Distributed Sequential Hypothesis Testing with Byzantine Sensors

Zishuo Li, *Student Member, IEEE*, Yilin Mo, *Member, IEEE* and Fei Hao

***Abstract*—This paper considers the problem of sequential binary hypothesis testing based on observations from a network of m sensors where a subset of the sensors is compromised by a malicious adversary. The asymptotic average sample number required to reach a certain level of error probability is selected as the performance metric of the system. We propose an asymptotically optimal voting algorithm for the sensor network with a fusion center and generalize it to fully-distributed networks, where the algorithm stays asymptotically optimal under the weak assumption that the sensor network is connected. Moreover, we prove that both of the proposed algorithms are asymptotically optimal in the presence of Byzantine sensors, in the sense that each of them forms a Nash equilibrium with the worst-case attack (flip-attack). Compared to existing distributed detection strategies, the proposed scheme has a low message complexity, which is independent of the error probability and the sample number, by taking advantage of the sparsity of votes. The results are corroborated by numerical simulations.**

***Index Terms*—Sequential analysis, Distributed algorithms, Wireless sensor networks, Byzantine attack, Fault tolerant systems, Asymptotic optimality.**

I. Introduction

Background and Motivation:

Distributed inference with sensor networks has drawn substantial research attention due to its wide application in wireless sensor networks [1], power grids, cognitive radio [2], smart building, Internet of Things, etc. As sensors in the network are usually spatially separated and communicate by wired/wireless channels, they are exposed to various interference and attacks. Therefore, it is crucial that the distributed detection schemes can withstand a certain number of corrupted agents.

Recent studies on resilient distributed detection include fault identification schemes [3] [4] and tolerant schemes [5] [6], etc., as summarized in [7]. Rawat et al. [3] quantified the reputation of a sensor by its time of mismatches with the final decision, and the sensor with worse reputation (more mismatches) over a threshold will be tagged as Byzantines and removed from the decision process. Ren et al. [6] pursued an efficient and resilient detection scheme by removing the statistics with the largest deviation from the decision-making process.

The aforementioned distributed detection schemes assume the existence of a fusion center (FC) that can communicate with all the sensors in the network. However, the fusion center is subject to single point of failure. Furthermore, due to various practical constraints such as transmitting distance of wireless channel and power limit of a sensor, it may be desirable to adopt a peer-to-peer local information exchange scheme, i.e., fully-distributed scheme. Research on fully-distributed detection problem progress significantly based on average consensus algorithm. The Belief Consensus algorithm proposed by Olfati-Saber et al. [8] solved the distributed detection problem using the average consensus algorithm to calculate the likelihood values (or beliefs) in a Bayesian network. Kar and Moura [9] [10] focused on the topology optimization problem subjecting to communication noise, random topology switch, and communication constraints. Besides the methods that only carry out consensus on sensors' states, works in [11] [12] solved the consensus problem by updating the state based on neighbors' states and new local observations at the same time, which is referred as consensus+innovation distributed algorithm.

However, naive average consensus algorithm utilized in the previous distributed detection schemes is not resilient when there are malicious agents in the network [13]. Research on resilient variants of consensus-based detection scheme includes attempts to exclude nodes from the value consensus process with significant deviated states [2] [14] and weight design to mitigate the effect of data falsification attacks [15]. Furthermore, most of the algorithms based on naive consensus and their secure variants suffer from high communication complexity, which is at least proportional to time because they perform value averaging (almost) every time step.

In contrast to the previous fixed sample size analysis or static stopping scheme that gives a decision or belief whenever new observations arise, another path to tackle the hypothesis testing problem is sequential hypothesis testing or sequential analysis approach proposed by Wald [16]. The number of samples needed for sequential analysis is not known in advance. The system stops taking observations as soon as the existing statistics are enough to make a decision. The goal is to make decisions about the hypothesis with as few observations as possible while controlling the probability of making mistakes. Since the number of samples is adjusted dynamically according to the current statistics, sequential testing is more sample-efficient than static ones [17]. Moreover, the optimality of *Sequential Probability Ratio Test* (SPRT) has been proved by Wald et al. [18], and the optimal nature of SPRT attracts a considerable amount of research on the fusion center formulation of multi-sensor SPRT [19] [20] [21]. However, to the best of our knowledge, research on either the security problem or the fully-distributed formulation of

Z. Li and Y. Mo are with the Department of Automation and BNRist, Tsinghua University, China. Email: lizs19@mails.tsinghua.edu.cn, ylmo@tsinghua.edu.cn.

F. Hao is with School of Automation Science and Electrical Engineering, Beihang University, China. Email: fhao@buaa.edu.cn.

This work is supported by the National Key Research and Development Program of China under Grant 2018AAA0101601.

sequential hypothesis testing has not been well explored.

Our work and contribution:

We consider the distributed binary hypothesis testing problem where a binary state $\theta = \{0,1\}$ is detected by a group of m sensors that generate observations according to a background hypothesis. c out of m sensors are manipulated by a malicious adversary who can inject arbitrary data into the observations and communication messages at compromised sensors. This paper aims to design a distributed detection scheme to decide on the time to stop and the hypothesis to choose based on observations from the partly corrupted sensor network with minimum average sample number under error probability constraints. Our previous result has been published in [22]. The main contributions of this paper are summarized as follows:

(1) We propose a voting detection scheme named VSPRT (*voting SPRT*, Section III, IV) in fusion center scenario and a generalized scheme named DVSPRT (*distributed voting SPRT*, Section V) in fully-distributed scenario.

(2) We quantify the *limit distribution* of the sample number of VSPRT and DVSPRT while most existing works consider the *expectation* of sample number. Based on this more refined analysis, we prove that our proposed VSPRT and DVSPRT are both order-1 asymptotic optimal and quantify their gap from the theoretical optimal. Moreover, the optimality of DVSPRT holds for arbitrary topology as long as the graph is connected.

(3) In the presence of attack, when the number of compromised sensors is known, we prove that the detection strategy VSPRT (DVSPRT) and system disturbing strategy flip-attack form a Nash equilibrium pair, i.e., the proposed VSPRT (DVSPRT) scheme achieves the fundamental limit among *all* possible detection strategies. When the number of compromised sensors is unknown, the proposed schemes are still resilient with appropriate parameter choice.

(4) We further prove that the proposed DVSPRT scheme has message complexity $O(mM)$[1], which is *independent* of error probability and sample number. In contrast, the message complexity of most fully-distributed detection schemes in the literature is $O(mMT)$, which scales linearly with respect to detection delay T, i.e., decreasing error probability requires more time (or more samples) and thus more communication energy.

Organization:

The rest of this paper is organized as follows: In Section II, we formulate the problem of sequential binary hypothesis testing, define the performance metric, and demonstrate corresponding fundamental limits. Section III proposes the voting scheme named VSPRT in fusion center formulation, quantifies its performance, and proves its optimality in the absence of attack. In Section IV, the Byzantine attack model is formulated, the performance of VSPRT under attack is quantified. In Section V, VSPRT is generalized to DVSPRT in fully-distributed scenario. We quantify the performance and prove the optimality in the absence and in the presence of attack. We further investigate the resiliency of DVSPRT with communication manipulation and link failure. In Section VI, the results are collaborated by numerical simulations. Section VII finally concludes the paper.

Notations:

We denote by $\mathbb{Z}^+$ the set of strictly positive integers and by $\mathbb{R}$ the set of real numbers. The cardinality of a set $\mathcal{S}$ is denoted as $|\mathcal{S}|$. The transpose of a matrix is denoted by superscript T. If not explicitly stated, ∞ represents $+\infty$. $N(\mu,\sigma^2)$ denotes normal distribution with mean μ and variance σ^2. In particular, $N(0,1)$ denotes standard normal distribution. Let f,g be real-valued functions whose ranges are both unbounded subsets of $\mathbb{R}$. $f(x) \sim g(x)$ with respect to a limit process represents $\lim \frac{f(x)}{g(x)} = 1$. The little o notation $f(x) = o(g(x))$ with respect to a limit process means $\lim \frac{f(x)}{g(x)} = 0$. The big O notation $f(x) = O(g(x))$ with respect to a limit process means $\limsup \frac{|f(x)|}{g(x)} < \infty$.

II. Problem Formulation

A. Sequential Binary Hypothesis Testing

We consider the problem of binary hypothesis testing where a group of m sensors infers a binary state $\theta \in \{0,1\}$ from their measurements. At each discrete time index k ($k \in \mathbb{Z}^+$), the observations are generated at each sensor $i \in \{1,2,...,m\}$ according to θ. Let the column vector $\boldsymbol{z}(k) = [z_1(k), z_2(k), ..., z_m(k)]^T \in \mathbb{R}^m$ denote the observations at time k from all m sensors, and $z_i(k)$ is the observation from sensor i.

For the null hypothesis H_0 ($\theta = 0$), probability measure generated by $z_i(k)$ is denoted as ν_0 and for the alternative hypothesis H_1 ($\theta = 1$), it is denoted as ν_1. In other words, for any Borel-measurable set $\mathscr{B} \subseteq \mathbb{R}$, the probability that $z_i(k) \in \mathscr{B}$ equals to $\nu_\theta(\mathscr{B})$. We assume that all observations from different sensors at different times are identically distributed and conditionally independent given the true hypothesis. Denote the probability space generated by all measurements given the true hypothesis H_θ as $(\Omega, \mathscr{F}, \mathbb{P}_\theta)$, i.e.,

$$\mathbb{P}_\theta(z_{i_1}(k_1) \in \mathscr{B}_1, \ldots, z_{i_l}(k_l) \in \mathscr{B}_l) = \begin{cases} \nu_0(\mathscr{B}_1)\nu_0(\mathscr{B}_2)\ldots\nu_0(\mathscr{B}_l), & \text{given } \theta = 0 \\ \nu_1(\mathscr{B}_1)\nu_1(\mathscr{B}_2)\ldots\nu_1(\mathscr{B}_l), & \text{given } \theta = 1 \end{cases},$$

where $(i_j,k_j) \neq (i_{j'},k_{j'})$ for all $j \neq j'$. The expectation taken with respect to $\mathbb{P}_\theta$ is denoted by $\mathbb{E}_\theta$. We make the following assumptions, which are conventional in statistical inference.

Assumption 1 (Detector knowledge) The probability measure $\nu_\theta, \theta \in \{0,1\}$ is known to the detector.

We further assume that probability measure ν_0 and ν_1 are well-defined:

Assumption 2 (Well-defined probability measure)

(1) Kullback-Leibler (K–L) divergence between ν_0, ν_1 is well-defined[2], i.e., $0 < D_0, D_1 < \infty$, where D_0, D_1 are defined

[1] m is the number of sensors and M is the number of communication links.

[2] The existence of K–L divergence implies that probability measure ν_0, ν_1 are absolutely continuous with respect to each other, that is, for any Borel-measurable set $\mathscr{B} \subseteq \mathbb{R}$, if $\nu_\theta(\mathscr{B}) = 0$ then $\nu_{1-\theta}(\mathscr{B}) = 0$, for both $\theta = 0,1$.

as

$$D_1 \triangleq \int_{z\in\mathbb{R}} \log\left(\frac{\mathrm{d}\nu_1(z)}{\mathrm{d}\nu_0(z)}\right)\mathrm{d}\nu_1,$$
$$D_0 \triangleq \int_{z\in\mathbb{R}} \log\left(\frac{\mathrm{d}\nu_0(z)}{\mathrm{d}\nu_1(z)}\right)\mathrm{d}\nu_0,$$

and $\frac{\mathrm{d}\nu_0(\cdot)}{\mathrm{d}\nu_1(\cdot)}, \frac{\mathrm{d}\nu_1(\cdot)}{\mathrm{d}\nu_0(\cdot)}$ are the Radon-Nikodym derivative.

