Quickest Change Detection in the Presence of Transient Adversarial Attacks

Thirupathaiah Vasantam  
Dept. of CICS  
University of Massachusetts  
Amherst, USA  
tvasantam@umass.edu

Don Towsley  
Dept. of CICS  
University of Massachusetts  
Amherst, USA  
towsley@cs.umass.edu

Venugopal V. Veeravalli  
Dept. of ECE  
University of Illinois  
Urbana-Champaign, USA  
vvv@illinois.edu

Abstract—We study a monitoring system in which the distributions of sensors’ observations change from a nominal distribution to an abnormal distribution in response to an adversary’s presence. The system uses the quickest change detection procedure, the Shewhart rule, to detect the adversary that uses its resources to affect the abnormal distribution, so as to hide its presence. The metric of interest is the probability of missed detection within a predefined number of time-slots after the changepoint. Assuming that the adversary’s resource constraints are known to the detector, we find the number of required sensors to make the worst-case probability of missed detection less than an acceptable level. The distributions of observations are assumed to be Gaussian, and the presence of the adversary affects their mean. We also provide simulation results to support our analysis.

Index Terms—Quick change detection, Transient change detection, Shewhart test, CUSUM test.

I. INTRODUCTION

The problem of quick detection of changes in statistical properties of a random process appears in many applications, ranging from fault detection, radar signal processing, industrial quality control, and navigational systems [1]–[4]. The existing works on this detection problem have focused on two types of models. The first is the quick change detection (QCD) problem, which deals with the case where the distribution changes from a nominal distribution to another distribution. The second is the transient change detection (TCD) problem, where the distribution changes from the nominal distribution to an abnormal distribution for a finite duration, and then it reverts back to the original nominal distribution. The problem of interest in this paper is a hybrid of the QCD and TCD problems. As in the QCD problem, the distribution of the observations changes persistently to a different distribution in response to an adversary; however, for a certain number of time-slots after the changepoint, the adversary controls the abnormal distribution by investing resources with the goal of hindering the change detection. Once the adversary’s resources expire, the distribution of the observations returns to the persistent abnormal distribution.

The main objective in the QCD problem is to minimize average detection delay, subject to certain false-alarm constraints. In the Bayesian framework, under the assumption that the changepoint is a random variable with a known distribution (typically geometric), the optimization problem is to minimize the average detection delay with an upper bound constraint on the probability of false-alarm [5]. When the changepoint is deterministic but unknown, the detection problem is studied using a minimax framework, where the objective is to minimize the worst-case average detection delay, subject to a lower bound constraint on the mean time to false-alarm [6], [7]. The Cumulative Sum (CUSUM) test introduced by Page [8], was shown to achieve optimal performance in [9].

For many applications such as monitoring in global navigation satellite systems (GNSSs) [10], monitoring in water distribution systems [8], monitoring in industrial processes [11], it is of interest to detect abnormalities in a monitoring process with a certain tolerable detection delay, say K time-slots after the changepoint, and if the detector announces a change in the distribution after K time-slots then it is considered to be a missed detection. Hence the goal here is to minimize the probability of missed detection (PMD) in K time-slots after the changepoint. Such a metric is commonly used in TCD problems, with K corresponding to the duration of the transient.

In [12], it was shown that the Shewhart test [13] minimizes the PMD when K = 1. The performance of CUSUM based algorithms for finite observation intervals was studied in [14], [15]. The performance of a window length-based CUSUM test was investigated in [3], [16], where they obtained some upper bounds on the PMD and proposed a numerical method to compute the PMD. Recently, some performance bounds for the finite moving average method were obtained in [2].

We assume that the detector uses M active sensors for detection, and that the adversary uses its resources to attack all of the active sensors. We find the least number of sensors that the detector must use to make the worst-case PMD in K time-slots after the changepoint less than some acceptable level.

The rest of the paper is organized as follows. In Section II we introduce the model. In Section III we define the stopping rule and provide some preliminary results. In Section IV we give the main results on the worst-case PMD achievable by the adversary. In Section V we provide some numerical results to validate our analysis, and in Section VI we give some

This work was supported in part by the Army Research Laboratory under Cooperative Agreement W911NF-17-2-0196 (IoBT CRA).
considering remarks.

