APPLICATION OF CUSUM METHOD FOR DETECTION OF DoS ATTACS

Vladimir Mazalov and Natalia Nikitina

Institute of Applied Mathematical Research,
Karelian Research Center of RAS
Petrozavodsk, Russia
E-mail: vmazalov@krc.karelia.ru

Introduction. DoS (Denial of Service) - attack is regular traffic + artificial traffic.

Page [1954] introduced CUSUM method.

Let $\{x_n\}$, $n = 1, 2, ..., \theta_0 - 1$ are iid with CDF $F(x, \alpha_0)$ and after $\theta \geq 0$ $x_n \sim F(x, \alpha)$, where $\alpha \neq \alpha_0$.

$$S_n = (S_{n-1} + q(x_n))^+, \tag{1}$$

where $z^+ = \max(0, z)$, $q(x) = \log \frac{dF(x,\alpha)}{dF(x,\alpha_0)}$, $S_0 = s \geq 0$.

$$\tau_b = \text{inf}\{n > 0 : S_n \geq b\} \tag{2}$$

Two main characteristics:

ARL (Average Run Length): $(\theta = \infty)$;

AD (Average Delay): $\theta = 0$.

For initial condition $S_0 = s$:

$$ARL = j_\infty(s) = E_s\{\tau_b|\theta = \infty\} \tag{3}$$

$$AD = j_0(s) = E_s\{\tau_b|\theta = 0\} \tag{4}$$

For some distributions:

$S_n = (S_{n-1} + x_n - a)^+$ where $a = const$, ARL is determined by

$$j(s) = 1 + E_s\{I(0 < S_1 < b)j(S_1)\} + P_s\{S_1 = 0\}j(0), \quad s < b. \quad (5)$$

For AD that is analogous with condition $\theta = 0$.

Shiryaev [1996] showed minimax optimality of the method.

Bernoulli distribution.

Let x_n, $n = 1, 2, ...$ are Bernoulli with parameter α_0:

$$F(x) = \begin{cases} 0, & x < 0 \\ 1 - \alpha_0, & 0 \leq x < 1 \\ 1, & x \geq 1 \end{cases}$$

Suppose that after change point x_n are Bernoulli with $\alpha > \alpha_0$,

$$S_n = \left(S_{n-1} + \ln \frac{\alpha^{x_n}(1-\alpha)^{1-x_n}}{\alpha_0^{x_n}(1-\alpha_0)^{1-x_n}} \right)^+ .$$

If $\alpha < \alpha_0$ then we change $\alpha_0' = 1 - \alpha_0$, $\alpha' = 1 - \alpha$.

$\Rightarrow$

$$q(x_n) = \ln \frac{\alpha^{x_n}(1-\alpha)^{1-x_n}}{\alpha_0^{x_n}(1-\alpha_0)^{1-x_n}} = \left(\ln \frac{\alpha}{\alpha_0} - \ln \frac{1-\alpha}{1-\alpha_0}\right) x_n + \ln \frac{1-\alpha}{1-\alpha_0} = \gamma x_n + \beta.$$

$\alpha > \alpha_0$, $\Rightarrow$ $\gamma > 0$, $\beta < 0$ and $\gamma + \beta > 0$.

For ARL:

$$S_1 = \begin{cases} 0, & x_1 = 0 \quad s + \beta \leq 0 \\ s + \beta > 0, & x_1 = 0 \quad s + \beta > 0 \\ s + \gamma + \beta > 0, & x_1 = 1. \end{cases}$$

$$E_s\{I(0 < S_1 < b)j(S_1)\} = \alpha_0 I(s+\gamma+\beta < b)j(s+\gamma+\beta)+$$
$$+(1\text{-}\alpha_0)I(0 < s+\beta < b)j(s+\beta)$$

$$P_s(S_1 = 0) = (1-\alpha_0)I(s \le -\beta)$$

$\Rightarrow$

$$j(s) = \begin{cases} 1+\alpha_0 j(s+\gamma+\beta)+(1-\alpha_0)j(s+\beta)^+, & 0 \le s < b \\ 0, & s = b \end{cases} \tag{6}$$

For AD we change α_0 on α.

Depending on α_0 and α there are different equation forms.