(2) Variance of log-likelihood ratio is well-defined, i.e., $V_1, V_0 < \infty$, where V_1, V_0 are defined as:

$$V_1 \triangleq \int_{z\in\mathbb{R}} \left[\log\left(\frac{\mathrm{d}\nu_1(z)}{\mathrm{d}\nu_0(z)}\right) - D_1\right]^2 \mathrm{d}\nu_1(z),$$
$$V_0 \triangleq \int_{z\in\mathbb{R}} \left[\log\left(\frac{\mathrm{d}\nu_0(z)}{\mathrm{d}\nu_1(z)}\right) - D_0\right]^2 \mathrm{d}\nu_0(z).$$

Due to the *Law of Large Numbers*, increasing number of observations leads to decreasing error probability. However, in many practical applications, observations are costly and introduce unnecessary delays in decisions. We adopt the framework of *Sequential Analysis* to quantify and optimize the error-delay trade-off. The observation sampling is terminated according to a specific rule, e.g., when error probability reaches a certain threshold. To be precise, at every time k, the decision is made by choosing one element from the set of decisions:

$$f_k \in \{\text{continue}, 0, 1\},$$

where the choice "continue" means taking next round of observations at time $k+1$ since existing observations are insufficient to support either hypothesis. Decision $f_k = \theta$ means stop taking observations and choosing hypothesis H_θ at time k ($\theta = 0,1$). A detection strategy or a hypothesis testing scheme[3] $f \triangleq \{f_1, f_2, \cdots\}$ is defined as an infinite sequence of decisions from time 1 to ∞.

B. Performance Evaluation and Fundamental Limits

Define the (random) stopping time T with respect to strategy f as:

$$T \triangleq \inf\{k | f_k \neq \text{continue}\}.$$

T is a $\{\mathscr{F}_k\}$-stopping time, where $\mathscr{F}_k$ is a σ-field of all the observations from time 1 to k: $\mathscr{F}_k = \sigma\{\boldsymbol{z}(1), \boldsymbol{z}(2), \cdots, \boldsymbol{z}(k)\}$. In the context of sequential test, T denotes the *sample number* or *delay* required to make a decision. We will use these two terms interchangeably in the remainder of the paper.

The type-I error (false alarm rate) and type-II error (missing detection rate) are respectively probabilities of making a wrong decision when the background hypothesis is H_0 and H_1:

$$\text{type-I error: } e_0 = \mathbb{P}_0(f_T = 1), \tag{1}$$
$$\text{type-II error: } e_1 = \mathbb{P}_1(f_T = 0), \tag{2}$$

where f_T represents the decision at termination moment T. We consider the following problem where the expected delay is minimized under error probability constraints, which is conventional in literature considering optimality of sequential test (e.g., [20] [23]).

Problem 1

$$\min_f \mathbb{E}_\theta[T], \;\; \theta = 0,1$$
$$\text{s.t. } e_0 \le \alpha, e_1 \le \beta. \tag{3}$$

Define the set of all admissible detection strategies that satisfy the error probability constraint as

$$\mathcal{F} \triangleq \{f | e_0 \le \alpha, e_1 \le \beta\}, \tag{4}$$

where $0 < \alpha, \beta < 1$. Wald et al. [18] has proved that for a single sensor, among all $f \in \mathcal{F}$, SPRT optimizes Problem 1 for both $\theta = 0$ and $\theta = 1$ simultaneously. However, for distributed detection problem, it is in general intractable from a dynamic programming point of view [24], and we turn to asymptotic optimality analysis. Following definition in [20] [23], we define the order of asymptotic optimality.

Definition 1 (Optimality) Let $\mathcal{T}^*(m)$ be the stopping time of the optimum detection strategy with m sensors that satisfies the two error probability constraints in (3) with equality. Then, as[4] $\alpha, \beta \to 0$, the detection strategy in $\mathcal{F}$ with stopping time T is said to be order-1 asymptotically optimal if

$$1 \le \frac{\mathbb{E}_\theta[T]}{\mathbb{E}_\theta[\mathcal{T}^*(m)]} \le 1 + o(1)$$

holds for both $\theta = 0$ and $\theta = 1$. It is order-2 asymptotically optimal if

$$0 \le \mathbb{E}_\theta[\mathcal{T}^*(m)] - \mathbb{E}_\theta[T] \le O(1)$$

holds for both $\theta = 0$ and $\theta = 1$.

Moreover, the minimum expected stopping time among all $f \in \mathcal{F}$ is provided in the following. The proof is referred to [25].

Proposition 1 (Fundamental Limit) Recalling that $\mathcal{T}^*(m)$ is the stopping time of the optimum detection strategy among $\mathcal{F}$ with m sensors, we have

$$\mathbb{E}_0[\mathcal{T}^*(m)] = \frac{1}{mD_0}\left[\alpha \log\frac{1-\beta}{\alpha} + (1-\alpha)\log\frac{\beta}{1-\alpha}\right], \tag{5}$$
$$\mathbb{E}_1[\mathcal{T}^*(m)] = \frac{1}{mD_1}\left[(1-\beta) \log\frac{1-\beta}{\alpha} + \beta\log\frac{\beta}{1-\alpha}\right]. \tag{6}$$

As $\alpha, \beta \to 0$, results above can also be written as

$$\mathbb{E}_0[\mathcal{T}^*(m)] = \frac{|\log\beta|}{mD_0} + O(1), \;\; \mathbb{E}_1[\mathcal{T}^*(m)] = \frac{|\log\alpha|}{mD_1} + O(1).$$

The results in Proposition 1 provide lower bounds of $\mathbb{E}_\theta[T]$ for all possible detection strategies. Based on these performance bounds, we will prove the optimality of our proposed detection strategies in Section III (fusion center) and Section V (fully-distributed).

III. Voting scheme with fusion center

In this section, we consider the scenario where there is a fusion center that can communicate with every sensor in the

[3] In the remainder of the paper, a *detection strategy* or a *detection scheme* specifically refers to a sequential binary hypothesis testing algorithm design, inducing when to stop and which hypothesis to choose, denoted as f.

[4] In order to prevent degradation problems, the limit process $\alpha, \beta \to 0$ in this paper is assumed to satisfy $0 < \lim \alpha/\beta < \infty$. This assumption is made throughout the paper unless stated otherwise.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSP.2021.3075147, IEEE Transactions on Signal Processing

network. This formulation covers many practical applications (e.g., building environment control system and wearable smart devices) where there is a control unit in local sensor network that has direct access to the data in every sensor. We will propose a voting scheme in this formulation based on single sensor SPRT and decision voting. It is named as VSPRT (short for *voting SPRT*) in this paper. We will present the VSPRT scheme, quantify its performance and prove its optimality. This scheme will be used as a baseline to evaluate the performance of fully-distributed detection schemes in subsequent sections.

A. Voting SPRT

Voting SPRT is a detection strategy where every sensor calculates its local cumulative log-likelihood ratio

$$S_i(n) \triangleq \sum_{k=1}^{n} l_i(k) = \sum_{k=1}^{n} \log\left(\frac{\mathrm{d}\nu_1(z_i(k))}{\mathrm{d}\nu_0(z_i(k))}\right) \tag{7}$$

and compares $S_i(n)$ with a pair of thresholds $h_0, h_1 > 0$. The thresholds are chosen according to the error probability constraints:

$$h_1 = \frac{-\log\alpha + \log\binom{m}{r}}{r}, \quad h_0 = \frac{-\log\beta + \log\binom{m}{r}}{r}, \tag{8}$$

where $\binom{m}{r}$ is the combinatorial number of picking r unordered outcomes from m possibilities. The integer r ($1 \le r \le m$) is the minimum number of votes required to support a hypothesis for final decision. This number r is an adjustable parameter of the VSPRT scheme. Sensor i casts a ballot supporting H_1 (H_0) at the first time when random walk $S_i(k)$ crosses the threshold h_1 (h_0). The corresponding stopping times are defined as

$$\tau_i^+(h_1) \triangleq \inf_{k\in\mathbb{Z}^+} \{k | S_i(k) \ge h_1\}, \tag{9}$$

$$\tau_i^-(h_0) \triangleq \inf_{k\in\mathbb{Z}^+} \{k | S_i(k) \le -h_0\}. \tag{10}$$

The two first-passage time $\tau_i^+(h_1)$ and $\tau_i^-(h_0)$ are also the moments when sensor i reports a vote supporting hypothesis H_1 and hypothesis H_0 respectively. In the following we omit the thresholds h_0, h_1 and parentheses and denote them as τ_i^+, τ_i^- for notation simplicity. The vote indicators at time k for hypothesis H_1 and hypothesis H_0 are defined respectively as

$$\delta_i^+(k) \triangleq \left\{ \begin{array}{ll} 1, & k \ge \tau_i^+ \\ 0, & k < \tau_i^+ \end{array} \right., \quad \delta_i^-(k) \triangleq \left\{ \begin{array}{ll} 1, & k \ge \tau_i^- \\ 0, & k < \tau_i^- \end{array} \right.. \tag{11}$$

The vote indicator is used to indicate whether sensor i has cast a vote at time k. Since every sensor has only one vote for each of the two hypotheses, each of the indicator changes at most once among all the time steps $k \in \mathbb{Z}^+$. The indicator $\delta_i^+(k)$ jumps from 0 to 1 when sensor i reports a vote supporting H_1. It is similar for $\delta_i^-(k)$ and H_0.

Remark 1 The random walk $S_i(k)$ may cross the same threshold multiple times but only the first cross of h_1 will cast a vote for hypothesis H_1, and only the first cross of $-h_0$ will cast a vote for hypothesis H_0. Moreover, one sensor may send votes for both hypotheses at different time steps (see Fig.1).

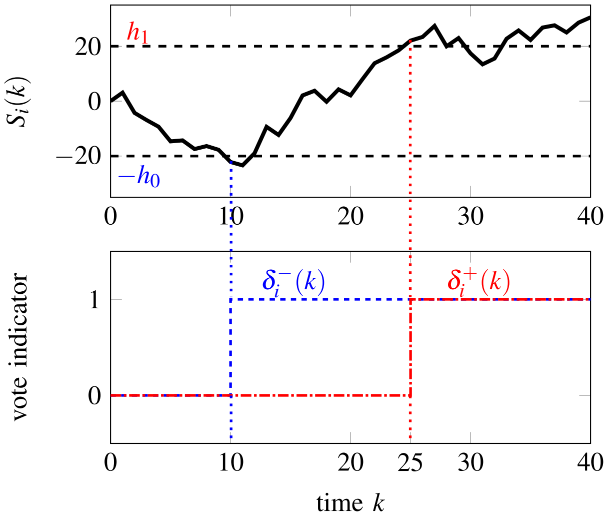

Fig. 1. An example with thresholds $h_1 = h_0 = 20$. The sensor i vote for both hypotheses.

Denote the first moment that there are (at least) r votes of same type as:

$$\tau^+(r) \triangleq \inf_{k\in\mathbb{Z}^+} \left\{ k \,\middle|\, \sum_{i=1}^{m} \delta_i^+(k) \ge r \right\}, \tag{12}$$

$$\tau^-(r) \triangleq \inf_{k\in\mathbb{Z}^+} \left\{ k \,\middle|\, \sum_{i=1}^{m} \delta_i^-(k) \ge r \right\}. \tag{13}$$

As soon as there are r votes supporting the same hypothesis, the VSPRT scheme stops sampling and chooses the corresponding hypothesis as the final decision, i.e.,

$$f_k(r) = \left\{ \begin{array}{ll} 0, & k = \tau^-(r) \le \tau^+(r) \\ 1, & k = \tau^+(r) < \tau^-(r) \\ \text{continue}, & k < \min\{\tau^+(r), \tau^-(r)\} \end{array} \right.. \tag{14}$$

The VSPRT scheme is denoted as $f(r) \triangleq \{f_k(r)\}_{k=1}^{\infty}$. The corresponding stopping time is defined as

$$\tau(r) \triangleq \min\{\tau^+(r), \tau^-(r)\}. \tag{15}$$

B. Performance of VSPRT

In this subsection, we quantify the performance of VSPRT. In existing works in the literature [6] [21] [23] and our previous work [22], the stopping time T is quantified using expectation $\mathbb{E}[T]$. It is insufficient to characterize the randomness of T. For instance, two stopping times may have the same expectation, but the one with larger variance has more uncertainty and larger probability of being extremely large.

