# On Byzantine Distributed Sequential Change Detection with Multiple Hypotheses

Yu-Jui Huang
Dept. of Applied Math., Univ. of Colorado
Boulder, CO 80309, USA
yujui.huang@colorado.edu

Shih-Chun Lin
Dept. of ECE, NTUST
Taiwan
sclin@ntust.edu.tw

Yu-Chih Huang
Dept. of Commun. Eng., NTPU
Taiwan
ychuang@mail.ntpu.edu.tw

***Abstract*—Sequential change point detection with multiple decentralized sensors is studied. Each sensor makes a local decision based on its own observations and reports it through a bandlimited link to a fusion center, which then decides whether the change has occurred. Since sensors in many applications such as cyber-physical systems are prone to a number of attacks such as Byzantine attacks, combating such a security breach becomes one of the most crucial issues. Previous works on sequential change detection under Byzantine attacks only focus on binary-hypothesis case, which significantly limits the applicability. In this paper, we consider the extension to the multi-hypothesis setting. We show that naively extending the existing method from the binary case to the multi-hypothesis one can result in a catastrophic event preventing the fusion center from making a conclusive decision. Thus we propose the other two new methods by allowing each sensor to cast multiple local alarms, and both can avoid this catastrophic event and improve the asymptotic detection delay. In analyzing detection delays of our multi-hypothesis schemes, we also show that for each hypothesis, asymptotically, it suffices to focus on the competing hypothesis that is closest in Kullback-Leibler distance. Through large sensor analysis, we also show that as the number of honest sensors grows, one of the proposed scheme, called the simultaneous rule, approaches the optimal performance within a factor of 2.**

## I. Introduction

Cyber-physical systems (CPS), which integrate techniques like communication and computation, are expected to provide high stability and robustness to the next generation of systems [1]. For example, the abnormal changes of voltage waveforms in smart grids are harmful to delicate electronic devices and recent advances of massive machine-type communications (mMTC) or internet of things (IoT) [2] allow the usage of advanced cyber-physical infrastructures for monitoring voltage quality events [3].

In status monitoring of CPS and many other examples, to quickly alarm the occurrence of an abnormal event is crucial. Moreover, sensors, cheap and distributed across a field, are prone to be compromised [4] and such security breaches can result in catastrophic consequences [1], [4]. Hence, the approach in [4], [5] that studies sequential change detection with decentralized sensors in the presence of compromised sensors forming a Byzantine attack is promising. While [4], [5] consider the binary case, i.e. the abnormal event can have only one state, in CPS such as smart grids, an abnormal event typically has multiple states [3] and thus the aforementioned techniques are inadequate.

In this paper, we tackle the problem of multi-hypothesis distributed sequential change detection under Byzantine attacks. We first adapt the binary one-shot rule in [5] to a simple multi-hypothesis decision rule by replacing the cumulative sums (CUSUM) local decision algorithm adopted in the binary case with the matrix CUSUM in [6]. The fusion center then declares the abnormal hypothesis that receives enough local alarms. However, with multiple abnormal hypotheses, the fusion center may never be able to make a conclusive decision; since it is possible that none of the hypotheses has enough local alarms after all sensors report. Moreover, even in the absence of the undecidable event, several bad observations could lead to false isolation at some nodes, which could in turn significantly increase the delay or trigger false isolation as each node only gets to report once. Motivated by the disadvantages of the one-shot scheme, we propose two new families of decision rules, namely the multi-shot rule and the simultaneous rule. Both families of decision rules adopt a "soft" version of matrix CUSUM at sensors and allow each sensor to cast multiple local alarms over time.

We perform the worst-case analysis in terms of the mean time to false isolation/false alarm and detection delay for the proposed fault-tolerant decision rules. The results show that both the multi-shot and simultaneous rules outperform the one-shot rule and effectively eliminate the possibility of the undecidable event. Among the three schemes, the simultaneous rule achieves the best performance but is the least energy-efficient. In the course of detection delay analysis, we establish a lemma (Lemma 1) indicating that even though there are multiple possible hypotheses, for each hypothesis, each sensor only has to worry about the competing hypothesis that is "closest" in Kullback-Leibler (KL) distance [7]. This result may be useful for further study of multi-hypothesis multi-channel change detection problem. Large sensor analysis, which is typically important for IoT applications, is also carried out.The results not only offer guidance about how to choose optimal parameters for our proposed rules, but also indicate that the proposed simultaneous rule can approach the optimal delay performance within a factor of 2.

For a positive integer $K$, define $[K] := \{1, \dots, K\}$ and $[K]^+ = \{0\} \cup [K]$. Function $(x)^+$ outputs $x$ if $x \geq 0$ and zero otherwise. For two real functions $f_1(x)$ and $f_2(x)$, as $x \to \infty$, we write $f_1(x) \sim f_2(x)$ when $f_1(x)/f_2(x) \to 1$ and $f_1(x) \gtrsim f_2(x)$ when $\liminf(f_1(x)/f_2(x)) \geq 1$. The $o(.)$ and $w(.)$ follow the asymptotic notations in [8].