1. **Let** $[\gamma + \beta] = [-\beta]$. Without loss of generality

   $-\beta = 1$, $b^* = \frac{b}{-\beta}$, $z = \frac{\gamma+\beta}{-\beta}$, $[z] = 1$.

$$j(s) = \begin{cases} 1 + \alpha_0 j(s+1) + (1-\alpha_0) j(s-1)^+, 0 \le s < b^* \\ 0, s \ge b^* \end{cases} \tag{7}$$

   For $0 \le s \le b^*$:

$$\begin{cases} j(0) & = 1 + \alpha_0 j(1) + (1-\alpha_0) j(0) \\ \dots & \\ j(n) & = 1 + \alpha_0 j(n+1) + (1-\alpha_0) j(n-1) \\ \dots & \\ j(b^*-1) & = 1 + \alpha_0 j(b^*) + (1-\alpha_0) j(b^*-2) \\ j(b^*) & = 0 \end{cases} \tag{8}$$

(a) Let $\alpha_0 = 0.5$. Denote $j(0) = t$. Then

$$\begin{cases} j(0) & = t \\ j(1) & = t - 2 \\ j(2) & = t - 6 \\ \quad \ldots & \\ j(n) & = t - 2(1 + 2 + \ldots + n) = t - n(n+1) \\ \quad \ldots & \\ j(b) & = t - b(b+1) \end{cases}$$

$j(b) = 0 \rightarrow t = b(b+1) \rightarrow$

$$j(s) = b^*(b^*+1) - s(s+1)$$

(b) Let $\alpha_0 \neq 0.5$.

Proposition 1. The solution for $\alpha_0 \neq 0.5$ is

$$j(n) = \frac{(2\alpha_0 - 1)(b - n) + \frac{(1-\alpha_0)^{b+1}}{\alpha_0^b} - \frac{(1-\alpha_0)^{n+1}}{\alpha_0^n}}{(2\alpha_0 - 1)^2},\ 0 \leq n \leq b^*.$$

2. Let $\gamma + \beta < -\beta$, i.e. $\begin{cases} 0 < \alpha_0 \leq 0.5, \\ \alpha > 1 - \alpha_0, \end{cases}$ or $0.5 < \alpha_0 < 1$.

Changing arguments

$\gamma + \beta = 1, b^* = \frac{b}{\gamma+\beta}, z = \frac{-\beta}{\gamma+\beta}$.

j(s)= $\begin{cases} 1 + \alpha_0 j(s+1) + (1-\alpha_0) j(s-m)^+, 0 \leq s < b^* \\ 0, s \geq b^* \end{cases}$

Where $m = [z] > 1$.

For $0 \le s \le b^*$: $$\begin{cases} j(0) & = 1 + \alpha_0 j(1) + (1-\alpha_0) j(0) \\ \dots & \\ j(m) & = 1 + \alpha_0 j(m+1) + (1-\alpha_0) j(0) \\ j(m+1) & = 1 + \alpha_0 j(m+2) + (1-\alpha_0) j(1) \\ \dots & \\ j(b^*-1) & = 1 + \alpha_0 j(b^*) + (1-\alpha_0) j(b^*-m-1) \\ j(b^*) & = 0 \end{cases}$$

Generating function $\phi(z)$.

$$\phi(z) = \sum_{n=0}^{\infty} j_n z^n = \frac{j_0 \alpha_0 (z-1) - j_0 (1-\alpha_0)(z^{m+1} - z) + z}{(\alpha_0 - z + (1-\alpha_0) z^{m+1})(z-1)}$$

Lemma. The equation $(1-\alpha_0)z^{m+1}+\alpha_0-z=p(z)$ has no multiple roots for $\alpha_0 \neq m/(m+1)$, otherwise, there are double roots 1.

$\Rightarrow$ For $\alpha_0 \neq \frac{m}{m+1}$:

$$\phi(z) = \frac{1}{1-\alpha_0} \times \frac{z}{(z-1)^2(\sum_{i=1}^m z^i - \frac{\alpha_0}{1-\alpha_0})} + j_0 \frac{1}{1-z} = \frac{1}{1-\alpha_0} \times$$

$$\times \left(\frac{A}{(z-1)^2} + \frac{B}{z-1} + \frac{C_1}{z-z_1} + \ldots + \frac{C_m}{z-z_m}\right) + j_0 \frac{1}{1-z},$$