In order to establish more accurate analysis on random stopping time T, we consider the γ-quantile $(0 < \gamma < 1)$ of distribution of T as a finer metric:

$$t_{\theta,\gamma}(T) \triangleq \inf_{t\in\mathbb{R}^+} \{t \,|\mathbb{P}_\theta(T \le t) \ge \gamma\}, \; \theta = 0, 1. \tag{16}$$

In other words, function $t_{\theta,\gamma}(T)$ with respect to γ is the inverse function of the cumulative distribution function (CDF) of T. This finer characterization of T enables us to quantify the higher-order optimality of detection strategy and evaluate real-world performance more accurately. Define the CDF of standard normal distribution as $\Phi(\cdot)$. The corresponding inverse function is denoted as $\Phi^{-1}(\cdot)$. The performance of VSPRT is quantified in the following theorem whose proof is provided in Appendix B.

Theorem 1 For VSPRT scheme defined in (14) with $m/2 < r \le m$, we have the following results:

$$t_{0,\gamma}\left(\tau^-(r)\right) \le \frac{|\log\beta|}{rD_0} + \Phi^{-1}\left(\gamma^{\frac{1}{m}}\right)\sqrt{\frac{V_0|\log\beta|}{rD_0^3}} + o\left(\sqrt{|\log\beta|}\right), \tag{17}$$

$$t_{1,\gamma}\left(\tau^+(r)\right) \le \frac{|\log\alpha|}{rD_1} + \Phi^{-1}\left(\gamma^{\frac{1}{m}}\right)\sqrt{\frac{V_1|\log\alpha|}{rD_1^3}} + o\left(\sqrt{|\log\alpha|}\right), \tag{18}$$

as $\alpha,\beta\to 0$. The equalities are achieved when $r = m$.

Based on Theorem 1, we are able to quantify the distribution of stopping time with $r = m$, i.e., $\tau^-(m)$ and $\tau^+(m)$. Define $N^m(0,1)$ as the probability distribution whose CDF is $[\Phi(\cdot)]^m$. The probability distributions of $\tau^-(m)$ and $\tau^+(m)$ are quantified in Corollary 1 whose proof is in Appendix B.

Corollary 1 In the absence of attack, the stopping times $\tau^+(m)$ and $\tau^-(m)$ satisfy the following as $\alpha,\beta\to 0$:

$$\frac{\tau^+(m) - \frac{|\log\alpha|}{D_1}}{\sqrt{\frac{V_1}{D_1^3}|\log\alpha|}} \xrightarrow{d} N^m(0,1), \quad \frac{\tau^-(m) - \frac{|\log\beta|}{D_0}}{\sqrt{\frac{V_0}{D_0^3}|\log\beta|}} \xrightarrow{d} N^m(0,1),$$

where $\xrightarrow{d}$ means convergence in distribution. Hence, the corresponding expectation satisfy

$$\mathbb{E}_1[\tau(m)] \le \mathbb{E}_1[\tau^+(m)] \le \frac{|\log\alpha|}{mD_1} + O\left(\sqrt{|\log\alpha|}\right), \tag{19}$$

$$\mathbb{E}_0[\tau(m)] \le \mathbb{E}_0[\tau^-(m)] \le \frac{|\log\beta|}{mD_0} + O\left(\sqrt{|\log\beta|}\right), \tag{20}$$

as $\alpha,\beta\to 0$, and VSPRT with $r = m$ is of order-1 optimal .

In order to give the readers a more intuitive understanding about the limit distribution $N^m(0,1)$, its cumulative distribution function (CDF) and probability density function (PDF) are illustrated in Fig. 2.

According to Theorem 1 and Corollary 1, choosing larger r leads to better performance because it reduces the first-order term $\frac{|\log\beta|}{rD_0}$ ($\frac{|\log\alpha|}{rD_1}$) and thus reduces detection delay while holding the same error probability. Therefore, choosing the largest $r = m$ yields the asymptotic least expected delay and further leads to order-1 optimality. This result coincides with Mei's SPRT in [19].

However, as one can verify, a random variable drawn from distribution $N^m(0,1)$ has strictly positive expectation when $m > 1$, which means there is a gap between $\mathbb{E}_\theta[\tau(m)]$ and the optimal $\mathbb{E}_\theta[\mathcal{T}^*(m)]$. The gap is of order $\sqrt{|\log\alpha|}$ and goes to infinity as $\alpha\to 0$. Similar results also apply on β. Therefore, our proposed VSPRT is not order-2 optimal when $m > 1$. Even though VSPRT is not higher-order optimal, it has the following merits:

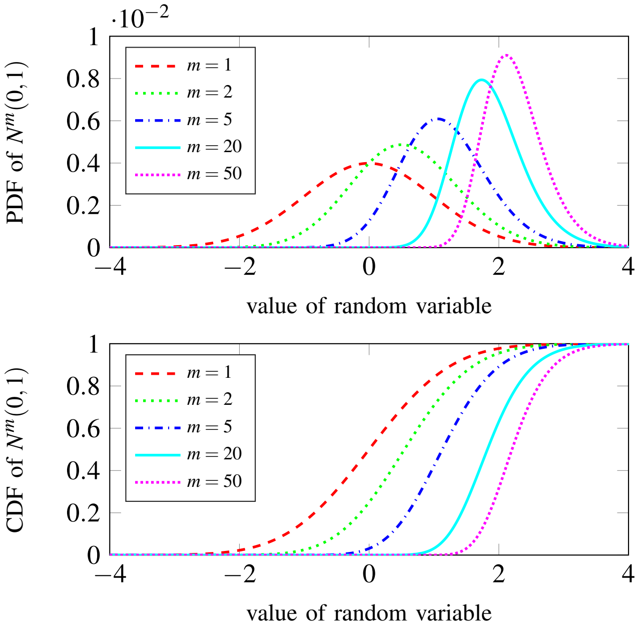

Fig. 2. The PDF and CDF of distribution $N^m(0,1)$ with different m. When $m > 1$, the expectation of distribution $N^m(0,1)$ is strictly positive.

(1) VSPRT is resilient to Byzantine sensors by a conservative choice of $r < m$. Moreover, as will be shown in Section IV, VSPRT is optimal against attack considering the worst-case performance.

(2) VSPRT is easily generalized to fully-distributed scenarios with low message complexity by taking advantage of the sparsity of the votes. In Section V, we leverage these merits to design a fully-distributed resilient detection scheme named DVSPRT (*distributed voting SPRT*).

IV. VSPRT with Byzantine Sensors

This section demonstrates that the VSPRT scheme is resilient to Byzantine attack on an unknown subset of sensors. The attack model is formulated, and the fundamental limit of the average sample number in the presence of attack is established. Moreover, we prove that VSPRT achieves this fundamental limit.

A. Attack Model

Malicious adversary manipulates data by adding bias values on the measurements of the compromised sensors. At time k, the measurements received by all the sensors can be collected as a vector

$$\boldsymbol{y}(k) = \boldsymbol{z}(k) + \boldsymbol{a}(k), \tag{21}$$

where $\boldsymbol{z}(k)$ is the true measurement generated according to background hypothesis, and $\boldsymbol{a}(k)$ is the bias vector injected by the attacker. The i-th entry $y_i(k)$ is the manipulated observation at sensor i. Define the support of vector $\boldsymbol{a} \in \mathbb{R}^m$ as $\mathrm{supp}(\boldsymbol{a}) \triangleq \{i | 1 \le i \le m, a_i \ne 0\}$ where a_i is the i-th entry of vector $\boldsymbol{a}$. Denote the index set of all sensors as $\mathcal{S} \triangleq \{1,2,\ldots,m\}$. We have the following assumptions on the malicious adversary.

Assumption 3 (Sparse Attack) There exists a time invariant index set $\mathcal{C} \subseteq \mathcal{S}$ with $|\mathcal{C}| = c$ such that $\bigcup_{k=1}^{\infty} \operatorname{supp}\{\boldsymbol{a}(k)\} = \mathcal{C}$. Furthermore, the detector knows the cardinality c, but it does not know the set $\mathcal{C}$. We further assume less than half of the sensors are compromised, i.e., $m > 2c$.

Remark 2 It is conventional in the literature (e.g., [26] [27]) to assume that the attacker possesses limited resources, i.e., can only corrupt a subset of sensors with known cardinality. Assumption 3 does not rule out the case where the number of compromised sensors is unknown. Number c is a design parameter set up by the system operator representing how many compromised sensors the detection scheme can tolerate. If the exact number of compromised sensors is no greater than c, the proposed scheme is still resilient. Otherwise, the system may be compromised, and we need a larger c for algorithm design.

Motivated by the unencrypted and encrypted communication in sensor networks, we define two kinds of attackers distinguished by their information set.

Assumption 4 (Attacker Knowledge)

A weak attacker has the following information: 1) the probability measure, i.e., ν_0 and ν_1; 2) the real system state θ; 3) the historical original measurements from compromised sensors: $\{z_i(n) : i \in \mathcal{C}, 1 \le n \le k\}$. Besides the information above, a strong attacker also knows the historical original measurements from honest sensors: $\{z_i(n) : i \in \mathcal{S} \setminus \mathcal{C}, 1 \le n \le k\}$.

Remark 3 In real-world scenarios, most binary hypothesis testing problems focus on monitoring an interested state, and an alarm is triggered when the state deviates from the normal one. For instance, the sensors monitor the smoke and temperature for fire alarm. In this case, the hypothesis H_0 represents the safe state and H_1 represents the abnormal state. It is possible that the malicious attacker is the cause of an abnormal state H_1 (e.g., causing fire) and intends to remain undetected by the system at the same time by manipulating sensor readings. Therefore, the assumption that the attacker knows the true hypothesis is reasonable for these scenarios and has a real-world background.

For an unencrypted sensor network, a Byzantine attacker is modeled as a strong attacker who has access to all sensors' observations. For an encrypted sensor network, only observations at compromised sensors are known to the adversary, and the Byzantine attacker is modeled as a weak attacker. It will be claimed in Remark 5 that the delay upper bound of VSPRT in presence of strong attacker and weak attacker is the same, i.e., in the sense of worst-case performance, knowing observations at honest sensors cannot benefit an attacker when using VSPRT.

An admissible attack strategy is a mapping from attacker's information set to the bias vector:

$$\text{weak attacker: } \left\{\theta, \mathcal{C}, k, \{z_i(n)\}_{i \in \mathcal{C}, n \le k}\right\} \xrightarrow{g} \boldsymbol{a}(k),$$

$$\text{strong attacker: } \left\{\theta, \mathcal{C}, k, \{z_i(n)\}_{i \in \mathcal{S}, n \le k}\right\} \xrightarrow{g} \boldsymbol{a}(k),$$

where g is a measurable function, and $\boldsymbol{a}(k)$ satisfies Assumption 3.

Remark 4 With the constraints in Assumptions 3 and 4, the adversary still has adequate knowledge about the system and can carry out complex attack strategies such as time-varying or probabilistic ones. The compromised sensors can "cooperate" since bias vector is designed based on global information from all compromised sensors.

Denote the probability measure and expectation under attack strategy g on set $\mathcal{C}$ as $\mathbb{P}_{\theta}^{g,\mathcal{C}}$ and $\mathbb{E}_{\theta}^{g,\mathcal{C}}$. The corresponding error probabilities under attack are defined as the largest one among all possible $\mathcal{C}$:

$$e_0^g \triangleq \max_{|\mathcal{C}|=c} \mathbb{P}_0^{g,\mathcal{C}}[f_T = 1], \; e_1^g \triangleq \max_{|\mathcal{C}|=c} \mathbb{P}_1^{g,\mathcal{C}}[f_T = 0]. \tag{22}$$

The expected delay is defined similarly:

$$\mathbb{E}_{\theta}^{g}[T] \triangleq \max_{|\mathcal{C}|=c} \mathbb{E}_{\theta}^{g,\mathcal{C}}[T], \; \theta = 0, 1. \tag{23}$$

Recalling definition in (16), $t_{\theta,\gamma}(\cdot)$ under attack g is defined as

$$t_{\theta,\gamma}^{g}(T) \triangleq \max_{|\mathcal{C}|=c} \inf_{t} \left\{ t | \mathbb{P}_{\theta}^{g,\mathcal{C}}(T \le t) \ge \gamma \right\}, \; \theta = 0, 1. \tag{24}$$

B. Fundamental Limits

In this subsection, we propose an attack strategy which provides a fundamental performance limit for all admissible detection scheme. Define sensor index set

$$\mathcal{O}_0 \triangleq \{1, 2, \ldots, c\}, \; \mathcal{O}_1 \triangleq \{m - c + 1, m - c + 2, \ldots, m\}.$$

The attacker first generates random observations $y_i(k)$ at time k for every sensor $i \in \mathcal{O}_{\theta}$ according to the distribution which is opposite to the real hypothesis, i.e., the following holds for each Borel set $\mathscr{B}$:

$$\mathbb{P}[y_i(k) \in \mathscr{B}] = \nu_1(\mathscr{B}), \; \forall i \in \mathcal{O}_1, \text{ given } \theta = 0. \tag{25}$$

$$\mathbb{P}[y_i(k) \in \mathscr{B}] = \nu_0(\mathscr{B}), \; \forall i \in \mathcal{O}_0, \text{ given } \theta = 1. \tag{26}$$

Then design the injected bias data $a_i(k)$ to make sure the final observation $z_i(k) + a_i(k)$ of sensor $i \in \mathcal{O}_0 \cup \mathcal{O}_1$ is the same as $y_i(k)$:

$$a_i(k) = y_i(k) - z_i(k), \; i \in \mathcal{O}_0 \cup \mathcal{O}_1. \tag{27}$$

We denote the attack strategy defined in (25) to (27) as g^*. It is called *flip-attack* in this paper. We have the following theorem quantifying the performance fundamental limits of all detection schemes under the proposed attack g^*.