## II. Problem Formulation

Consider a network with a fusion center and $K$ distributed sensors, indexed by $[K]$, respectively. The fusion center tries to monitor an abrupt event and decide whether the event has occurred and which type it is. The observations of all $K$ sensors are sequences of independent random variables with known distributions, subject to the same distribution change at a unknown but deterministic time $\nu$. After this distribution change, there are $Q$ different possible types. Specifically, let $P_0$ be the pre-change probability density function (PDF) and $P_1, \ldots, P_Q$ the post-change PDF corresponding to the states $1, \ldots, Q$, respectively. For each $k \in [K]$, we denote by $X_t^k$ the observation made by sensor $k$ at time $t$. We can now define $Q+1$ different hypotheses as follows. Under the hypothesis $H_q$, $q \in [Q]$, the random variables $X_1^k, X_2^k, \ldots, X_{\nu-1}^k$ are independent and identically distributed (i.i.d.) with the PDF $P_0$, while $X_\nu^k, X_{\nu+1}^k, \ldots$ are i.i.d. with the PDF $P_q$. Under the hypothesis $H_0$, $X_t^k$ are i.i.d. with the PDF $P_0$ for all $t$. We write $\mathbf{X}_t = [X_t^1, \ldots, X_t^K]$ for each $t$ and denote by $\mathbf{X}_{t_1}^{t_2}$ the collection of $\mathbf{X}_{t_1}, \mathbf{X}_{t_1+1}, \ldots, \mathbf{X}_{t_2}$ for each $t_1, t_2$ with $t_2 > t_1$.

Among the sensors, there is an unknown subset $\mathcal{N} \subset [K]$ of honest sensors, with the remaining $M := K - |\mathcal{N}|$ sensors being compromised by the attacker. We assume that $M$ the exact number (or a maximum) of compromised sensors is known, and it is less than the number of honest sensors, i.e., $|\mathcal{N}| \geq M$. As [5], there is an noiseless link of a finite number of bits associated with each sensor to the fusion center. Two types of bandwidth constraints are considered; namely each link has $\lceil \log_2(Q) \rceil$ bits and that has $Q$ bits. At each time index $t$, a honest sensor $k$ makes a local decision individually by mapping its own observations up to time $t$ to an element in $\mathcal{X}$ satisfying the bandwidth constraint. Depending on the adopted reporting mechanism that will be discussed later and the bandwidth constrain, each sensor decides whether it should alarm the fusion center through the channel it is associated with. The $M$ compromised sensors, on the other hand, try to disrupt/confuse the final decision of fusion center by sending attack signals which again belong to $\mathcal{X}$.

Let $T^{\hat{q}}$ be the stopping time where $\hat{q} \in [Q]$ is the decision. We allow $T^{\hat{q}} = \infty$, corresponding to the case when the fusion center *cannot* make a conclusive decision. We sometimes suppress the superscript $\hat{q}$ and simply write $T$ when only the stopping time matters. Let $g$ be an attack strategy of the $M$ compromised sensors. We assume that the attacker knows $\nu$, $\mathbf{X}_1^t$, and the decision rule employed by the fusion center, and hence $g$ is a function of these arguments. We also write $g = \emptyset$ when all the compromised sensors are absent. When a change under hypothesis $H_q$, $q \in [Q]$, happens at time $\nu$ and the strategy employed by the $M$ compromised sensors is $g$, the underlying probability measure is denoted by $\mathsf{P}_\nu^{q,g}$. Moreover, when no change ever happens, i.e., $\nu = \infty$, we denote by $\mathsf{P}_\infty^{q=0,g}$ the underlying probability measure. Following the single-sensor case in [6], [9], we consider the performance metrics as follows:

- **Detection Delay:** The mean detection delay is given by

$$\mathcal{D}[T] := \sup_{q \in [Q]} \sup_{g,\nu} \operatorname{ess\,sup} \mathbb{E}_\nu^{q,g}[T - \nu | T > \nu, \mathbf{X}_1^\nu]. \quad (1)$$

- **False Alarm:** Without any abnormal changes, the mean time to false alarm is given by

$$\mathcal{A}[T] := \inf_g \mathbb{E}_\infty^{q=0,g}[T]. \quad (2)$$

- **False Isolation:** The mean time to false isolation is given by

$$\mathcal{I}[T] := \inf_{q \in [Q]} \inf_g \inf_{\hat{q} \in [Q] \setminus \{q\}} \mathbb{E}_0^{q,g}[T^{\hat{q}}]. \quad (3)$$

Our objective is to design fault-tolerant decision rules such that $\mathcal{D}[T]$ can be minimized, with large $\mathcal{I}[T]$ and $\mathcal{A}[T]$.