where $z_1, ..., z_m$ are roots of $\sum_{i=1}^m z^i - \frac{\alpha_0}{1-\alpha_0} = 0$, and constants A, B, C_1,...,C_m are determined by the equations:

$$
\begin{cases}
B + \sum_{i=1}^{m} C_i & = 0 \\
A + \sum_{i=1}^{m} C_i(z_i - 1) & = 0 \\
A + \sum_{i=1}^{m} C_i z_i(z_i - 1) & = 0 \\
\cdots & \\
A + \sum_{i=1}^{m} C_i z_i^{m-2}(z_i - 1) & = 0 \\
A - \frac{B}{1-\alpha_0} + \sum_{i=1}^{m} C_i\left(\frac{-2\alpha_0}{(1-\alpha_0)z_i} + \frac{z_i^{m-1}-1}{z_i-1}\right) & = 1 \\
A\frac{\alpha_0}{\alpha_0-1} + B\frac{\alpha_0}{1-\alpha_0} + \sum_{i=1}^{m} C_i\frac{\alpha_0}{(1-\alpha_0)z_i} & = 0
\end{cases}
$$

$$\phi(z) = \sum_{n=0}^{\infty} \left(\tfrac{A(n+1)}{1-\alpha_0} + j_0 - \tfrac{B}{1-\alpha_0} - \sum_{i=1}^{m} \tfrac{C_i}{1-\alpha_0} \tfrac{1}{z_i^{n+1}}\right) z^n = \sum_{n=0}^{\infty} j_n z^n$$

Find j_0 from condition $j(b^*) = 0$:

$$j_0 = \sum_{i=1}^{m} \frac{C_i}{1-\alpha_0} \frac{1}{z_i^{b^*+1}} - \frac{A}{1-\alpha_0}(b^*+1) + \frac{B}{1-\alpha_0}$$

Thus, for $\alpha_0 \neq \frac{m}{m+1}$

$$j(n) = \frac{A}{1-\alpha_0}(n-b^*) + \sum_{i=1}^{m} \frac{C_i(1-z_i^{b^*-n})}{(1-\alpha_0) z_i^{b^*+1}} \qquad (9)$$

For $\alpha_0 = \frac{m}{m+1}$ the same arguments:

3. Let $\gamma + \beta > -\beta$, i.e. $\begin{cases} 0 < \alpha_0 < 0.5, \\ \alpha_0 < \alpha < 1 - \alpha_0. \end{cases}$

Change arguments $\beta = -1, b^* = \frac{b}{-\beta}, z = \frac{\gamma+\beta}{-\beta}$.

Then

$$j(s) = \begin{cases} 1 + \alpha_0 j(s+m) + (1-\alpha_0) j(s-1)^+, 0 \leq s < b^* \\ 0, s \geq b^* \end{cases}$$

where $m = [z] > 1$.

For $0 \leq s \leq b^*$:

$$
\begin{cases}
j(0) & = 1 + \alpha_0 j(m) + (1-\alpha_0) j(0) \\
j(1) & = 1 + \alpha_0 j(m+1) + (1-\alpha_0) j(0) \\
j(2) & = 1 + \alpha_0 j(m+2) + (1-\alpha_0) j(1) \\
\ldots & \\
j(b^* - m) & = 1 + \alpha_0 j(b^*) + (1-\alpha_0) j(b^* - m - 1) \\
\ldots & \\
j(b^* - 1) & = 1 + \alpha_0 j(b^* - 1 + m) + (1-\alpha_0) j(b^* - 2) \\
j(b^*) & = 0
\end{cases}
$$

Changing

$j_n = J_n + \frac{n}{1-\alpha_0(m+1)}$ for $\alpha_0 \neq \frac{1}{m+1}$

$j_n = J_n - \frac{n^2}{m}$ for $\alpha_0 = \frac{1}{m+1}$:

$$J_n = \alpha_0 J_{n+m} + (1-\alpha_0)J_{n-1}$$

Characteristic equation:

$$\alpha_0\lambda^{m+1} - \lambda + 1 - \alpha_0 = 0. \tag{9}$$

From Lemma changing $\alpha_0 = 1 - \alpha_0'$ it follows that the (9) has no multiple roots if $\alpha_0 \neq \frac{1}{m+1}$. Then