Theorem 2 For any admissible detection strategy f under flip-attack g^*, we have the following results for the stopping time T with respect to strategy f:

$$\inf_{f \in \mathcal{F}} \mathbb{E}_0^{g^*}[T] \ge \mathbb{E}_0[\mathcal{T}^*(m - 2c)] = \frac{|\log \beta|}{(m - 2c) D_0} + O(1), \tag{28}$$

$$\inf_{f \in \mathcal{F}} \mathbb{E}_1^{g^*}[T] \ge \mathbb{E}_1[\mathcal{T}^*(m - 2c)] = \frac{|\log \alpha|}{(m - 2c) D_1} + O(1), \tag{29}$$

where $\mathcal{F} \triangleq \{f | e_0 \le \alpha, e_1 \le \beta\}$.

Proof Under attack g^*, the compromised sensor set is $\mathcal{C} = \mathcal{O}_\theta$ given hypothesis H_θ. In this case, for either $\theta = 0$ or $\theta = 1$, sensors in $\mathcal{O}_0$ will follow distribution ν_0 and sensors in $\mathcal{O}_1$ will follow distribution ν_1. In other words, only sensors in $\mathcal{S} \setminus (\mathcal{O}_0 \cup \mathcal{O}_1)$ have different distributions under different hypotheses, and sensors in $\mathcal{O}_0 \cup \mathcal{O}_1$ provide no information for distinguishing the hypotheses. As we assume $m > 2c$, $\mathcal{S} \setminus (\mathcal{O}_0 \cup \mathcal{O}_1) \neq \varnothing$. Therefore,

$$\mathbb{E}_\theta^{g^*}[T]\Big|_{\mathcal{S}} = \mathbb{E}_\theta[T]|_{\mathcal{S}\setminus(\mathcal{O}_0\cup\mathcal{O}_1)},$$

where the expectation $\mathbb{E}_\theta^g[T]|_{\mathcal{S}}$ restricted on a set $\mathcal{S}$ means the detection scheme only takes observations in set $\mathcal{S}$. Since $|\mathcal{S} \setminus (\mathcal{O}_0 \cup \mathcal{O}_1)| = m - 2c$, according to Proposition 1, the results are obtained. □

Theorem 2 provides a performance fundamental limit in presence of Byzantine attack. No detection strategy can have strictly lower expected sample number than $\mathbb{E}_\theta[\mathcal{T}^*(m-2c)]$ in presence of flip-attack. In the following subsection, we quantify the performance of VSPRT in presence of attack and prove that VSPRT achieves the performance bound in Theorem 2.

C. Achievability

In the presence of attack, the VSPRT scheme uses manipulated observations to calculate log-likelihood ratios:

$$l_i(k) = \log\left(\frac{\mathrm{d}\nu_1(y_i(k))}{\mathrm{d}\nu_0(y_i(k))}\right).$$

The thresholds chosen according to probability constraints are:

$$h_1 = \frac{-\log\alpha + \log\binom{m}{r-c}}{r-c},\ h_0 = \frac{-\log\beta + \log\binom{m}{r-c}}{r-c}. \quad (30)$$

The remaining procedures are all the same as Subsection III-A. The following theorem quantifies the performance of VSPRT in the presence of attack, and the proof is provided in Appendix C for legibility.

Theorem 3 For any admissible attack strategy g on arbitrary sensor set $\mathcal{C}$ with $|\mathcal{C}| = c$. The following results hold for $m/2 < r \leq m - c$ as $\alpha, \beta \to 0$:

$$t_{0,\gamma}^g\left(\tau^-(r)\right) \leq \frac{|\log\beta|}{(r-c)D_0} + \sqrt{\frac{V_0|\log\beta|}{(r-c)D_0^3}}\ \Phi^{-1}(\gamma^{\frac{1}{m}}) + o\left(\sqrt{|\log\beta|}\right). \quad (31)$$

$$t_{1,\gamma}^g\left(\tau^+(r)\right) \leq \frac{|\log\alpha|}{(r-c)D_1} + \sqrt{\frac{V_1|\log\alpha|}{(r-c)D_1^3}}\ \Phi^{-1}(\gamma^{\frac{1}{m}}) + o\left(\sqrt{|\log\alpha|}\right). \quad (32)$$

According to Theorem 3, increasing r ($r \leq m-c$) will decrease the delay. By choosing $r = m-c$, the fundamental limits in Theorem 2 are achieved. We cast the detection problem as a zero-sum game between detecting strategy f and attack strategy g with pay-off of f defined as[5] either ρ_0 or ρ_1:

$$\rho_0(f,g) \triangleq \lim_{\alpha,\beta\to 0} \frac{|\log\beta|}{\mathbb{E}_0^g[T]},\ \rho_1(f,g) \triangleq \lim_{\alpha,\beta\to 0} \frac{|\log\alpha|}{\mathbb{E}_1^g[T]}. \quad (33)$$

Since the detection strategy pursues smaller error probability α (or β) with lower expected delay $\mathbb{E}_\theta^g[T]$, larger $\rho_\theta(f,g)$ ($\theta = 0,1$) represents better performance. The detection strategy f aims at increasing ρ_θ, and the malicious attacker g intends to decrease ρ_θ. Based on Theorem 3, we have the following performance bound of VSPRT scheme $f(r)$.

Corollary 2 Under any admissible attack strategy g, if $r \leq m-c$, for arbitrary admissible attack g, we have

$$\rho_\theta(f(r),g) \geq (r-c)\cdot D_\theta,\ \theta = 0,1. \quad (34)$$

Corollary 2 indicates that, when the number c of compromised sensors is unknown, as long as we choose r such that $r \leq m-c$, the system performance has a lower bound. Moreover, if we know the number c, the following Nash equilibrium is obtained.

Corollary 3 VSPRT detection strategy $f^* \triangleq f(m-c)$ and flip-attack strategy g^* form a Nash equilibrium pair, i.e., for any admissible strategy f and g, the following holds:

$$\rho_\theta(f,g^*) \leq \rho_\theta(f^*,g^*) \leq \rho_\theta(f^*,g), \quad (35)$$

where

$$\rho_\theta(f^*,g^*) = (m-2c)\cdot D_\theta,\ \theta = 0,1. \quad (36)$$

Proof (proof of Corollaries 2 and 3) We consider the case where $\theta = 1$. It can be proved similarly when $\theta = 0$. According to Theorem 3, one obtains

$$\mathbb{E}_1^g[\tau(r)] \leq \frac{|\log\alpha|}{(r-c)D_1} + O\left(\sqrt{|\log\alpha|}\right).$$

Thus,

$$\rho_1(f(r),g) = \lim_{\alpha,\beta\to 0} \frac{|\log\alpha|}{\mathbb{E}_1^g[\tau(r)]} \geq (r-c)D_1, \quad (37)$$

and Corollary 2 is obtained. According to Theorem 2, one obtains

$$\rho_1(f,g^*) = \lim_{\alpha,\beta\to 0} \frac{|\log\alpha|}{\mathbb{E}_1^{g^*}[T]} \leq (m-2c)D_1. \quad (38)$$

Enforcing $r = m-c$ in (37), and combing it with (38) lead to

$$\rho_1(f,g^*) \leq (m-2c)D_1 \leq \rho_1(f^*,g).$$

Plugging in $f = f^*$ and $g = g^*$ in (37) and (38) results in $(m-2c)D_1 \leq \rho_1(f^*,g^*) \leq (m-2c)D_1$. The proof of Corollary 3 is thus accomplished. □

Since neither the attacker's policy set nor the detector's policy set is compact, the Nash equilibrium pair does not necessarily exist. Corollary 3 is of significance because it proves its existence. If we define the worst performance among all possible attacks as $\tilde{\rho}_\theta(f) = \inf_g \rho_\theta(f,g)$, inequalities in Theorem 2 imply $\forall f$, $\tilde{\rho}_\theta(f) \leq (m-2c)D_\theta$. Combining it with the second inequality in (35) leads to $\tilde{\rho}_\theta(f^*) = (m-2c)D_\theta$, i.e., the VSPRT scheme f^* achieves the performance upper

[5] Pay-off of g is defined as $-\rho_0$ or $-\rho_1$ accordingly.

bound and is optimal among all possible f. Notice that the optimality is defined against all admissible attacks. We introduce flip-attack because it is one of the attack strategies that achieve the performance bound.

Remark 5 Noticing that flip-attack only requires observations in $\mathcal{O}_0$ (when $\theta = 0$) or $\mathcal{O}_1$ (when $\theta = 0$), the flip-attacker belongs to the category of weak attacker (recalling definition in Assumption 4) since it does not need to know observations from honest sensors in $\mathcal{S} \setminus (\mathcal{O}_0 \cup \mathcal{O}_1)$. In other words, the information of a weak attacker is sufficient to support the attack that causes the worst performance, and knowing more observations from honest sensors cannot enable the strong attacker to incur further performance loss.

In the next section, we generalize VSPRT in fully-distributed scenario and prove that the optimality and the resiliency are preserved.

V. Fully Distributed Voting Scheme

In many real-world scenarios, sensor network performs a peer-to-peer local information exchange and there does not exist a fusion center. We model the network topology as a digraph where the directed edges represent communication channels. We propose a fully-distributed detection scheme in this network where every sensor makes decision based on local observations and information shared from its neighbors. It is named as *distributed voting SPRT* (DVSPRT), and we prove that this scheme has the same asymptotic performance as VSPRT both in the presence and in the absence of attack.

We assume the model of the sensor network is a directed graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, where $\mathcal{V}$ is the set of nodes (sensors) with $|\mathcal{V}| = m$. Edge set $\mathcal{E}$ is the set of links or communication channels among sensors: $(i, j) \in \mathcal{E}$ represents that sensor i can send information to j. Define the number of communication links as $M \triangleq |\mathcal{E}|$. The (incoming) neighborhood set $\mathcal{N}_j$ of sensor j is defined as all the sensors that can send messages to j, i.e. $\mathcal{N}_j \triangleq \{i | (i, j) \in \mathcal{E}\}$. Denote $(A)_{ij}$ as the element at i-th row j-th column of matrix A. Define adjacency matrix of sensor network as A, with $(A)_{ij} = 1$ if $(i, j) \in \mathcal{E}$ and $(A)_{ij} = 0$ otherwise. The distance from vertex i to j $(i \neq j)$ is the shortest length of path that starts from i and ends in j:

$$\mathrm{dis}(i, j) \triangleq \min_{n \in \mathbb{Z}^+} \{n | (A^n)_{ij} = 1\}.$$

Let $\mathrm{dis}(i, i) = 0$ for each $i \in \mathcal{V}$. If $(A^n)_{ij} = 0$ for all positive integer n, i.e., there does not exist a path from i to j, the distance is defined as $\mathrm{dis}(i, j) = \infty$. Define the diameter of a digraph $\mathcal{G}$ as

$$\mathrm{dia}\,\mathcal{G} \triangleq \max_{i, j \in \mathcal{V}} \mathrm{dis}(i, j).$$

We say that $\mathcal{G}$ is strongly connected if $\mathrm{dia}\,\mathcal{G} < \infty$.