## III. Proposed Fault-tolerant Decision Rules

In this section, we first describe the local decision rule at each honest sensor, and then propose three global fault-tolerant decision rules adopted at the fusion center.

### A. Local decision rule: "Soft" Matrix CUSUM

Since the honest sensors are not allowed to cooperate with each other, it is natural to adopt the matrix CUSUM algorithm in [6] as each sensor's local decision rule, which is known to be asymptotically optimal for the single-sensor multi-hypothesis setting. The original matrix CUSUM in [6] is reviewed as follows. At the sensor $k \in \mathcal{N}$, for each hypothesis $q \in [Q]$, we compute the CUSUM statistics $Y_t^k(q,j)$ for every $j \neq q \in [Q]^+$ at time $t$ recursively through $Y_0^k(q,j) = 0$ and $Y_t^k(q,j) = \left(Y_{t-1}^k(q,j) + \ell_t^k(q,j)\right)^+$, where $\ell_t^k(q,j) = \log \frac{P_q(X_t^k)}{P_j(X_t^k)}$ is the log-likelihood ratio (LLR) between $P_q$ and $P_j$. The results are put into a $Q \times Q$ matrix $\mathbf{Y}_t$ with the $q$th row given by

$$\mathbf{Y}_t^k := [Y_t^k(q,0), \cdots, Y_t^k(q,j), \cdots, Y_t^k(q,Q)]. \quad (4)$$

Let $Y_{t,q}^k = \min_{j \in [Q]^+,\, j \neq q} Y_t^k(q,j)$ be the minimum of the $q$th row. The matrix CUSUM procedure proposed in [6] locally determines that the event has occurred at the first time that any $Y_{t,q'}^k, q' \in [Q]$ exceeds a pre-defined threshold $h$.

In [6], since there is only one node, it makes perfect sense for the procedure to terminate after the alarm; however, in our setting, the task is not done yet until the fusion center has determined the occurrence of the event. Therefore, we adapt the matrix CUSUM procedure to the "soft" version as follows. Whenever a $Y_{t,q'}^k$ exceeds the threshold $h$ at time index $t$, the hypothesis $H_{q'}$ is *softly* decided by informing the fusion center that this hypothesis is *acceptable* at the sensor $k$. Now each honest sensor may keep monitoring the event and report multiple hypotheses to the fusion center. Later in Sec. III-B, this soft version will help us resolve the "undecidable event", which disables the fusion center to make a conclusive decision.

Formally, for the soft matrix CUSUM procedure, a hypothesis $H_{q'}$ is acceptable by the node $k$ at time

$$\sigma_k^{q'}(h) := \inf \left\{ t \in \mathbb{N} : Y_{t,q'}^k \geq h \right\}. \quad (5)$$

In contrast, for the original matrix CUSUM [6], a hypothesis $H_q$ is hard decided at time

$$\tilde{\sigma}_k^q(h) := \begin{cases} \sigma_k^q(h), & \text{if } \sigma_k^q(h) = \sigma_k(h) := \min_{q' \in [Q]} \sigma_k^{q'}(h) \\ & \text{and } q = \arg\max_{q' \in [Q]} \left( Y_{t,q'}^k |_{t=\sigma_k(h)} \right), \\ \infty, & \text{else} \end{cases} \quad (6)$$

### B. Fault-tolerant decision rules

As a baseline, the one-shot rule which uses the original matrix CUSUM is first introduced. Then, the two proposed rules based on the "soft" matrix CUSUM are presented.

**1) One-shot $d$-th alarm** $\tilde{\tau}_{(d)}(h)$: This family of rules is a direct extension of the one-shot rule for the binary case in [5] to the multi-hypothesis setting. Each sensor adopts the original matrix CUSUM [6] as its local report mechanism and reports the first acceptable non-zero hypothesis as soon as the sensor finds it. Formally, for each $k \in \mathcal{N}$, sensor $k$ alarms $H_{q^*}$ at the time index $\tilde{\sigma}_k^{q^*}(h)$, where $\tilde{\sigma}_k^{q^*}(h)$ is the only finite time index among all $\tilde{\sigma}_k^q(h)$s, $q \in [Q]$ in (6). If a tie happens at a node $k$, then among those $q$ resulting in the same $\tilde{\sigma}_k^q(h)$, the one with the largest $Y_{t,q}^k$ is reported. For the case that two or more hypotheses observe same $Y_{t,q}^k$, we break the tie randomly. The fusion center declares that an abrupt event has occurred at the first time that a hypothesis, say $H_q$, has received $d$ local reports with $H_q$. It also declares that the hypothesis $H_q$ is true.