j(n)=$\frac{n}{1-\alpha_0(m+1)} + \sum\limits_{i=0}^{m} C_i\lambda_i^n$, where λ_0,...,λ_m are roots of(9)($\lambda_0 = 1$), and constants C_0,...,C_m are determined by equations:

$$\begin{cases} \sum_{i=1}^{m} C_i(1 - z_i^m) &= \frac{1}{\alpha_0} + \frac{m}{1-\alpha_0(m+1)} \\ \alpha_0 C_0 + \sum_{i=1}^{m} C_i(z_i^{b^*-1} - (1-\alpha_0) z_i^{b^*-2}) &= \frac{\alpha_0(b^*-1+m)}{\alpha_0-1+\alpha_0 m} \\ \dots & \\ \alpha_0 C_0 + \sum_{i=1}^{m} C_i(z_i^{b^*-m} - (1-\alpha_0) z_i^{b^*-m-1}) &= \frac{\alpha_0 b^*}{\alpha_0-1+\alpha_0 m} \end{cases}$$

$j(0) = j_0(b, \alpha_0)$. $j_0(b, \alpha_0)$ is increasing in b.

So, minimum of $AD = j_0(b)$ in condition that the false alarm is not large ($ARL \geq a$) yields $\mathbf{b} = min\{b : j_\infty(b) \geq a\}$.

The mean delay is $j_0(\mathbf{b})$.

Change of protocol

Attacker doesnt know α_0.

Denote z_n are the jobs in the traffic, $n = 1, 2, \ldots$. Let in regular traffic z_n are distributed with some CDF F_z with median m.

Introduce x_n taking 0, if $z_n < m$, and 1, if $z_n \geq m$.

Then for regular case the frequency of 0 and 1 are equal, so $\alpha_0 = 0.5$.

After intrusion α is changing in respect of $\alpha_0 = 0.5$. If $\alpha > 0.5$, then number of 1 is larger than 0.

Change the FIFO protocol.

Collect the jobs in some buffer.

Generate random variable z with CDF F_z and chooze the job in buffer which size is larger than z and lies closer to z than other jobs.

Numerical experiments for normal distribution: regular 1000 jobs and additional 10000 intrusions.

ξ_0	ξ_1	**M**	Rate of mistakes	Mean delay
$N(0.7, 0.1)$	$N(0.3, 0.1)$	1000	0.21	-0.04
$N(0.7, 0.1)$	$N(0.3, 0.1)$	2000	0.02	0.13
$N(0.7, 0.1)$	$N(0.3, 0.1)$	3000	0.004	0.15
$N(0.7, 0.1)$	$N(0.4, 0.1)$	1000	0.40	-0.04
$N(0.7, 0.1)$	$N(0.4, 0.1)$	2000	0.14	0.25
$N(0.7, 0.1)$	$N(0.4, 0.1)$	3000	0.057	0.39
$N(0.7, 0.25)$	$N(0.2, 0.25)$	1000	0.69	-0.04
$N(0.7, 0.25)$	$N(0.2, 0.25)$	2000	0.49	0.37
$N(0.7, 0.25)$	$N(0.2, 0.25)$	3000	0.35	0.71

Page, E. S. Continuous Inspection Schemes. Biometrika, 41, 100-114. 1954.

Shiryaev, A.N. Minimax optimality of CUSUM method in case of continuous time // Uspehi Math. Nauk. 1996. V.51. No.4. p. 173-174.

Lucas, J.M., Crosier, R.B. Fast Initial Response for CUSUM Quality Control Schemes: Give Your CUSUM a Head Start. Technometrics, 199-205. 1982.

Gan, F.F. Exact Run Length Distributions for One-Sided Exponential CUSUM Schemes. Vol. 2, no. 1, 297-312. 1992.

Busaba, J., Sukparungsee, S., Areepong, Y. and Mititelu, G. Analysis of Average Run Length for CUSUM Procedure with Negative Exponential Data. Chiang Mai J. Sci. 2012; 39(2), 200-208.

Vardeman, S., Ray, D. Average Run Lengths for CUSUM Schemes When Observations Are Exponentially Distributed. Technometrics, 3 Vol. 27, No.2, 145-150. 1985.

Mazalov V.V., Zhuravlev D.N. On a CUSUM method in detecting of changing of traffic // Programming and Computer Software, Iss. 6. 2002. P. 156-162.