A. Distributed Voting SPRT

Distributed voting SPRT (DVSPRT) is based on single sensor SPRT and distributed votes propagation. The single sensor SPRT is the same as in VSPRT scheme and we concentrate on the voting propagation process. In fully-distributed scenario, every sensor maintains a transcript of vote list that records the source and type of the vote currently known. Define the set of vote list known at time k by sensor i as $\Delta_i(k) \subseteq \{-m, -m+1, \cdots, -1, 1, 2, \cdots, m\}$, which is initialized as empty set, i.e., $\Delta_i(0) := \varnothing$. Recalling the definition of stopping times τ_i^+ and τ_i^- in (9) and (10), the vote list is updated at time k as:

$$\Delta_i(k) = \begin{cases} \Delta_i(k-1) \bigcup \left\{ \bigcup_{j \in \mathcal{N}_i} \Delta_j(k-1) \right\} \bigcup \{+i\}, \ k = \tau_i^+, \\ \Delta_i(k-1) \bigcup \left\{ \bigcup_{j \in \mathcal{N}_i} \Delta_j(k-1) \right\} \bigcup \{-i\}, \ k = \tau_i^-, \\ \Delta_i(k-1) \bigcup \left\{ \bigcup_{j \in \mathcal{N}_i} \Delta_j(k-1) \right\}, \ \text{otherwise}. \end{cases} \tag{39}$$

Define the time that sensor i collects at least r positive (negative) votes as

$$T_i^+(r) \triangleq \inf_{k \in \mathbb{Z}^+} \left\{ k : \left| \Delta_i(k) \cap \mathbb{Z}^+ \right| \geq r \right\}, \tag{40}$$

$$T_i^-(r) \triangleq \inf_{k \in \mathbb{Z}^+} \left\{ k : \left| \Delta_i(k) \cap \mathbb{Z}^- \right| \geq r \right\}, \tag{41}$$

where $\mathbb{Z}^+$ ($\mathbb{Z}^-$) is the set of strictly positive (strictly negative) integers. The final decision at sensor i is made once there are r votes supporting the same hypothesis in set $\Delta_i(k)$:

$$f_{i,k}(r) = \begin{cases} 0, & k = T_i^-(r) \leq T_i^+(r) \\ 1, & k = T_i^+(r) < T_i^-(r) \\ \text{continue}, & k < \min\{T_i^+(r), T_i^-(r)\} \end{cases}. \tag{42}$$

The DVSPRT scheme based on local information at sensor i is defined as $f_i(r) \triangleq \left\{ f_{i,k}(r) \right\}_{k=1}^{\infty}$. The stopping time of $f_i(r)$ is

$$T_i(r) \triangleq \min\{T_i^+(r), T_i^-(r)\}. \tag{43}$$

The DVSPRT algorithm at sensor i is presented in Algorithm 1.

Algorithm 1 DVSPRT at sensor i

```
Initialize $\Delta_i(0) := \varnothing$, $f_{i,0}(r) = $ continue, $k := 0$.
while $f_{i,k}(r) = $ continue do
    Calculate $S_i(k)$ according to (7).
    Update local vote set $\Delta_i(k)$ according to (39).
    Make decision according to (42).
    $k := k + 1$.
end while
```

The vote list Δ_i is changed only when sensor i itself reports a vote (at time τ_i^+, τ_i^-) or its neighbors' sets are changed. Therefore, the updating equation (39) can be designed as event-based, i.e., update the set Δ_i only when $k = \tau_i^+$ or $k = \tau_i^-$ or when its neighbors' sets Δ_j $(j \in \mathcal{N}_i)$ are updated at last time step. By this design, the number of messages that travel in the network is no larger than $2m \cdot M$ (every link at most transmits $2m$ votes). Define the message complexity as the amount of messages traveling through graph edges. The message complexity of DVSPRT is $O(mM)$, which is independent of α, β, h_0, h_1 and expected delay $\mathbb{E}_\theta[T]$. This merit attributes to the sparsity of the votes. In comparison, message complexity of most of consensus-based algorithms (e.g. [12] [15]) scales linearly with respect to detection time, i.e., the message complexity is $O(mMT)$. As error probabilities α and β approach zero, the message number of these algorithms goes to infinity while the message number of our proposed scheme is bounded.

B. Performance analysis

DVSPRT differs from VSPRT in that the vote-counting procedure of DVSPRT is carried out in a decentralized manner. In the following, we first focus on the delay caused by distributed vote counting and prove that the delay is bounded by the diameter of the network topology graph.

Lemma 1 For arbitrary r satisfying $1 \le r \le m$ and arbitrary admissible attack g, the stopping time $T_i(r)$ of DVSPRT and the stopping time $\tau(r)$ of VSPRT satisfy

$$\max_{i \in \mathcal{S}} T_i(r) - \tau(r) \le \mathrm{dia}\,\mathcal{G}. \tag{44}$$

Remark 6 The diameter of the graph is used to bound the maximum time that a vote reaches all the other sensor nodes in $\mathcal{G}$ (also know as *flooding time* in a graph). According to the information transmission protocol defined in (39), the difference between delay of distributed and centralized vote-counting is upper bounded by the maximum flooding time, i.e., $\mathrm{dia}\,\mathcal{G}$.

Proof Define the oracle voting list Δ which includes the votes immediately after it is generated, i.e., at time k the set is

$$\Delta(k) \triangleq \bigcup_{i \in \mathcal{S}} \Delta_i(k). \tag{45}$$

According to the vote transmission mechanism (39), a vote travels one path length every time step and the following holds:

$$\Delta_i(k + \mathrm{dia}\,\mathcal{G}) \supseteq \Delta(k). \tag{46}$$

Therefore, the following holds for arbitrary i, r and H_θ:

$$\begin{aligned} T_i^+(r) &= \inf_{k \in \mathbb{Z}^+} \left\{ k : |\Delta_i(k) \bigcap \mathbb{Z}^+| \ge r \right\} \\ &\le \inf_{k \in \mathbb{Z}^+} \left\{ k : |\Delta(k) \bigcap \mathbb{Z}^+| \ge r \right\} + \mathrm{dia}\,\mathcal{G} = \tau^+(r) + \mathrm{dia}\,\mathcal{G}. \end{aligned}$$

Similarly, one obtains $T_i^-(r) \le \tau^-(r) + \mathrm{dia}\,\mathcal{G}$. Combining the results leads to

$$\min\{T_i^+(r), T_i^-(r)\} \le \min\{\tau^+(r), \tau^-(r)\} + \mathrm{dia}\,\mathcal{G},\ \forall i \in \mathcal{S}.$$

Recalling the definition of $T_i(r)$ and $\tau(r)$ in (43) and (15), (44) holds for arbitrary i, r and arbitrary hypothesis H_θ. □

Based on Lemma 1, one obtains the following upper bound.

Theorem 4 For arbitrary sensor i and r satisfying $m/2 < r \le m$, in the presence of any admissible attack g on any set $\mathcal{C}$ with $0 \le |\mathcal{C}| < m/2$, the stopping times of DVSPRT and VSPRT with the same error probability constraints α, β satisfy

$$t^{g,\mathcal{C}}_{1,\gamma}\left(T_i^+(r)\right) \le t^{g,\mathcal{C}}_{1,\gamma}\left(\tau^+(r)\right) + \mathrm{dia}\,\mathcal{G}, \tag{47}$$

$$t^{g,\mathcal{C}}_{0,\gamma}\left(T_i^-(r)\right) \le t^{g,\mathcal{C}}_{0,\gamma}\left(\tau^-(r)\right) + \mathrm{dia}\,\mathcal{G}. \tag{48}$$

Remark 7 The result includes the case of $|\mathcal{C}| = 0$, i.e., there is no attack.

As shown in Theorem 4, DVSPRT inherits the performance of VSPRT in the absence of attack (Corollary 1) and in the presence of attack (Corollary 3), which is summarized in the following corollary. The corresponding proof is in Appendix D.

Corollary 4 Assume $\mathcal{G}$ is strongly connected. Let $m/2 < r \le m$, for abtrary $i \in \mathcal{S}$, in the absence of attack, the expected delays of DVSPRT satisfy:

$$\mathbb{E}_0[T_i(r)] \le \frac{|\log \beta|}{rD_0} + O\left(\sqrt{|\log \beta|}\right), \tag{49}$$

$$\mathbb{E}_1[T_i(r)] \le \frac{|\log \alpha|}{rD_1} + O\left(\sqrt{|\log \alpha|}\right). \tag{50}$$

Therefore, DVSPRT is of order-1 optimal in the absence of attack. For any admissible attack strategy g, the expected delays of DVSPRT satisfy:

$$\mathbb{E}_0^g[T_i(r)] \le \frac{|\log \beta|}{(r-c)D_0} + O\left(\sqrt{|\log \beta|}\right), \tag{51}$$

$$\mathbb{E}_1^g[T_i(r)] \le \frac{|\log \alpha|}{(r-c)D_1} + O\left(\sqrt{|\log \alpha|}\right), \tag{52}$$

where c is the number of compromised sensors.

DVSPRT has the same asymptotic performance as VSPRT in both scenarios (with and without attack). On the one hand, DVSPRT is order-1 optimal in the absence of attack. This implies generalizing our proposed scheme to fully-distributed scenario does not pay extra price (asymptotically). On the other hand, in the presence of attack, DVSPRT inherits the performance in Corollaries 2 and 3. In other words, DVSPRT forms a Nash equilibrium with flip-attack strategy g^*, and achieves the performance bound in Theorem 2 among all possible detection strategies.

The optimality in absence of attack is significant for the study of full-distributed detection schemes. Notice that other detection schemes in fully-distributed scenario may not necessarily be order-1 optimal, e.g., the *consensus-innovation SPRT* (CISPRT) proposed in [28]. According to [29], CISPRT is order-1 optimal if and only if the topology graph $\mathcal{G}$ is fully-connected, i.e., each sensor can directly send messages to all other sensors. In contrast, our proposed DVSPRT is order-1 optimal as long as $\mathcal{G}$ is connected, which is much weaker than the fully-connectivity.

We list the stopping time notations in Table I for reference. Notation τ is used in single sensor and fusion center context while T is used in fully-distributed context.

TABLE I
TABLE OF STOPPING TIME NOTATIONS

Notation	Meaning of the stopping time	Definition at
$\tau_i^+(h_1)$ or τ_i^+	sensor i votes for H_1	(9)
$\tau_i^-(h_0)$ or τ_i^-	sensor i votes for H_0	(10)
$\tau^+(r)$	r sensors votes for H_1	(12)
$\tau^-(r)$	r sensors votes for H_0	(13)
$\tau(r)$	fusion center get r votes: $\min\{\tau^+(r), \tau^-(r)\}$	(15)
$T_i^+(r)$	sensor i collect r votes for H_1	(40)
$T_i^-(r)$	sensor i collect r votes for H_0	(41)
$T_i(r)$	sensor i collect r votes: $\min\{T_i^+(r), T_i^-(r)\}$	(43)

C. Resiliency under Communication Manipulation and Link Failure

In the previous sections, we consider the scenario where the attacker only manipulates the observations. However, the influence of communication manipulation and link failure is also significant in applying a fully-distributed algorithm and discussed in this subsection. We first provide the solution to communication manipulation. Suppose that the attacker can manipulate the vote list $\Delta_i(k)$ at each compromised senor $i \in \mathcal{C}$. In this case, besides voting for wrong hypothesis, the corrupted sensor can also cast fake votes by impersonating honest sensors. In the presence of such an attacker, every sensor needs to validate whether votes in neighbors' vote list are real ones collected from honest sensors' local votes or impostor ones from the attacker. The problem can be solved by implementing *digital signature*[6] on each vote, i.e., every vote is signed by the sensor who casts it, and every sensor is able to authenticate the signature. In this case, we have the following corollary whose proof is in Appendix E.

Corollary 5 Suppose that besides observation manipulation, the malicious adversary can also manipulate the vote list Δ_i. In presence of such attack g on arbitrary set $\mathcal{C}$ with $|\mathcal{C}| = c$, if $\mathcal{G}$ is $(c+1)$-vertex connected[7], the asymptotic performance of DVSPRT with digital signature is given by (51) and (52) for arbitrary honest sensor $i \in \mathcal{S} \setminus \mathcal{C}$.