**2) Multi-shot $d$-th alram** $\tau_{(d)}(h)$: This family of rules requires each sensor to adopt the soft version of matrix CUSUM and to alarm whenever a hypothesis $H_q$, $q \in [Q]$, is acceptable. Formally, for each $k \in \mathcal{N}$, sensor $k$ reports $H_q$ at the time index $\sigma_k^q(h)$, for every $q \in [Q]$. In this reporting mechanism, we stipulate that for each sensor, every hypothesis can be reported at most once, and a reported hypothesis cannot be withdrawn. In other words, once reported by a sensor, a hypothesis will be promoted as a candidate by that sensor ever since. If a tie happens at a honest node $k$, then all the hypothesis indexes have the same $\sigma_k^q(h)$ will be reported one after another, starting from the one with the largest $Y_{t,q}^k$. For the case that two or more hypotheses observe same $Y_{t,q}^k$, we break the tie randomly. Consecutive ties and/or multi-way ties can be easily resolved by equipping each node with a queue of size $Q-1$ and clearing the queue on the first-come first-serve basis. The fusion center declares that an abrupt event has occurred at the first time that a hypothesis, say $H_q$, has been deemed acceptable by $d$ sensors. It also declares that the hypothesis $H_q$ is true.

**3) Simultaneous $d$-th alarm** $T_d(h)$: Each sensor constantly transmits $Q$ bits local decision at time index $t$ to indicate whether $H_q$ is acceptable, $\forall q \in [Q]$. The fusion center declares that an abrupt event of type $q$ has occurred at the first time that a hypothesis, say $H_q$, has been simultaneously accepted by more than $d$ sensors.

We note that all the decision rules $T$ mentioned above are non-decreasing functions in each of its argument (corresponding to the entries of $\mathbf{Y}_t$) and the worst CUSUM statistic that the pre-change observations can impose is $Y_t^k(q,j)=0$; hence, Lemma 3 in [5] can be applied to simplify the detection delay in (1) into

$$\mathcal{D}[T] = \sup_{q\in[Q]} \sup_{g} \mathbb{E}_0^{q,g}[T]. \tag{7}$$

Also, it is worth noting that the soft matrix CUSUM reduces to the original CUSUM adopted in [5] when $Q=1$, i.e. binary hypothesis. Thus, the proposed multi-shot and simultaneous $d$-th alarm include the one-shot and voting rules in [5] as special cases, respectively.

**Remark 1.** *We note that the three families of rules have different bandwidth and/or energy requirements. The one-shot scheme is the most bandwidth- and energy-efficient one as it requires each link to support $\lceil \log_2 Q \rceil$ bits and this link is used only once. The multi-shot scheme also requires links to support $\lceil \log_2 Q \rceil$ bits while each link might be used at most $Q$ times. As for the simultaneous rule, it requires each link to support $Q$ bits and each link is constantly used.*

## IV. Main Results

We now carry out the worst-case analysis on the performance of the multi-shot $d$-th alarm and simultaneous $d$-th alarm rules. For the one-shot $d$-th alarm, we point out two notable differences compared to the binary counterpart which not only makes the analysis more involved but also significantly degrade the performance. First, for $d > |\mathcal{N}|/Q$, the *undecidable event* may happen; namely, it is possible that there is no hypothesis index with enough local alarms for making final decision even though all the honest sensors have raised alarms; thereby, $\tilde{\tau}_{(d)}(h) = \infty$. Secondly, even in the absence of compromised sensors, since each sensor only gets to report at most once, the analysis becomes quite involved when a tie happens. Of course, one can expect that the probability of ties becomes negligible when $h$ is large enough; the precise analysis is required to make rigorous statement and is left for future work. The performance analysis of $\tilde{\tau}_{(d)}$ under the assumption that there is no tie is provided in [10]. Due to the space limitation, all the results are provided without proofs except for Lemma 1. Please refer to [10] for the proofs.

To facilitate the discussion, some definitions are provided first. Similar to [5], from (5), we define the ordered time indexes over $|\mathcal{N}|$ honest sensors as if there is no compromised sensor, for softly deciding hypothesis $H_q$ (cf. the $q$th row of CUSUM matrix (4)) as $\sigma_{(1)}^q(h) \le \ldots \le \sigma_{(|\mathcal{N}|)}^q(h),\ q \in [Q]$. We also let $S_\ell^q(h)$ be the first time that the hypothesis $H_q$ is simultaneously softly-decided by $\ell$ honest sensors as

$$\inf\big\{t \in \mathbb{N} : Y_{t,q}^k \ge h\ \forall k \in \mathcal{L}, \text{for some } \mathcal{L} \subset [\mathcal{N}], |\mathcal{L}| = \ell\big\} \tag{8}$$

Finally, we will use $\mathbb{E}_\nu^q$ to represent the expectation when the change with hypothesis index $q$ happens at time $\nu$ and the compromised sensors are absent.