II. PROBLEM MODEL

Consider a system with $M$ sensors that take observations to detect an adversary’s presence in the system. Let $X_n = (X_n^{(1)}, \ldots, X_n^{(M)})$ where $X_n^{(i)}$ is the observation of sensor $i$ at time-slot $n$. The elements of the sequence $\{X_n\}_{n \geq 1}$ are assumed to be independent random variables. Furthermore, $\{X_n^{(i)}\}_{1 \leq i \leq M}$ are assumed to be independent and identically distributed random variables for each $n$. We assume that the observations are real-valued and continuous, and have probability density functions (pdfs). The pdf of $X_n^{(i)}$ is denoted by $p_{X,n}$. The nominal pdf of the system is denoted by $f_0$. In previous works, the distribution is assumed to change from a distribution with pdf $f_0$ to another distribution with pdf $f_1$ at a deterministic but unknown time instant referred to as the changepoint, denoted by $\nu$. In this paper, we assume that an adversary changes the pdf $p_{X,n}$ from $f_0$ to $\psi_{\nu(\theta)}$, where the parameter $\theta$ is chosen by the adversary and the function $\gamma(\theta)$ is defined as

$$\gamma(\theta) = \frac{\theta}{M}. \tag{1}$$

We make an assumption that the KL divergence decreases monotonically in $\theta$ and $\lim_{\theta \to \infty} D(\psi_{\nu(\theta)}, f_0) = 0$, indicating that $\psi_{\nu(\theta)}$ is nearly the same as $f_0$ when $\theta$ is large. If the adversary does not put any effort to hide its presence, then $\theta = 0$. Also, we assume that $\psi_{\nu(\infty)} = f_0$ and $\psi_{\nu(\theta)} = f_1$. Furthermore, the adversary is assumed to have a finite amount of resources to change the post-change distribution’s pdf from $f_1$ to $\psi_{\nu(\theta)}$, $\theta > 0$, for a duration of $L_\theta$ time-slots after the changepoint. Precisely, we consider the following framework: at time-slot $n$ the pdf $p_{X,n}$ is equal to $\psi_{\nu(\theta)}$ where the function $\gamma(\theta)$ satisfies

$$\gamma(\theta) = \begin{cases} \infty, & \text{for } 1 \leq n \leq \nu \\ \frac{\theta}{M}, & \text{for } \nu + 1 \leq n \leq \nu + L_\theta \\ 0, & \text{for } n \geq \nu + L_\theta + 1, \end{cases} \tag{3}$$

satisfying $\theta \in \mathbb{R}_+$ and $L_\theta \in \mathbb{Z}_+$ is a decreasing function of $\theta$. Let $A$ be the total amount of resources of the adversary and $\theta$ the amount of invested resources in each time-slot, then $L_\theta$ is the largest integer satisfying $L_\theta \leq \frac{A}{\theta}$. Let $Q_\delta(K, M, A)$ be the PMD in $K$ time-slots after the changepoint, where $K$ is a fixed parameter with $K \geq L_\theta$. An adversary’s objective is to maximize its impact on the system by maximizing $Q_\delta(K, M, A)$. Hence, the adversary’s objective is to find $\theta$ that maximizes $Q_\theta(K, M, A)$. We assume that the system operator uses a detector with the Shewhart stopping rule to detect changes in the distributions of the observations under the assumption that $f_0$ and $f_1$ are pre-change and post-change pdfs, respectively. The detector is unaware of the adversary’s actions during the transient regime. However, under the assumption that the detector has information about the adversary’s resources, we first compute $\theta$ that results in the worst-case PMD. We then find the number of sensors to be used by the detector to make the worst-case PMD less than a predefined parameter $\delta$.

In this paper, we study the scenario where the distributions are Gaussian and focus on the mean-change problem. However, the analysis can be generalized to other settings. For a random variable $Z_n$, we write the conditional probabilities and expectations as $\mathbb{P}_{\nu, \theta}(Z_n)$ and $\mathbb{E}_{\nu, \theta}[Z_n]$ when the changepoint is $\nu$ and each sensor’s observation has pdf $\psi_{\nu(\theta)}$ in time-slot $n$. Also, $\mathbb{P}_\infty(Z_n)$ and $\mathbb{E}_\infty[Z_n]$ are the conditional probabilities and expectations of $Z_n$ when the observations of sensors have nominal distributions in time-slot $n$.