According to Corollrary 5, by filtering out fake votes using digital signature, the honest sensors can achieve performance bound $(r-c)D_\theta$ based on (51) and (52).

Remark 8 In Lamport's early study of Byzantine generals [30], he analyzed different solutions under Byzantine agents with oral messages and written (signed) messages. An oral message is a piece of information whose contents are completely under the control of the transponder. A written message is a piece of information whose authenticity could be verified by others, and the intermediary can not manipulate the information. In Subsection V-A, sharing integers from $\Delta_i(k)$ with neighbors can be interpreted as passing oral messages, and the signed votes in this subsection are written messages.

Besides the case where communication is under the manipulation of a malicious adversary, sensor communications also fail randomly because of noise, congestion, and internal errors. We consider the problem where communication channels fail at random times. It is conventional to model the graph with Bernoulli random topology, e.g., [10] [31].

In the random topology model, the communication channel $(i, j) \in \mathcal{E}$ fail at random times. The probability that edge (i, j) is online at arbitrary time k is p_{ij} $(0 \le p_{ij} \le 1)$. We assume that for distinct pairs of edges, the corresponding Bernoulli process is statistically independent. Let us collect the probabilities as a matrix P with its entry on i-th row, j-th column equals to p_{ij} when $(i, j) \in \mathcal{E}$ and equals to 0 when $(i, j) \notin \mathcal{E}$. Define the probability measure with respect to such a Bernoulli random topology under true hypothesis θ as $\mathbb{P}_\theta^P$. Corrsponding expectation is denoted as $\mathbb{E}_\theta^P$. Define a graph $\overline{\mathcal{G}} = (\mathcal{V}, \overline{\mathcal{E}})$ with edge set $\overline{\mathcal{E}}$ defined as the set of all edges with positive link probability: $\overline{\mathcal{E}} \triangleq \{(i, j) \in \mathcal{E} | p_{ij} > 0\}$. We have the following assumption on $\overline{\mathcal{G}}$.

Assumption 5 $\overline{\mathcal{G}}$ is strongly connected.

In order to quantify the delay caused by random link failure, we define the weighted distance in the graph following [32]. Define a directed path $\mathrm{w}(i, j)$ from sensor node i to j as an alternating sequence of vertices and edges:

$$\mathrm{w}(i, j) = \{i = v_0, e_1, v_1, \cdots, e_n, v_n = j\},$$

such that for $l = 1, \ldots, n$, the vertices v_{l-1} and v_l are the endpoints of edge e_l, i.e., $e_l = (v_{l-1}, v_l)$. Define the set of all the paths from i to j in $\overline{\mathcal{G}}$ as $\mathcal{W}(i, j)$. The weighted distance between distinct sensor nodes i_0 and j_0 is defined as

$$\mathrm{dis}^P(i_0, j_0) = \min_{\mathrm{w}(i_0,j_0) \in \mathcal{W}(i_0,j_0)} \sum_{(i,j) \in \mathrm{w}(i_0,j_0)} \frac{1}{p_{ij}}. \tag{53}$$

According to Assumption 5, for every pair of nodes i and j in graph $\overline{\mathcal{G}}$, $\mathrm{dis}^P(i, j) < \infty$. In this random topology network, the expected detection delay of DVSPRT is quantified in the following theorem.

Theorem 5 Given P satisfying Assumption 5, under same error probability constraints α, β, the difference of expected delay of DVSPRT in perfect network and in random failure network parameterized by P is bounded, i.e., for all sensor i, all possible r and hypothesis θ, we have

$$0 \le \mathbb{E}_\theta^P[T_i(r)] - \mathbb{E}_\theta[T_i(r)] \le \max_{j \in \mathcal{V}} \mathrm{dis}^P(j, i). \tag{54}$$

Theorem 5 indicates that for each decider sensor i, the expected delay introduced by random topology failure is bounded by a constant term $\max_{i,j \in \mathcal{V}} \mathrm{dis}^P(j, i)$. Combining (54) with (49) and (50), one obtains

$$\lim_{\alpha,\beta \to 0} \frac{\mathbb{E}_\theta^P[T_i(m)]}{\mathbb{E}_\theta[\mathcal{T}^*(m)]} = 1, \ \theta = 0, 1, \tag{55}$$

i.e., DVSPRT is still order-1 optimal when the communication channels fail at random times as long as Assumption 5 is satisfied. In comparison, the efficiency of consensus algorithms relies on link probability P [10] [33], and their efficiency (convergence rate) in random graph is strictly less than the efficiency with perfect communication for certain class of P even when $\overline{\mathcal{G}}$ is strongly connected. Considering that the connectivity of $\overline{\mathcal{G}}$ is a very weak assumption, DVSPRT has resiliency advantage over consensus-based algorithms under random link failure by taking advantage of the low-communication design of the voting scheme.

VI. Simulation

In this subsection, we assume that the probability distribution of two hypotheses are Gaussian distributions. The background distribution of null hypothesis and alternative hypothesis are $H_0 : N(-1, 1)$ and $H_1 : N(1, 1)$. In this case,

[6] A digital signature is a mathematical scheme for verifying the authenticity of digital messages or documents. Some examples of the digital signature algorithm are RSA, DSA, and ECDSA.

[7] Strongly connected digraph $\mathcal{G}$ is said to be κ-vertex connected if any removal of $\kappa - 1$ vertices leaves a strongly connected digraph.

the K–L divergences are $D_0 = D_1 = 2$, and variances are $V_0 = V_1 = 4$.

We first evaluate the performance of VSPRT in the absence of attack, i.e., validate Theorem 1 and Corollary 1 by simulation. In Fig. 3, we choose four different m ($m = 2, 4, 10, 20$) with thresholds $h_0 = h_1 = 10000$. The empirical distribution function of normalized stopping time $\left(\tau^-(m) - \frac{h_0}{D_0}\right) / \sqrt{\frac{V_0}{D_0^3} \cdot h_0}$ with 100 samples for each value of m is illustrated in Fig. 3. The dashed lines are the corresponding theoretical cumulative distribution function $[\Phi(\cdot)]^m$. Fig. 3 shows that the empirical distribution corresponds to the theoretical distribution $[\Phi(\cdot)]^m$.

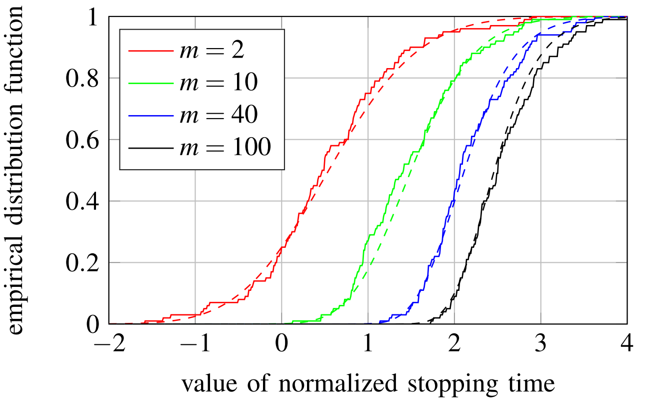

Fig. 3. CDF of random stopping time of VSPRT with $r = m$.

In order to simulate the error probability with higher accuracy, the simulation experiments in the following adopt the importance sampling approach [34]. To validate the result in Corollary 1, the simulation is performed with $m = 10$ sensors and $h_0 = h_1$. The values of the thresholds are chosen in an increasing value list ranging from 50 to 1000. We calculate the expected delay $\mathbb{E}_0[\tau(r)]$, the error probability e_1 and the corresponding constraint β. The result is shown in Fig. 4.

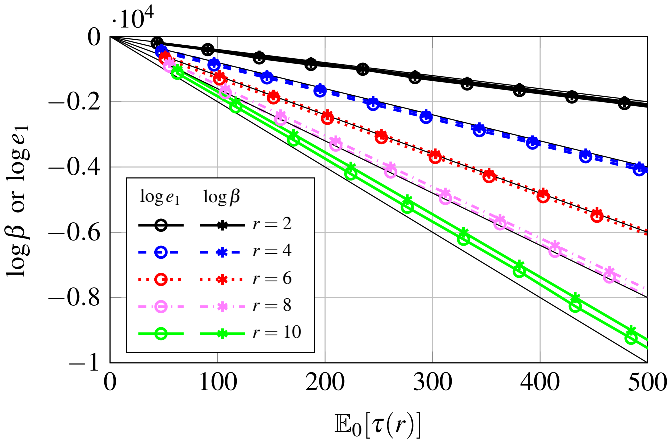

Fig. 4. Performance of VSPRT with $m = 10$ sensors and different r in the absence of attack.

As shown in Fig. 4, the absolute value of slope of every line is approximately $2r$ (as denoted by black thin solid line), which is in accordance with our asymptotic result $\frac{|\log\beta|}{\mathbb{E}_0[\tau(r)]} \sim rD$ as $\alpha, \beta \to 0$. The probability constraint $e_1 \leq \beta$ is satisfied (asterisk mark is above the circle mark for every line). Moreover, the gap between e_1 and β is reasonably small, which corresponds to the theory. The topology graph in fully-distributed scenario simulation (Fig. 6 and Fig. 8) is denoted in Fig. 5.

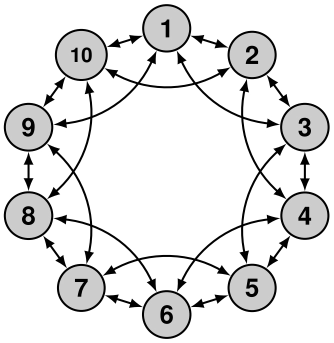

Fig. 5. Topology Graph of sensor network used for simulation in fully-distributed case.

In the presence of attack, we validate Corollary 3 by showing VSPRT and DVSPRT achieves the performance bound under attack. In Fig. 6, we choose $m = 10$ and $r = m - c$. As topology graph in Fig. 5 is a 4-connected graph, we choose $c = 0, 1, 2, 3$ in the simulation to prevent system degradation. The compromised sensor sets are $\mathcal{C} = \{1\}, \mathcal{C} = \{1, 2\}$, and $\mathcal{C} = \{1, 2, 10\}$ respectively. We use the local information at sensor 1 for final decision. As shown in Fig. 6, the absolute value of slope of every line is close to $2(m - 2c)$ (as denoted as black thin line), which validates Corollary 3.

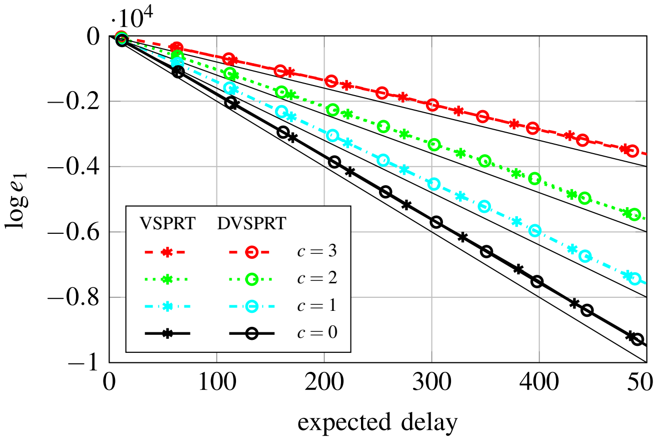

Fig. 6. Performance of equilibrium strategy pair (f^*, g^*) when $m = 10$, $r = m - c$ with different c. The expected delay is $\mathbb{E}_0^{g^*}[\tau(m-c)]$ for VSPRT and is $\mathbb{E}_0^{g^*}[T_1(m-c)]$ for DVSPRT.

In order to evaluate the efficiency of our proposed detection scheme, we compare it with several detection schemes in literature in the absence of attack. The following algorithms are simulated with 10 sensors, and the fully-distributed algorithms in Fig. 8 adopt the network topology in Fig. 5. The parameter r in our proposed VSPRT and DVSPRT is chosen as $r = 10$. Fig. 7 compares our proposed VSPRT with other schemes in fusion center formulation. The simulation includes the *Decentralized SPRT* (D-SPRT) proposed in [20] [35], *Dual-SPRT* and *SPRT-CSPRT* proposed in [21]. Moreover, the order-2 optimal *Centralized SPRT* (CSPRT, see e.g., [23] [36]) is also evaluated as a benchmark of optimality, which is conventional in literature (e.g., [21] [23]). In Fig. 7, the slope of every line represents the decrease rate of logarithm error probability with respect to expected delay, i.e., the efficiency of the corresponding algorithm. The maximum magnitude of the slope equals to $mD_1 = 20$, which corresponds to that of the black thin line (theoretical optimal). The displayed schemes are all at least order-1 optimal. The decrease rates (slopes) are almost the same, which means VSPRT has almost the same finite time efficiency as other schemes in absence of attacks.