To perform the worst-case analysis, we assume that all the compromised sensors know the actual $\nu$ and the actual hypothesis $q$. They can then collaboratively attack/confuse the fusion center. Thus, it is obvious that choosing any $d \le M$ is bad for false alarm and and false alarm in (2) and (3), respectively, while any $d > |\mathcal{N}|$ is bad for detection delay in (7). We therefore confine the choice of $d$ to some reasonable region and obtain the following result.

**Proposition 1.** *Fix $h > 0$. For any $Q$, and $d \in \{M+1, ..., |\mathcal{N}|\}$, for multi-shot $d$-th alarm, we have*

$$\mathcal{I}[\tau_{(d)}(h)] \ge \min_{q\in[Q]} \min_{\hat{q}\in[Q]\setminus\{q\}} \mathbb{E}_0^{q,\emptyset}[\sigma_{(d-M)}^{\hat{q}}(h)], \tag{9}$$

$$\mathcal{A}[\tau_{(d)}(h)] \ge \min_{q} \mathbb{E}_\infty^{q=0,\emptyset}[\sigma_{(d-M)}^{q}(h)], \tag{10}$$

$$\mathcal{D}[\tau_{(d)}(h)] \le \max_{q} \mathbb{E}_0^{q,\emptyset}[\sigma_{(d)}^{q}(h)] + Q - 1; \tag{11}$$

*while for simultaneous $d$-th alarm*

$$\mathcal{I}[T_d(h)] = \min_{q\in[Q]} \min_{\hat{q}\in[Q]\setminus\{q\}} \mathbb{E}_0^{q,\emptyset}[S_{d-M}^{\hat{q}}(h)]; \tag{12}$$

$$\mathcal{A}[T_d(h)] = \min_{q} \mathbb{E}_\infty^{q=0,\emptyset}[S_{d-M}^{q}(h)]; \tag{13}$$

$$\mathcal{D}[T_d(h)] \le \max_{q} \mathbb{E}_0^{q,\emptyset}[S_{d}^{q}(h)]. \tag{14}$$

Note that for the multi-shot $d$-th alarm rule, we only provide lower bounds on the mean time to false alarm/isolation because of ties. Also, for both families of rules, only upper bounds on the delay performance are provided because the definitions of detection delay in (1) and (7) do not require the alarmed hypothesis to be the true one, but our analysis in Proposition 1 does. Moreover, the $Q-1$ in (11) is longest extra delay caused by ties. Based on Proposition 1, in what follows, we provide explicit upper and lower bounds on the detection delay and the mean time to false isolation/alarm, respectively.

### A. False alarm/isolation analysis

The asymptotic performance of the mean time to false alarm/isolation of the proposed families of rules are given in the following. Please see [10] for the proofs.

**Theorem 1.** *Fix $h > 0$. If $M < d \le |\mathcal{N}|$, both the mean time to false isolation $\mathcal{I}[\tau_{(d)}(h)]$ in* (9) *and the mean time to false alarm $\mathcal{A}[\tau_{(d)}(h)]$ in* (10) *for the multi-shot $d$-th alarm are lower-bounded by*

$$\frac{d-M}{(d-M+1)} \left( \begin{array}{c} |\mathcal{N}| \\ d-M \end{array} \right)^{\frac{-1}{d-M}} \exp(h). \tag{15}$$

**Theorem 2.** *Fix $h > 0$. If $M < d \le |\mathcal{N}|$, both the mean time to false isolation $\mathcal{I}[T_{(d)}(h)]$ in* (12) *and the mean time to false alarm $\mathcal{A}[T_{(d)}(h)]$ in* (13) *are lower-bounded by*

$$\frac{1}{2} \left( \begin{array}{c} |\mathcal{N}| \\ d-M \end{array} \right)^{-1} \exp\left((d-M)h\right). \tag{16}$$

### B. Detection delay analysis

For analyzing the delay performance, it is intuitive that for each hypothesis $q \in [Q]$, although there are total $Q+1$ hypotheses, one only has to worry about the one that is "*closest*" to $q$. However, delay analysis is more involved and thus in the following we resort to the asymptotic analysis where $h \to \infty$. We make this observation precise in terms of the KL distance in Lemma 1 whose proof is presented in Appendix A. To this end, we define for each pair of $q, j \in [Q]^+$, $q \ne j$, the KL distance from $P_j$ to $P_q$ as $I(q,j) := \int \log\left(P_q(x)/P_j(x)\right) P_q(x) dx$. Let $\sigma^2(q,j)$ be the second moment of $I(q,j)$ as $\sigma^2(q,j) := \mathbb{E}_q\left[\left(\log\left(P_q(x)/P_j(x)\right) - I(q,j)\right)^2\right]$. Then we assume:

**Assumption 1.** *For any $q \in [Q]$,*

(i) *$0 < I(q,j) < \infty$ and $\sigma^2(q,j) < \infty$, $\forall j \in [Q]^+, j \ne q$.*
(ii) *Let $I^q := \min_{0\le j\le Q,\ j\ne q} I(q,j)$. Assume $I^q$ admits a unique minimizer $j^* \in [Q]\setminus\{q\}$.*