III. STOPPING RULE

In this section, we first define the stopping rule, and then we derive an expression for $Q_\delta(K, M, A)$. Let $g_\theta$ be the joint pdf of $X_n$ when the adversary uses $\theta$ resources in each time-slot in the transient regime after the changepoint and $g_\infty$ be the joint pre-change pdf of $X_n$. Next, we define the stopping test. The detector is assumed to have information that the adversary has at most $A$ resources.

Definition 1: Shewhart test: For given false-alarm probability $\alpha$ the stopping time $T$ is defined as

$$T \triangleq \inf \{ n \geq 1 : w(X_n) \geq h' \}, \tag{4}$$

where $w(X_n) = \sup_{\theta \in [0, A]} \log \left( \frac{g_\theta(X_n)}{g_\infty(X_n)} \right)$ and $h'$ is selected such that $\mathbb{P}_\infty(w(X_n) \geq h') = \alpha$.

Now we use the assumption that the distributions of observations are Gaussian. Let $\phi_z$ be the pdf of the Gaussian distribution $\mathcal{N}(\mu_z, 1)$, where $z$ is a parameter that defines the mean $\mu_z$. The function $\phi_z$ decreases monotonically in $z$ satisfying $\lim_{z \to \infty} \mu_z = 0$. Since the observations’ distributions are Gaussian

$$\phi_{\nu(\theta)}(\psi_{\nu(\theta)}), \tag{5}$$

for $\theta \in \mathbb{R}_+$. The nominal and the persistent abnormal pdfs are assumed be $f_0 = \phi_\infty$ and $f_1 = \phi_0$, respectively.

For the mean-change problem, it can be verified that the likelihood ratio $\log \left( \frac{g_\theta(X_n)}{g_\infty(X_n)} \right)$ is a monotonically increasing function in $Y_n$ defined by

$$Y_n = \sum_{i=1}^{M} X_n^{(i)}. \tag{6}$$

Hence the Shewhart stopping time $T$ simplifies to the following form:

$$T \triangleq \inf \{ n \geq 1 : Y_n \geq h \}, \tag{7}$$

where $h$ is selected such that

$$\mathbb{P}_\infty(Y_n \geq h) = \alpha. \tag{8}$$
Let $q_0$ be the PMD in a time-slot given by

$$q_0 = \mathbb{P}_{\nu, \theta}(Y_m < h).$$

Then it can be shown that

$$q_0 = \Phi_{\infty}^{-1}(1 - \alpha) - \sqrt{M} \mu_{\infty}(0),$$

where, $\Phi_{\infty}(\cdot)$ is the cumulative distribution function (CDF) of $\mathcal{N}(0, 1)$ and $\Phi_{\infty}^{-1}(\cdot)$ is the inverse function of $\Phi_{\infty}(\cdot)$.

We give an expression for $Q_0(K, M, A)$ in the following Lemma and skip the proof as it follows immediately.

**Lemma 1:** For given $\alpha$ with $\mu_0 > 0$ and $\mu_0 > 0$, we obtain

$$Q_0(K, M, A) = q_0^L \times q_0^{K-L_0}.$$  

(11)

Note that the PMD $Q_0(K, M, A)$ decreases monotonically with the number of sensors $M$.

**Remark 1:** Since $\mu_0$ decreases monotonically in $\theta$, we have that

$$q_0 > q_0.$$  

(12)

The above inequality reflects that the probability of missed detection in a single time-slot increases with the amount of invested resources of the adversary.

Note that although $q_0$ increases with $\theta$, the length of the transient duration $L_0$ decreases with $\theta$. Hence, the adversary chooses $\theta$ so as to maximize $Q_0(K, M, A)$.