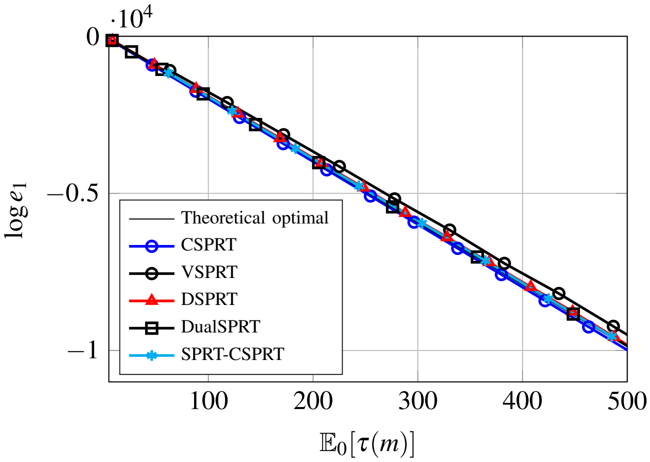

Fig. 7. Performance of distributed detection schemes with fusion center where $m = 10$.

Fig. 8 compares our proposed DVSPRT with other schemes in fully-distributed formulation. The simulation covers *sample-dissemination-based distributed SPRT* (SD-DSPRT) and *consensus-algorithm-based distributed SPRT* (CA-DSPRT) proposed in [23]. We also simulate our DVSPRT scheme with random link failure. In the random topology simulation, the link probability p_{ij} of every directed edge in the graph is generated randomly from the uniform distribution on open interval $(0,1)$. As shown in Fig. 8, the slope of DVSPRT is close to that of other schemes and the theoretical optimal. Thus, the finite time performance of DVSPRT in the absence of attack is validated. Moreover, the performance of DVSPRT with random link failure is asymptotically the same as DVSPRT with perfect communication.

VII. Conclusion and Future Work

This paper studies the sequential binary hypothesis testing problem with Byzantine agents in both fusion center and fully-distributed formulations. The performance metric is formulated as the detection delay with type-I, type-II error probability constraints. We investigate the asymptotic performance as error probabilities approach zero. In the absence of attack, the definition of optimality and the theoretical optimal of a detection strategy are introduced in Section II. We formulate the VSPRT scheme in the fusion center formulation and the DVSPRT scheme in the fully-distributed formulation based on single sensor SPRT and a decide-by-vote mechanism.

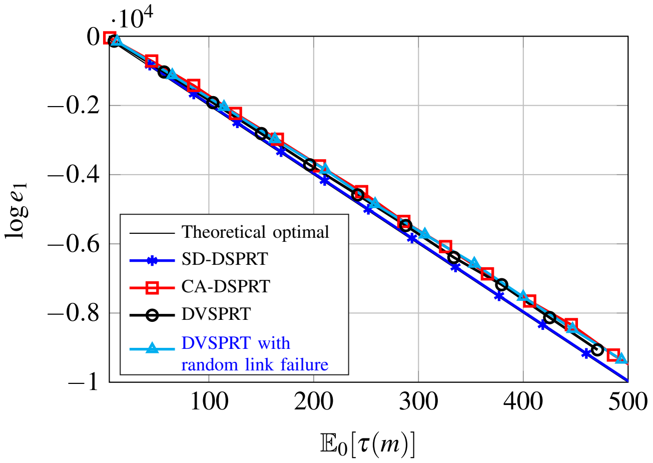

Fig. 8. Performance of fully-distributed detection schemes with $m = 10$ sensors and network topology $\mathcal{G}$ in Fig. 5.

We prove that our proposed detection schemes VSPRT and DVSPRT are order-1 optimal with voting parameter $r = m$ in the absence of attack. Moreover, in the presence of Byzantine attacks, they both achieve the performance bound considering the worst-case performance, and each of them forms a Nash equilibrium pair with the flip-attack when choosing $r = m - c$. The fact that the DVSPRT scheme inherits the performance of VSPRT indicates that there is "no price of decentralization" of our fully-distributed algorithm. Moreover, we prove that DVSPRT still holds order-1 optimality under random link failure with a mild assumption. The main results are verified by numerical simulations.

Even though our proposed schemes can achieve the performance bound in the presence of attack by choosing $r = m - c$, this parameter choice does not lead to the most efficient algorithm when there is no attack. Therefore, it can be the object of future work to design a detection scheme that can achieve optimality simultaneously in both scenarios (with and without attack).

Appendix A
Central Limit Theorem of First Passage Time

Assume that $\{x(n)\}_{n\geq 1}$ is a sequence of i.i.d. random variables with probability measure $\mathbb{P}_x(\cdot)$ and expectation $\mathbb{E}_x(\cdot)$. The expectation and variance of $x(1)$ are denoted as

$$\mu_x \triangleq \mathbb{E}_x[x(1)],\ V_x \triangleq \mathbb{E}_x[(x(1)-\mu_x)^2]. \tag{56}$$

Partial sum of $x(n)$ is defined as $W(n) \triangleq \sum_{k=1}^{n} x(k)$. Denote the first passage time of a positive threshold h as

$$\tau^+(h) \triangleq \inf\{n \in \mathbb{Z}^+ | W(n) > h\}. \tag{57}$$

The following Central Limit Theorem (CLT) of positive first passage time is from Allan Gut [37] Theorems 5.1, 5.2 and Remarks 5.1, 5.3 in Chapter 2. The symmetrical result of negative first passage time can be easily derived from it.

Lemma 2 (Central Limit Theorem of first passage time) Assume $0 < \mu_x < \infty$ and $V_x < \infty$, then the following holds:

$$\frac{\tau^+(h) - \frac{h}{\mu_x}}{\sqrt{\frac{V_x}{\mu_x^3} \cdot h}} \xrightarrow{d} N(0,1) \text{ as } h \to \infty, \tag{58}$$

where $\xrightarrow{d}$ means convergence in distribution, and $N(0,1)$ is the standard normal distribution.

Appendix B
Proof of Theorem 1 and Corollary 1

Proof (Proof of Theorem 1) We prove (18), and (17) could be handled similarly. Define a normalized random variable

$$Z_1(h_1) = \frac{\tau_1^+(h_1) - \frac{h_1}{D_1}}{\sqrt{\frac{V_1}{D_1^3} \cdot h_1}}.$$

According to Lemma 2, we have $Z_1(h_1) \xrightarrow{d} N(0,1)$ as $h_1 \to \infty$. According to definition in (16), one obtains

$$t_{1,\gamma}\left(\tau^+(r)\right) \triangleq \inf\left\{t \,\middle|\, \mathbb{P}_1(\tau^+(r) \le t) \ge \gamma\right\}.$$

For better readability, we denote $t_{1,\gamma}(\tau^+(r))$ with $t_{1,\gamma}$ for the rest of this subsection. As the probability $\mathbb{P}_1(\tau^+(r) \le t)$ is non-decreasing with respect to t, one obtains

$$\mathbb{P}_1[\tau^+(r) \le t_{1,\gamma}] = \gamma.$$

Event $\{\tau^+(r) \le t_{1,\gamma}\}$ implies that there are r sensors that already sent positive votes at time $t_{1,\gamma}$. Assuming the set of sensors that contribute to these r votes as $\mathcal{R} = \{i_1, i_2, \ldots, i_r\}$, one obtains

$$\gamma = \mathbb{P}_1[\tau^+(r) \le t_{1,\gamma}] = \mathbb{P}_1\left[\max_{i\in\mathcal{R}} \tau_i^+ \le t_{1,\gamma}\right] \ge \left(\mathbb{P}_1[\tau_1^+ \le t_{1,\gamma}]\right)^r.$$

The last inequality reduces to equality when $r = m$. One obtains $\mathbb{P}_1\left[\tau_1^+ \le t_{1,\gamma}\right] \le \gamma^{\frac{1}{r}}$ or

$$\mathbb{P}_1\left[Z_1(h_1) \le \frac{t_{1,\gamma} - \frac{h_1}{D_1}}{\sqrt{\frac{V_1}{D_1^3} \cdot h_1}}\right] \le \gamma^{\frac{1}{r}}.$$

Because $Z_1(h_1) \xrightarrow{d} N(0,1)$, we have

$$\frac{t_{1,\gamma} - \frac{h_1}{D_1}}{\sqrt{\frac{V_1}{D_1^3} \cdot h_1}} \le \Phi^{-1}(\gamma^{\frac{1}{r}}) + o(1) \text{ as } h_1 \to \infty, \tag{59}$$

or equivalently

$$t_{1,\gamma}(\tau^+(r)) \le \frac{h_1}{D_1} + \sqrt{\frac{V_1}{D_1^3} \cdot h_1}\; \Phi^{-1}(\gamma^{\frac{1}{r}}) + o\left(\sqrt{h_1}\right). \tag{60}$$

The inequality in (60) becomes equality when $r = m$.

We proceed to deal with the error probabilities and first prove that the error probability constraints $e_0 \le \alpha$ and $e_1 \le \beta$ are satisfied by choosing thresholds h_0, h_1 as in (8). Let us define the following events for a single sensor i:

$$\mathcal{E}_i^- \triangleq \left\{\inf_{k\in\mathbb{Z}^+} S_i(k) \le -h_0\right\},\ \mathcal{E}_i^+ \triangleq \left\{\sup_{k\in\mathbb{Z}^+} S_i(k) \ge h_1\right\}.$$

Notice that event $\mathcal{E}_i^-$ implies that sensor i reports a wrong vote when the true hypothesis is H_1. Event $\{\tau^-(r) < \tau^+(r)\}$ implies that there exists an index set $\mathcal{R} \triangleq \{i_1, i_2, \ldots, i_r\} \subseteq \mathcal{S}$ such that for every entry i in set $\mathcal{R}$, event $\mathcal{E}_i^-$ occurs. Considering the statistical independence of every cumulative log-likelihood ratio, one obtains

$$\mathbb{P}_1[\tau^-(r) < \tau^+(r)] \le \sum_{|\mathcal{R}|=r} \prod_{i\in\mathcal{R}} \mathbb{P}_1\left(\mathcal{E}_i^-\right) = \binom{m}{r} \prod_{i=1}^{r} \mathbb{P}_1\left(\mathcal{E}_i^-\right).$$

Then the error probability with $\theta = 1$ satisfies

$$e_1 \le \binom{m}{r}\left(\mathbb{P}_1[\mathcal{E}_1^-]\right)^r \le \binom{m}{r}\exp(-rh_0), \tag{61}$$

and the last inequality holds because we have the following characteristics of single sensor SPRT (see e.g. [38]):

$$\mathbb{P}_0[\mathcal{E}_i^+] \le (1 - \mathbb{P}_1[\mathcal{E}_i^-]) \cdot \exp(-h_1) \le \exp(-h_1),$$
$$\mathbb{P}_1[\mathcal{E}_i^-] \le (1 - \mathbb{P}_0[\mathcal{E}_i^+]) \cdot \exp(-h_0) \le \exp(-h_0).$$

Substituting h_0 with $\frac{-\log\beta + \log\binom{m}{r}}{r}$ in (61) leads to $e_1 \le \beta$. Similarly, one can prove $e_0 \le \alpha$. Recalling the choices of h_0, h_1 in (8), one obtains $h_1 \sim \frac{|\log\alpha|}{r}$. Replacing h_1 in (60) with $\frac{|\log\alpha|}{r}$ leads to (18). □

Proof (Proof of Corollary 1) According to Theorem 1, one obtains

$$\frac{t_{1,\gamma}(\tau^+(m)) - \frac{|\log\alpha|}{mD_1}}{\sqrt{\frac{V_1}{mD_1^3} \cdot |\log\alpha|}} = \Phi^{-1}(\gamma^{\frac{1}{r}}) + o(1) \text{ as } \alpha \to 0.$$

