$$  \hspace{1cm} (3)

$x_t, x_{t-1}, \ldots$: Output values

$\alpha_1, \alpha_2, \ldots$: Model coefficients, where $p$ is the model order

$a_t$: Random shock at time $t$

- Can be written as an infinite series of random shocks
- Consider an AR(2) model:

$$x_t = \alpha_1 x_{t-1} + \alpha_2 x_{t-2} + a_t$$  \hspace{1cm} (4)

$$x_{t-1} = \alpha_1 x_{t-2} + \alpha_2 x_{t-3} + a_{t-1}$$  \hspace{1cm} (5)

$$x_{t-2} = \alpha_1 x_{t-3} + \alpha_2 x_{t-4} + a_{t-2}$$  \hspace{1cm} (6)

$$\vdots$$

$$x_t = a_t + \psi_1 a_{t-1} + \psi_2 a_{t-2} + \ldots$$  \hspace{1cm} (7)

**Computing ACF:**

$$E(x_t x_{t-k}) = E(a_t x_{t-k} + \psi_1 a_{t-1} x_{t-k} + \psi_2 a_{t-2} x_{t-k} + \ldots)$$  \hspace{1cm} (8)

$$\gamma_k = E(x_{t-k} a_{t-1}) + \psi_1 E(x_{t-k} a_{t-2}) + \psi_2 E(x_{t-k} a_{t-3}) + \ldots$$  \hspace{1cm} (9)

where $\gamma_k$ is the autocovariance. Above equation can be generalised into:

$$\gamma_k = \sigma_a^2 \sum_{j=0}^{\infty} \psi_j \psi_{j+k}$$  \hspace{1cm} (10)

$\sigma_a^2$: Variance of $a_t$ with mean zero

In terms of the impulse response (ACF), it becomes

$$\rho_k = \frac{\sigma_a^2 \sum_{j=0}^{\infty} \psi_j \psi_{j+k}}{\gamma_0}$$  \hspace{1cm} (11)

- Hence, an AR process is an infinite impulse response system
- For stability $\Rightarrow \sum_{j=0}^{\infty} |\psi_j| < \infty$
Time Series Models

**Auto-Regressive(AR) Model**

Multiply with $x_{t-k}$ on Equation (4) and take expectation on both sides:

$$\gamma_k = \alpha_1 \gamma_{k-1} + \alpha_2 \gamma_{k-2}$$  \hspace{1cm} (12)

Dividing by $\gamma_0$, (12) becomes:

$$\rho_k = \alpha_1 \rho_{k-1} + \alpha_2 \rho_{k-2}$$  \hspace{1cm} (13)

$$\rho_k - \alpha_1 \rho_{k-1} - \alpha_2 \rho_{k-2} = 0$$  \hspace{1cm} (14)

Characteristic equation:

$$\lambda^2 - \alpha_1 \lambda - \alpha_2 = 0$$  \hspace{1cm} (15)

The general solution is of the form:

$$\rho_k = C_1 (\lambda_1)^k + C_2 (\lambda_2)^k$$  \hspace{1cm} (16)

$\lambda_1, \lambda_2$: Roots (if distinct)

$C_1$ and $C_2$: Arbitrary constants

- For Stability $\Rightarrow |\lambda_1| < 1$ and $|\lambda_2| < 1$

- Yule-Walker Equation - Estimating model coefficients

---

**Moving Average(MA) Model**

An MA model can be written as

$$x_t = a_t - \psi_1 a_{t-1} - \psi_2 a_{t-2} - ... - \psi_q a_{t-q}$$  \hspace{1cm} (17)

$x_t$: Output Signal at time $t$

$a_t, a_{t-1}, ...$: Random shocks or white noise process

$\psi_1, \psi_2, ... , \psi_q$: Model coefficients, where $q$ is the model order

- Finite linear filter model
- Can be written as an infinite series of past values
- Consider an MA model of order 1

$$x_t = a_t - \psi_1 a_{t-1}$$  \hspace{1cm} (18)
Moving Average (MA) Model

Multiply with $x_{t-k}$ on equation (18) and take expectation on both sides,

$$
\gamma_k = E(a_t x_{t-k} - \psi_1 a_{t-1} x_{t-k})
\gamma_0 = E(a_t x_t - \psi_1 a_{t-1} x_t)
$$