Next, we show that if the adversary decides to invest $\theta$ resources in a time-slot, then it must invest $\frac{\theta}{M}$ resources on each sensor to maximize the probability of missed detection. Assuming that the detector uses the stopping test $T$ defined in (7), suppose $q_{0}^{(1)}$ is the probability of missed detection per time-slot when the adversary spends $\theta_{i}$ resources on Sensor $i$ ($1 \leq i \leq M$) such that $\sum_{i=1}^{M} \theta_{i} = \theta$. Similarly, suppose $q_{0}^{(2)}$ is the probability of missed detection per time-slot when the adversary spends $\frac{\theta}{M}$ resources on each sensor.

**Lemma 2:** We show that

$$q_{0}^{(2)} \geq q_{0}^{(1)}.$$  

(13)

**Proof** It can be shown that

$$q_{0}^{(1)} = \Phi_{\infty} \left( \Phi_{\infty}^{-1}(1 - \alpha) - \frac{M}{\sqrt{M}} \sum_{i=1}^{M} \mu_{\theta_{i}} \right)$$

and

$$q_{0}^{(2)} = \Phi_{\infty} \left( \Phi_{\infty}^{-1}(1 - \alpha) - \sqrt{M} \mu_{\frac{\theta}{M}} \right).$$  

(14)

(15)

To prove the result, we need to show that

$$\sqrt{M} \mu_{\frac{\theta}{M}} \leq \frac{1}{\sqrt{M}} \sum_{i=1}^{M} \mu_{\theta_{i}}.$$  

(16)

That is, we need to show

$$\mu_{\frac{\theta}{M}} \leq \frac{1}{M} \sum_{i=1}^{M} \mu_{\theta_{i}}.$$  

(17)

Since $\mu_{\theta}$ is strictly convex in $\theta$, from Jensen’s inequality [1], we obtain

$$\frac{1}{M} \sum_{i=1}^{M} \mu_{\theta_{i}} \geq \mu_{\frac{1}{M} \sum_{i=1}^{M} \theta_{i}} = \mu_{\frac{\theta}{M}}.$$  

(18)

This completes the proof.

**IV. MAIN RESULTS**

In this section, we show that there exists a unique $\theta$ that maximizes $Q_0(K, M, A)$ under certain sufficient conditions for given $K$ and $A$. In our analysis, we study various types of functions for $L_0$. Although $L_0$ is an integer value, we allow a real valued $L_0$ to simplify our analysis.

Next, we define some useful notation. Define $r_0$ as

$$r_0 = \log(Q_0(K, M, A)).$$  

(19)

Then we have

$$r_0 = L_0 \log(q_0) + (K-L_0) \log(q_0)$$

$$= L_0 \log \left( \frac{q_0}{q_0} \right) + K \log(q_0).$$  

(20)

The optimal $\theta$ that maximizes $Q_0(K, M, A)$ is a solution of the following equation

$$\frac{dr_0}{d\theta} = \frac{dL_0}{d\theta} \log \left( \frac{q_0}{q_0} \right) + \frac{L_0 dq_0}{q_0} \frac{d\theta}{d\theta} = 0.$$  

(21)

Next, we establish the following preliminary result.

**Lemma 3:** Let $\phi_{\infty}(\cdot)$ and $\Phi_{\infty}(\cdot)$ be the pdf and CDF of a $\mathcal{N}(0, 1)$ random variable. Then, for $x \in \mathbb{R}$

$$\frac{\phi_{\infty}(x)}{\Phi_{\infty}(x)} + x > 0.$$  

(22)

**Proof** For $x \in \mathbb{R}^+$, clearly, we have $\frac{\phi_{\infty}(x)}{\Phi_{\infty}(x)} + x > 0$. We next show that even for $x < 0$, the result $\frac{\phi_{\infty}(x)}{\Phi_{\infty}(x)} + x > 0$ holds. For $y > 0$, if $X$ is an $\mathcal{N}(0, 1)$ random variable, then we can write

$$\mathbb{E}(X|X > y) = \frac{1}{1-\Phi_{\infty}(y)} \int_{z=y}^\infty \phi_{\infty}(z) dz$$

$$= \frac{\phi_{\infty}(y)}{1-\Phi_{\infty}(y)}.$$  

(23)