By writing $\mathbb{P}_q$ for $\mathsf{P}_0^{q,g=\emptyset}$, we have:

**Lemma 1.** *Suppose $h$ is large enough and Assumption 1 holds. For any $q \in [Q]$, it holds $\mathbb{P}_q$-a.s. that*
*(i) The first time $H_q$ is softly decided at the honest sensor $k$, $\sigma_k^q(h)$ in* (5)*, equals to*

$$\sigma_k^{q,j^*}(h) := \inf\{t \in \mathbb{N} : Y_t^k(q,j^*) \ge h\}. \tag{17}$$

*(ii) For any $|\mathcal{N}| \ge d \ge 1$, the first time $H_q$ is simultaneously softly-decided by $d$ honest sensors, $S_d^q(h)$, equals to*

$$S_d^{q,j^*}(h) := \inf\left\{t \in \mathbb{N} : Y_t^{(|\mathcal{N}|-d+1)}(q,j^*) \ge h\right\}, \tag{18}$$

*where the ordered CUSUM statistics $Y_t^k(q,j^*)$s for hypotheses $q$ and $j^*$, at time $t$, are $Y_t^{(1)}(q,j^*) \le \ldots \le Y_t^{|\mathcal{N}|}(q,j^*)$.*

We now present the results on the asymptotic delay performance. Let $Z_{(1)}$, $Z_{(2)}$, …, $Z_{(|\mathcal{N}|)}$ be the order statistics of standard independent normal random variables. For each $d \in \{1,2,\ldots,|\mathcal{N}|\}$, we denote by $\xi_d$ the expected value of $Z_{(d)}$. Moreover, for each $q \in [Q]$, we set $D_{d:|\mathcal{N}|}^q := \xi_d \sqrt{\frac{\sigma^2(q,j^*)}{I^q}}$.

**Theorem 3.** *Suppose Assumption 1 holds. As $h \to \infty$, for any $q \in [Q]$ and $1 \le d \le |\mathcal{N}|$, we have $\mathbb{E}_0^{q,\emptyset}[\sigma_{(d)}^q(h)] = \frac{h}{I^q} + D_{d:|\mathcal{N}|}^q \sqrt{h}(1+o(1))$, and the detection delay of the multi-shot $d$-th alarm in* (11) *is upper-bounded as*

$$\mathcal{D}[\tau_{(d)}(h)] \le \max_q \left( \frac{h}{I^q} + D_{d:|\mathcal{N}|}^q \sqrt{h}(1+o(1)) \right). \tag{19}$$

**Theorem 4.** *Suppose Assumption 1 holds. As $h \to \infty$, for any $q \in [Q]$ and $1 \le d \le |\mathcal{N}|$, we have $\mathbb{E}_0^{q,\emptyset}[S_d^q(h)] \le \frac{h}{I^q} + D_{d:|\mathcal{N}|}^q \sqrt{h}(1+o(1))$, and the detection delay of the simultaneous $d$-th alarm in* (14) *is upper-bounded as*

$$\mathcal{D}[T_d(h)] \le \max_q \left( \frac{h}{I^q} + D_{d:|\mathcal{N}|}^q \sqrt{h}(1+o(1)) \right). \tag{20}$$

Although the upper bounds in Theorems 3 and 4 are identical, we will show the superiority of the simultaneous rule in the next section when detection delay and mean time to false alarm/isolation are jointly considered.

**Remark 2.** *Another application of Lemma 1 is to simplify the computation at the honest sensors. Asymptotically, it suffices to compute one CUSUM statistics $Y_t^k(q,j^*)$ out of those in* (4)*. An numerical example to validate this observation is given in [10, Remark IV.1].*

## V. Discussions

We compare the performance of the two proposed rules with a large number of sensors under Assumption 1. Note that unlike the analysis in [5], the term $D_{d:|\mathcal{N}|}^q \sqrt{h}$ in (19) may not be neglected even when $h \to \infty$.

**Corollary 1.** *For the multi-shot $d$-th alarm $\tau_{(d)}(h)$ with $d > M$, one can ensure $\mathcal{I}[\tau_{(d)}(h)] \ge \gamma$ and $\mathcal{A}[\tau_{(d)}(h)] \ge \gamma$ by selecting*

$$h = \log\gamma + \frac{1}{d-M} \log \left( \begin{array}{c} |\mathcal{N}| \\ d-M \end{array} \right) + \log\left(\frac{d-M+1}{d-M}\right).$$

*Moreover, when $|\mathcal{N}| \to \infty$ and $\gamma = \omega(|\mathcal{N}|)$, the optimal $d$ minimizing $\mathcal{D}[\tau_{(d)}(h)]$ is $d^* = M+1$.*