(19)

$$
\gamma_0 = E(a_t (a_t - \psi_1 a_{t-1}) - \psi_1 a_{t-1} (a_t - \psi_1 a_{t-1}))
\gamma_0 = \sigma_a^2 + \psi_1^2 \sigma_a^2
$$

(20)

$$
\gamma_1 = -\psi_1 \sigma_a^2
$$

(21)

$$
\gamma_2 = 0
$$

(22)

- $\gamma_k = 0$ for all values of $k > 1$
- Hence, an MA process is a finite impulse response system
- Time invariant MA process is always stationary

Duality Property: For Model Identification

- For an AR($p$) process, ACF converges slowly, but PACF cut-off after lag $p$
- For an MA($q$) process, PACF converges slowly, but ACF cut-off after lag $q$
Time Series Models

Time Series Transformations

- Study on Time invariant feature - inconclusive
- Transformation of Time Series
- Averaging and Differencing

Figure: Average Time Series
Difference Series

**Figure: Difference Time Series**

Analysis and Results
Analysis and Results

Stationarity Check: Mean Estimation

### Data Set-1
<table>
<thead>
<tr>
<th>Day</th>
<th>Monday</th>
<th>Tuesday</th>
<th>Wednesday</th>
<th>Thursday</th>
<th>Friday</th>
<th>Average</th>
</tr>
</thead>
</table>

### Data Set-2
<table>
<thead>
<tr>
<th>Day</th>
<th>Monday</th>
<th>Tuesday</th>
<th>Wednesday</th>
<th>Thursday</th>
<th>Friday</th>
<th>Average</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>7.8968</td>
<td>8.1568</td>
<td>8.4121</td>
<td>8.4447</td>
<td>8.2699</td>
<td>8.2355</td>
</tr>
</tbody>
</table>

### Data Set-3
<table>
<thead>
<tr>
<th>Day</th>
<th>Monday</th>
<th>Tuesday</th>
<th>Wednesday</th>
<th>Thursday</th>
<th>Friday</th>
<th>Average</th>
</tr>
</thead>
</table>

**Mean: Original Series**

### Data Set-1
<table>
<thead>
<tr>
<th>Day</th>
<th>Monday</th>
<th>Tuesday</th>
<th>Wednesday</th>
<th>Thursday</th>
<th>Friday</th>
<th>Average</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>5.5403</td>
<td>5.0008</td>
<td>5.6499</td>
<td>5.7435</td>
<td>5.3730</td>
<td>5.4615</td>
</tr>
</tbody>
</table>

### Data Set-2
<table>
<thead>
<tr>
<th>Day</th>
<th>Monday</th>
<th>Tuesday</th>
<th>Wednesday</th>
<th>Thursday</th>
<th>Friday</th>
<th>Average</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>5.0499</td>
<td>5.0958</td>
<td>5.1332</td>
<td>5.0452</td>
<td>5.2722</td>
<td>5.1292</td>
</tr>
</tbody>
</table>

### Data Set-3
<table>
<thead>
<tr>
<th>Day</th>
<th>Monday</th>
<th>Tuesday</th>
<th>Wednesday</th>
<th>Thursday</th>
<th>Friday</th>
<th>Average</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>4.8475</td>
<td>4.2121</td>
<td>3.7834</td>
<td>3.9591</td>
<td>3.9951</td>
<td>4.1017</td>
</tr>
</tbody>
</table>

**Mean: Difference Series**

### Data Set-1
<table>
<thead>
<tr>
<th>Day</th>
<th>Monday</th>
<th>Tuesday</th>
<th>Wednesday</th>
<th>Thursday</th>
<th>Friday</th>
<th>Average</th>
</tr>
</thead>
</table>

### Data Set-2
<table>
<thead>
<tr>
<th>Day</th>
<th>Monday</th>
<th>Tuesday</th>
<th>Wednesday</th>
<th>Thursday</th>
<th>Friday</th>
<th>Average</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>7.8969</td>
<td>8.1533</td>
<td>8.4100</td>
<td>8.4461</td>
<td>8.2724</td>
<td>8.23572</td>
</tr>
</tbody>
</table>