(24)

Since $\phi_{\infty}(y) = \phi_{\infty}(-y)$ and $\Phi_{\infty}(y) + \Phi_{\infty}(-y) = 1$, we get

$$\mathbb{E}(X|X > y) = \frac{\phi_{\infty}(-y)}{\Phi_{\infty}(-y)}.$$  

(25)

Due to the fact that $\mathbb{E}(X|X > y) > y$, we obtain

$$\frac{\phi_{\infty}(-y)}{\Phi_{\infty}(-y)} > y.$$  

(26)

Hence, $\frac{\phi_{\infty}(-y)}{\Phi_{\infty}(-y)} + (-y) > 0$ for $y > 0$. 

**Theorem 1:** If $\mu_{\theta}$ is strictly convex and $L_0$ is strictly concave, then there exists a unique critical point for $r_0$ denoted by $\theta^*$. Furthermore, $r_0$ increases with $\theta$ up to $\theta^*$ and then it decreases with $\theta$. The critical point $\theta^*$ is found by solving (21).
Proof From (24), it can be shown that

$$\frac{d^2 r_0}{d \theta^2} = \frac{d^2 L_\theta}{d \theta^2} \log \left( \frac{q_0}{q_0} \right) + 2 \frac{d L_\theta}{d \theta} \frac{1}{q_0} \frac{dq_0}{d \theta} + \frac{L_\theta}{q_0} \frac{d^2 q_0}{d \theta^2}$$

Also, we can show that

$$\frac{dq_0}{d \theta} = \frac{1}{\sqrt{M}} \phi_\infty(x^* - \sqrt{M} \mu_\gamma(\theta)) \left( -\frac{d \mu_\gamma(\theta)}{d \theta} \right)$$

and

$$\frac{d^2 q_0}{d \theta^2} = \left( x^* - \sqrt{M} \mu_\gamma(\theta) \right) \frac{1}{M} \phi_\infty(x^* - \sqrt{M} \mu_\gamma(\theta)) \left( -\frac{d \mu_\gamma(\theta)}{d \theta} \right)$$

By using (28), (29), and (30), we obtain

$$\frac{d^2 r_0}{d \theta^2} = \frac{d^2 L_\theta}{d \theta^2} \log \left( \frac{q_0}{q_0} \right) + 2 \frac{d L_\theta}{d \theta} \frac{1}{q_0} \frac{1}{\sqrt{M}} \phi_\infty(x^* - \sqrt{M} \mu_\gamma(\theta)) \left( -\frac{d \mu_\gamma(\theta)}{d \theta} \right)$$

Now, if we simplify the third term of the right side of (32) and then it decreases with \( \theta \). Furthermore, \( r_0 \) increases with \( \theta \) up to \( \theta^* \) and then it decreases with \( \theta \). The critical point \( \theta^* \) satisfies

$$\theta^* = -\frac{\sqrt{M} q_\theta \log \left( \frac{q_{q_0}}{q_0} \right)}{\phi_\infty(x^* - \sqrt{M} \mu_\gamma(\theta^*)) \frac{d \mu_\gamma(\theta^*)}{d \theta}}.$$
Let $b_0$ be defined as

$$b_0 = - \log \left( \frac{q_0}{q_0} \right) + \frac{1}{q_0} \left( \frac{dq_0}{d\theta} \right).$$  \hfill (41)

Then every critical point satisfies $b_0 = 0$. We will show that $\frac{db_0}{d\theta} < 0$ which implies that there exists a unique solution to $b_0 = 0$. It can be verified that

$$\frac{db_0}{d\theta} = - \frac{1}{q_0} \frac{dq_0}{d\theta} \left( - \frac{d\gamma(\theta)}{d\theta} \right)$$

from (28) and (29). We can write

$$\frac{db_0}{d\theta} = - \frac{1}{q_0} \frac{1}{\sqrt{M}} \phi_{\infty}(x^* - \sqrt{M}\mu(\theta)) \left( - \frac{d\gamma(\theta)}{d\theta} \right)$$

$$- \frac{1}{q_0} \left( \frac{1}{\sqrt{M}} \phi_{\infty}(x^* - \sqrt{M}\mu(\theta)) \left( - \frac{d\gamma(\theta)}{d\theta} \right) \right)^2$$