**Corollary 2.** *For simultaneous $d$-th alarm $T_d(h)$ with $M < d \leq p|\mathcal{N}|$, $p \in (0,1]$, one can ensure $\mathcal{I}[T_d](h) \geq \gamma$ and $\mathcal{A}[T_d](h) \geq \gamma$ by selecting*

$$h = \frac{1}{d-M}\left(\log\gamma + \log\left(2\binom{|\mathcal{N}|}{d-M}\right)\right). \tag{21}$$

*Moreover, when $|\mathcal{N}| \to \infty$ and $\sqrt{\log\gamma} \sim |\mathcal{N}|$, $\mathcal{D}[T_{\tilde{d}}(h)] \sim 2|\mathcal{N}|/I^*$, where $\tilde{d} = M + \lceil \frac{1}{2}|\mathcal{N}| \rceil$.*

One can rigorously show when $M \leq |\mathcal{N}|/2-1$ and $|\mathcal{N}| \to \infty$, the corresponding detection delay upper-bound on $\mathcal{D}[T_{\tilde{d}}(h)]$ is strictly smaller than that on $\mathcal{D}[\tau_{(d^*)}(h)]$. Please refer to [10, Remark V.1] for details. This shows the superiority of the simultaneous rules over the multi-shot rules. Moreover, by revealing the identities of all honest sensors to the fusion center and adapting the techniques in [11] to the multi-hypothesis case, we obtain a simple converse as follows:

**Proposition 2.** *For any $T$ with both $\mathcal{I}[T] \geq \gamma$ and $\mathcal{A}[T] \geq \gamma$, as $\gamma \to \infty$, $\mathcal{D}[T] \gtrsim \frac{\log\gamma}{|\mathcal{N}|I^*}$.*

Now, when $\sqrt{\log\gamma} \sim |\mathcal{N}|$, one observes that the scaling with respect to $|\mathcal{N}|$ in Corollary 2 and that in Proposition 2 are within a factor of 2.

We now study the asymptotic performance for fixed $|\mathcal{N}|$.

**Corollary 3.** *For any $|\mathcal{N}| > M$, by plugging the threshold in* (21) *with $d = |\mathcal{N}|$ into* (20)*, one shows an achievability on the first-order asymptotic delay as*

$$\mathcal{D}[T_{|\mathcal{N}|}(h)] \sim \frac{\log(\gamma)}{(|\mathcal{N}|-M)I^*}. \tag{22}$$

Encouraged by our recent success of proving a tight converse for the binary case in [12], we believe that the converse in Proposition 2 is not tight and (22) is the optimal asymptotic performance. We leave the proof as future work.

## Appendix A
## Proof of Lemma 1

Fix $q \in [Q]$ and $k \in \mathcal{N}$. For any $j \in [Q]^+$ with $j \neq q$, the CUSUM statistics $Y_t^k(q,j)$ at sensor $k$ can be decomposed as $Y_t^k(q,j) = Z_t^k(q,j) + \xi_t^k(q,j)$, where

$$Z_t^k(q,j) := \sum_{s=1}^{t} \log\left(\frac{P_q(X_s^k)}{P_j(X_s^k)}\right), \xi_t^k(q,j) := -\min_{0\leq s<t} Z_s^k(q,j).$$

Under $\mathbb{P}_q$, $Z^k(q,j)$ is a random walk with drift $I(q,j) > 0$ and variance $\sigma^2(q,j) < \infty$. It follows that $Z_t^k(q)$, defined as $(Z_t^k(q,1),\ldots,Z_t^k(q,q-1),Z_t^k(q,0),Z_t^k(q,q+1),\ldots,Z_t^k(q,Q))$, is a $Q$-dimensional random walk. Also $Y_t^k(q)$, which is similarly defined as $Z_t^k(q)$ by replacing $Z_t^k(q,j)$ with $Y_t^k(q,j)$, is a $Q$-dimensional perturbed random walk, as discussed in [13, Section 6.10][1].

Now for any $j \in [Q]^+$ with $j \notin \{q, j^*\}$, at time index $\sigma_k^{q,j^*}(h)$ in (17), the CUSUM statistics for hypotheses $(q,j)$

$$\frac{Y^k_{\sigma_k^{q,j^*}(h)}(q,j)}{h} \to \frac{I(q,j)}{I(q,j^*)} = \frac{I(q,j)}{I^q} \quad \text{as } h\to\infty, \quad \mathbb{P}_q\text{-a.s.,}$$

by [13, Theorem 10.1, p.206]. This, together with Assumption 1, implies that it holds $\mathbb{P}_q$-a.s. that $\forall j \in [Q]^+ \setminus \{q, j^*\}$

$$\frac{Y^k_{\sigma_k^{q,j^*}(h)}(q,j)}{h} > 1, \tag{23}$$

as $h$ is large enough. Now, observe that from (5), $\sigma_k^q(h) = \inf\left\{t \in \mathbb{N} : \min_{0\leq j\leq Q,\ j\neq q} Y_t^k(q,j) \geq h\right\}$, and the RHS equals to