### Data Set-3
<table>
<thead>
<tr>
<th>Day</th>
<th>Monday</th>
<th>Tuesday</th>
<th>Wednesday</th>
<th>Thursday</th>
<th>Friday</th>
<th>Average</th>
</tr>
</thead>
</table>

**Mean: Average Series**

Cyriac James, Hema A. Murthy (IITM)  
June 23, 2011 23 / 35
Stationarity Check: Autocorrelation Estimation of Difference Series

(g) ACF: Data Set-1
(h) ACF: Data Set-2
(i) ACF: Data Set-3

Stationarity Check: Autocorrelation Estimation of Average Series

(j) ACF: Data Set-1
(k) ACF: Data Set-2
(l) ACF: Data Set-3
Analysis and Results

Stability Check

(m) Roots: Orig. Series
(n) Roots: Diff. Series
(o) Roots: Avg. Series

Model Identification

(p) Sample ACF - Difference Series
(q) Sample PACF - Difference Series
Analysis and Results

Modeling and Prediction

- Only AR and no MA component
- AR model of order 2 - from PACF
- Parameter Estimation: Yule-Walker Method
- Training: One day data

Model Validation: ACF Spread of Prediction Error

(r) Data Set-1  
(s) Data Set-2  
(t) Data Set-3
Model Validation: Root Mean Square Error

<table>
<thead>
<tr>
<th>Day</th>
<th>Model Mon-1</th>
<th>Model Mon-2</th>
<th>Model Mon-3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mon-1</td>
<td>9.0393</td>
<td>9.0493</td>
<td>9.0509</td>
</tr>
<tr>
<td>Tue-1</td>
<td>6.9171</td>
<td>6.8318</td>
<td>6.8235</td>
</tr>
<tr>
<td>Wed-1</td>
<td>7.5437</td>
<td>7.6765</td>
<td>7.5391</td>
</tr>
<tr>
<td>Thur-1</td>
<td>7.6595</td>
<td>7.6819</td>
<td>7.6610</td>
</tr>
<tr>
<td>Fri-1</td>
<td>6.2821</td>
<td>6.3041</td>
<td>6.2892</td>
</tr>
<tr>
<td>Mon-2</td>
<td>7.6121</td>
<td>7.6061</td>
<td>7.6297</td>
</tr>
<tr>
<td>Tue-2</td>
<td>7.7220</td>
<td>7.7161</td>
<td>7.7566</td>
</tr>
<tr>
<td>Thur-2</td>
<td>7.5915</td>
<td>7.5793</td>
<td>7.6356</td>
</tr>
<tr>
<td>Fri-2</td>
<td>7.7785</td>
<td>7.7825</td>
<td>7.7899</td>
</tr>
<tr>
<td>Mon-3</td>
<td>7.6859</td>
<td>7.7005</td>
<td>7.6736</td>
</tr>
<tr>
<td>Tue-3</td>
<td>6.4507</td>
<td>6.4603</td>
<td>6.4648</td>
</tr>
<tr>
<td>Wed-3</td>
<td>7.5276</td>
<td>7.5402</td>
<td>7.5327</td>
</tr>
<tr>
<td>Thur-3</td>
<td>8.9074</td>
<td>8.8949</td>
<td>8.9275</td>
</tr>
<tr>
<td>Fri-3</td>
<td>8.1178</td>
<td>8.1250</td>
<td>8.1197</td>
</tr>
</tbody>
</table>

**Figure:** RMSE: Model built on Monday Traffic

- Mean and Variance consistent across all models
- Model valid for a long period of time
- Gives an estimate of threshold to be fixed
Analysis and Results

Prediction of SYN Attack

- Trace driven Simulation
- Results are ensemble average over 50 such simulated attacks
- SYN rate: 10 syn/sec to 20 syn/sec
- Threshold error based on RMSE

Detection Efficacy

- (a) False Positive Vs False Negative
  - Probability of False Positive (FP)
  - Probability of False Negative (FN)

- (b) Detection Delay
  - Detection Delay (in seconds)
**Conclusion**

- Systematic approach
  - Stationarity
  - Stability
  - Appropriate Transformation
- Stressed on model identification and validation
- Demonstrated the efficacy of the model
  - For modeling normal traffic
  - For longer period of time
  - Detecting TCP SYN DoS attacks
- Effective for *Distributed* SYN attacks as well
- Approach can be extended for other DoS attacks as well