$$\times \left( \frac{1}{q_0} \frac{1}{\sqrt{M}} \phi_{\infty}(x^* - \sqrt{M}\mu(\theta)) \right) + \frac{1}{q_0} \frac{1}{M} \phi_{\infty}(x^* - \sqrt{M}\mu(\theta)) \left( - \frac{d^2\gamma(\theta)}{d\theta^2} \right).$$ \hfill (43)
that the detector uses the Shewhart stopping test, we showed the existence of a unique optimal parameter for the adversary to maximize the PMD. We then find sufficient number of sensors to be used such that the worst-case PMD is less than an acceptable level. In future work, it is of interest to extend the analysis to the setting where the detector can use different types of sensors and has budget constraints on resources that it can spend on sensors.

REFERENCES

[1] H. Vincent Poor and Olympia Hadjiliadis, *Quickest detection*, vol. 9780521621045, Cambridge University Press, Jan. 2008.

[2] D. Egea-Roca, J. A. López-Salcedo, G. Seco-Granados, and H. Vincent Poor, “Performance bounds for finite moving average tests in transient change detection,” *IEEE Transactions on Signal Processing*, vol. 66, no. 6, pp. 1594–1606, 2018.

[3] Blaise Kévin Guépié, Lionel Fillatre, and Igor Nikiforov, “Sequential detection of transient changes,” *Sequential Analysis*, vol. 31, no. 4, pp. 528–547, 2012.

[4] B. Bakhache and I. Nikiforov, “Reliable detection of faults in measurement systems,” *International Journal of Adaptive Control and Signal Processing*, vol. 14, no. 7, pp. 526–547, 2000.

[5] A. G. Tartakovsky and V. V. Veeravalli, “General asymptotic bayesian theory of quickest change detection,” *Theory of Probability and Its Applications*, vol. 49, no. 3, pp. 458–497, Oct. 2005.

[6] G. Lorden, “Procedures for reacting to a change in distribution,” *The Annals of Mathematical Statistics*, vol. 42, no. 6, pp. 1897–1908, 1971.

[7] Moshe Pollak, “Optimal detection of a change in distribution,” *Ann. Statist.*, vol. 13, no. 1, pp. 206–227, 03 1985.

[8] E. S. Page, “Continuous inspection schemes,” *Biometrika*, vol. 41, no. 1/2, pp. 100–115, 1954.

[9] George V. Moustakides, “Optimal stopping times for detecting changes in distributions,” *Ann. Statist.*, vol. 14, no. 4, pp. 1379–1387, 12 1986.

[10] R. Toledo-Moreo, B. Úbeda, J. Santa, M. A. Zamora-Izquierdo, and A. F. Gómez-Skarmeta, “An analysis of positioning and map-matching issues for gns-based road user charging,” in *13th International IEEE Conference on Intelligent Transportation Systems*, 2010, pp. 1486–1491.

[11] Anastasios Pouliezos and George S. Stavrakakis, *Real Time Fault Monitoring of Industrial Processors*, vol. 12, Springer Netherlands, 1994.

[12] George V. Moustakides, “Multiple optimality properties of the shewhart test,” *Sequential Analysis*, vol. 33, no. 3, pp. 318–344, 2014.

[13] W. A. Shewhart, “Economic quality control of manufactured product,” *Bell System Technical Journal*, vol. 9, no. 2, pp. 364–389, 1930.

[14] Z. J. Wang and P. Willett, “A variable threshold page procedure for detection of transient signals,” *IEEE Transactions on Signal Processing*, vol. 53, pp. 4397–4402, 2005.

[15] Zhen Wang and P. Willett, “A performance study of some transient detectors,” *IEEE Transactions on Signal Processing*, vol. 48, no. 9, pp. 2682–2685, 2000.

[16] Lionel Fillatre, Igor V. Nikiforov, and Van Long Do, “Sequential detection of transient changes in stochastic-dynamical systems,” *Journal de la Societe Francaise de Statistique*, vol. 156, no. 4, pp. 60–97, 2015.