$$\inf\left\{t\in\mathbb{N}: \min_{0\leq j\leq Q,\ j\notin\{q,j^*\}} Y_t^k(q,j) \geq h \text{ and } Y_t^k(q,j^*) \geq h\right\}$$
$$= \sigma_k^{q,j^*}(h), \quad \text{as } h \text{ is large enough}, \qquad \mathbb{P}_q\text{-a.s.},$$

where the last line follows from (23). Since this relation is true for all $k \in \mathcal{N}$ and $\mathcal{N}$ is a finite set, we conclude that $\sigma_k^q(h) = \sigma_k^{q,j^*}(h)$ for all $k \in \mathcal{N}$ as $h$ is large enough, $\mathbb{P}_q$-a.s. This concludes the proof for part (i).

For part (ii), from (8), $S_d^q(h)$ is equal to

$$\inf\big\{t\in\mathbb{N}: \min_{0\leq j\leq Q,\ j\neq q} Y_t^k(q,j) \geq h \ \ \forall k\in\mathcal{L}, \text{ for some } \mathcal{L}\subset[\mathcal{N}],\ |\mathcal{L}|=d\big\}.$$

Then from (23), $S_d^q(h)$ becomes

$$\inf\big\{t\in\mathbb{N}: Y_t^k(q,j^*) \geq h \ \forall k\in\mathcal{L}, \text{for some } \mathcal{L}\subset[\mathcal{N}], |\mathcal{L}|=\ell\big\}$$
$$= \inf\left\{t\in\mathbb{N}: Y_t^{(K-d+1)}(q,j^*) \geq h\right\}.$$

Then as $h\to\infty$, $\mathbb{P}_q$-a.s. we have $S_d^q(h) = S_d^{q,j^*}(h)$.

[1]Note that while the exposition in [13, Section 6.10] focuses on two-dimensional perturbed random walks, the same results there can be generalized to multi-dimensional cases as stated in [13, Remark 10.1, p. 208].

## References


[1] J. Wurm, Y. Jin, Y. Liu, S. Hu, K. Heffner, F. Rahman, and M. Tehranipoor, "Introduction to cyber-physical system security: A cross-layer perspective," *IEEE Trans. Multi-Scale Comput. Syst., to appear*.

[2] Y.-P. E. Wang, X. Lin, A. Adhikary, A. Grovlen, Y. Sui, Y. Blankenship, J. Bergman, and H. S. Razaghi, "A primer on 3GPP narrowband internet of things," *IEEE Comm. Mag.*, vol. 55, no. 3, pp. 117–123, March 2017.

[3] "Operations and maintenance saving from advanced metering infrastructure - initial results," Technical Report, U.S. Dept. Energy, Office Elect. Del. Energy Rel., Dec. 2012. [Online]. Available: http://energy.gov/sites/prod/files/AMI%5FSavings%5FDec2012Final.pdf

[4] S. Li, Y. Yılmaz, and X. Wang, "Quickest detection of false data injection attack in wide-area smart grids," *IEEE Trans. Smart Grid*, vol. 6, no. 6, pp. 2725–2735, Nov. 2015.

[5] G. Fellouris, E. Bayraktar, and L. Lai, "Efficient Byzantine sequential change detection," *IEEE Trans. Inf. Theory*, vol. 64, no. 5, pp. 3346–3360, May 2018.

[6] T. Oskiper and H. V. Poor, "Online activity detection in a multiuser environment using the matrix CUSUM algorithm," *IEEE Trans. Inf. Theory*, vol. 48, no. 2, pp. 477–493, 2002.

[7] T. Cover and J. Thomas, *Elements of Information Theory*. New York: Wiley, 1991.

[8] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, *Introduction to algorithms*. MIT press, 2009.

[9] I. V. Nikiforov, "A generalized change detection problem," *IEEE Trans. Inf. Theory*, vol. 41, no. 1, pp. 171–187, Jan. 1995.

[10] Y.-J. Huang, S.-C. Lin, and Y.-C. Huang, "On Byzantine distributed sequential change detection with multiple hypotheses." [Online]. Available: http://www-o.ntust.edu.tw/%7Esclin/paper/MultiQCD.pdf

[11] Y. Mei, "Information bounds and quickest change detection in decentralized decision systems," *IEEE Trans. Inf. Theory*, vol. 51, no. 7, pp. 2669–2681, Jul. 2005.

[12] Y.-C. Huang, S.-C. Lin, and Y.-J. Huang, "A tight converse to the asymptotic performance of Byzantine distributed sequential change detection," in *Proc. IEEE ISIT*, 2019, submitted.

[13] A. Gut, *Stopped random walks*, 2nd ed., ser. Springer Series in Operations Research and Financial Engineering. Springer, New York, 2009, limit theorems and applications.