This is equivalent to

$$\frac{\tau^+(m) - \frac{|\log\alpha|}{mD_1}}{\sqrt{\frac{V_1}{mD_1^3}|\log\alpha|}} \xrightarrow{d} N^m(0,1).$$

The other one could be proved similarly. We proceed to prove (19), and (20) can be tackled in the same way. It can be verified that the expectation of a random variable with CDF $[\Phi(x)]^m$ $(m > 1)$ is strictly positive, i.e.,

$$\mathbb{E}_1\left[\frac{\tau^+(m) - \frac{|\log\alpha|}{mD_1}}{\sqrt{\frac{V_1}{mD_1^3}|\log\alpha|}}\right] = \frac{\mathbb{E}_1[\tau^+(m)] - \frac{|\log\alpha|}{mD_1}}{\sqrt{\frac{V_1}{mD_1^3}|\log\alpha|}} = C(\alpha) > 0,$$

where $C(\alpha)$ is a constant for each given α. Thus, one obtains

$$\mathbb{E}_1[\tau(m)] \le \mathbb{E}_1[\tau^+(m)] \le \frac{|\log\alpha|}{rD_1} + O\left(\sqrt{|\log\alpha|}\right). \;\square \tag{62}$$

Appendix C
Proof of Theorem 3

Proof We prove (32) and (31) could be dealt with similarly. We claim the following inequalities hold for arbitrary attack g, arbitrary time t and same threshold h_0, h_1:

$$\mathbb{P}_1^g[\tau^+(r-c) \le t] \ge \mathbb{P}_1[\tau^+(r) \le t], \tag{63}$$
$$\mathbb{P}_0^g[\tau^-(r-c) \le t] \ge \mathbb{P}_0[\tau^-(r) \le t], \tag{64}$$
$$\mathbb{P}_1^g[\tau^-(r) \le \tau^+(r)] \le \mathbb{P}_1[\tau^-(r-c) \le \tau^+(r-c)], \tag{65}$$
$$\mathbb{P}_0^g[\tau^+(r) \le \tau^-(r)] \le \mathbb{P}_0[\tau^+(r-c) \le \tau^-(r-c)]. \tag{66}$$

We prove (63) and (65). The other two can be proved in the same way. For any time t, we have that $\{\tau^+(r) \le t\}$ in the absence of attack implies $\{\tau^+(r-c) \le t\}$ under any admissible attack, since the number of manipulated votes is at most c. Therefore, inequality (63) holds. Similarly, for (65), event $\{\tau^-(r) \le \tau^+(r)\}$ under attack implies that at least $r-c$ honest sensors have reported votes for H_1, which is equivalent to the occurrence of event $\{\tau^-(r-c) \le \tau^+(r-c)\}$ in the absence of attack. We proceed to prove (32). Based on (60) and (63), one obtains

$$\begin{aligned} t^g_{1,\gamma}\left(\tau^+(r)\right) &\le t_{1,\gamma}\left(\tau^+(r+c)\right) \\ &\le \frac{h_1}{D_1} + \sqrt{\frac{V_1}{D_1^3}\cdot h_1}\ \Phi^{-1}(\gamma^{\frac{1}{m}}) + o\left(\sqrt{h_1}\right). \quad (67) \end{aligned}$$

We proceed to prove that the probability constraints are satisfied. According to (66), one obtains

$$e^g_0 \le \mathbb{P}_0[\tau^+(r-c) \le \tau^-(r-c)] \le \binom{m}{r-c}\exp(-(r-c)h_1),$$

where the last inequality comes from the symmetric result of (61). Recalling the choice of h_1 in (30), one concludes that the error probability constraint $e^g_0 \le \alpha$ is satisfied. Notice that the choice of h_1 in (30) leads to $\lim_{\alpha,\beta\to 0}\frac{|\log\alpha|}{h_1} \ge r-c$. Therefore, substituting h_1 in (67) with $\frac{|\log\alpha|}{r-c}$ will increase the right-hand-side of (67), i.e.,

$$\begin{aligned} t^g_{1,\gamma}\left(\tau^+(r)\right) \le \frac{|\log\alpha|}{(r-c)D_1} + \sqrt{\frac{V_1|\log\alpha|}{(r-c)D_1^3}}\ \Phi^{-1}(\gamma^{\frac{1}{m}}) \\ + o\left(\sqrt{|\log\alpha|}\right). \ \square \end{aligned}$$

Appendix D
Proof of Corollary 4

Proof According to (60) and Lemma 1, one obtains

$$\mathbb{E}_1[T^+_i(r)] \le \frac{h_1}{rD_1} + O\left(\sqrt{h_1}\right) + \mathrm{dia}\,\mathcal{G}.$$

Recalling the definition in (45), one obtains $\Delta_i(k) \subseteq \Delta(k)$ for arbitrary $i \in \mathcal{S}, k \in \mathbb{Z}^+$. Therefore, if sensor i is the decider sensor, the error probability satisfies

$$\begin{aligned} e_1 &\le \mathbb{P}_1\left(\exists k,\ |\Delta_i(k)\bigcap\mathbb{Z}^-| \ge r\right) \le \mathbb{P}_1\left(\exists k,\ |\Delta(k)\bigcap\mathbb{Z}^-| \ge r\right) \\ &\le \binom{m}{r}\left(\mathbb{P}_1[\mathscr{E}^-_1]\right)^r \le \binom{m}{r}\exp(-rh_0), \end{aligned}$$

which coincides with (61). This means the error probability constraints of DVSPRT is satisfied. Recalling the choices of h_0, h_1 in (8), one obtains $h_1 \sim \frac{|\log\alpha|}{r}$. Replacing h_1 with $\frac{|\log\alpha|}{r}$ leads to $\mathbb{E}_1[T_i(r)] \le \mathbb{E}_1[T^+_i(r)] \le \frac{|\log\alpha|}{rD_1} + O\left(\sqrt{|\log\alpha|}\right)$. Therefore, (50) is proved, and the other one can be obtained in the same way. We proceed to prove (52), and (51) can be dealt with similarly. Based on Theorem 4, by taking maximum among all $|\mathcal{C}| = c$, one obtains

$$\begin{aligned} t^g_{1,\gamma}\left(T^+_i(r)\right) &\le t^g_{1,\gamma}\left(\tau^+(r)\right) + \mathrm{dia}\,\mathcal{G} \\ &\le \frac{|\log\alpha|}{(r-c)D_1} + \sqrt{\frac{V_1|\log\alpha|}{(r-c)D_1^3}}\ \Phi^{-1}(\gamma^{\frac{1}{m}}) + o\left(\sqrt{|\log\alpha|}\right), \end{aligned}$$

where the last inequality comes from (32) in Theorem 3. This leads to

$$\mathbb{E}^g_1[T^+_i(r)] \le \frac{|\log\alpha|}{(r-c)D_1} + O(\sqrt{|\log\alpha|}).$$

Recalling the definition of $T_i(r) \triangleq \min\{T^-_i(r), T^+_i(r)\}$, we have $\mathbb{E}^g_0[T_i(r)] \le \mathbb{E}^g_0[T^-_i(r)]$. Therefore, (52) is proved. $\square$

Appendix E
Proof of Corollary 5

Proof We study the set Δ_i of arbitrary honest decider sensor $i \in \mathcal{S}\setminus\mathcal{C}$. As $\mathcal{G}$ is $(c+1)$-vertex connected, for arbitrary sensor j, there is a path from j to i where all the intermediate vertices are honest sensors. On the one hand, if arbitrary sensor j has cast a vote, the signed vote will reach sensor i and be included in Δ_i with delay bounded by $\mathrm{dia}\,\mathcal{G}$. On the other hand, if j has not cast any vote, with the help of digital signature, vote of j will never be included in Δ_i. Therefore, $\Delta_i(k) \subseteq \Delta(k)$ and $\Delta_i(k+\mathrm{dia}\,\mathcal{G}) \supseteq \Delta(k)$ still hold under communication manipulation. Recalling the proof of Lemma 1, one obtains that the result (44) still holds in this scenario. As a result, Theorem 4 and Corollary 4 still hold, and thus (51) and (52) are obtained. $\square$

Appendix F
Proof of Theorem 5

Proof The lower bound zero is trivial and we concentrate on the upper bound. For a vote at sensor node i_0, the time that it reaches i_1 is

$$\sum_{k=1}^{\infty} k(1-p_{i_0 i_1})^{k-1} p_{i_0 i_1} = \frac{1}{p_{i_0 i_1}},\ 0 < p_{i_0 i_1} \le 1.$$

For an arbitrary $\mathrm{w}(i_0, i_n) = \{i_0, (i_0, i_1), i_1, \cdots, (i_{n-1}, i_n), i_n\}$, considering the statistical independence of the Bernoulli process, the expected time that a vote travel from i_0 to i_n in $\mathrm{w}(i_0, i_n)$ is $\sum_{l=0}^{n-1}(1/p_{i_l i_{l+1}})$. Since i_n will receive a vote cast by i_0 as soon as there is a message passed through any path in $\mathcal{W}(i_0, i_n)$, recalling the definition in (53), the expected voting time lag from i_0 to i_n is less than or equals to $\mathrm{dis}^P(i_0, i_n)$. Therefore, considering all possible votes cast by any $j \in \mathcal{V}$, we have for all r, θ satisfing $1 \le r \le m, \theta = 0, 1$,

$$\mathbb{E}^P_\theta[T^+_i(r)] - \mathbb{E}_\theta[\tau^+(r)] \le \max_{j\in\mathcal{V}} \mathrm{dis}^P(j, i). \quad (68)$$

Since the delay only depends on link probability P and holds for different types of votes, (68) also holds for $T^-_i(r)$ and $\tau^-(r)$. Considering the definition that $\tau(r) = \min\{\tau^-(r), \tau^+(r)\}$ and $T_i(r) = \min\{T^-_i(r), T^+_i(r)\}$, the second inequality in (54) is obtained. $\square$

References

[1] H. Varaee, G. Mirjalily, and A. Pouramini, “An analytical technique to determine the decision thresholds of multi-bit distributed detection in sensor networks,” in *2009 Second International Conference on Computer and Electrical Engineering*, vol. 2, 2009, pp. 32–35.

[2] F. Yu, M. Huang, and H. Tang, “Biologically inspired consensus-based spectrum sensing in mobile Ad Hoc networks with cognitive radios,” *IEEE Network*, vol. 24, no. 3, pp. 26–30, 2010.

[3] A. S. Rawat, P. Anand, H. Chen, and P. K. Varshney, "Collaborative spectrum sensing in the presence of byzantine attacks in cognitive radio networks," *IEEE Transactions on Signal Processing*, vol. 59, no. 2, pp. 774–786, 2011.

[4] A. Vempaty, K. Agrawal, P. Varshney, and H. Chen, "Adaptive learning of byzantines' behavior in cooperative spectrum sensing," in *2011 IEEE Wireless Communications and Networking Conference*, 2011, pp. 1310–1315.

[5] R. Chen, J. . Park, and K. Bian, "Robust distributed spectrum sensing in cognitive radio networks," in *IEEE INFOCOM 2008 - The 27th Conference on Computer Communications*, 2008, pp. 1876–1884.

[6] X. Ren, J. Yan, and Y. Mo, "Binary hypothesis testing with byzantine sensors: Fundamental tradeoff between security and efficiency," *IEEE Transactions on Signal Processing*, vol. 66, no. 6, pp. 1454–1468, March 2018.

[7] A. Vempaty, L. Tong, and P. K. Varshney, "Distributed inference with Byzantine data: State-of-the-art review on data falsification attacks," *IEEE Signal Processing Magazine*, vol. 30, no. 5, pp. 65–75, 2013.

[8] R. Olfati-Saber, E. Franco, E. Frazzoli, and J. Shamma, "Belief consensus and distributed hypothesis testing in sensor networks," *Network Embedded Sensing and Control*, vol. 331, pp. 169–182, 07 2006.

[9] S. Kar and J. M. F. Moura, "Consensus Based Detection in Sensor Networks : Topology Optimization under Practical Constraints," *1st International Workshop on Information Theory in Sensor Networks*, 2007.

[10] S. Kar and J. M. F. Moura, "Sensor networks with random links: Topology design for distributed consensus," *IEEE Transactions on Signal Processing*, vol. 56, no. 7, pp. 3315–3326, 2008.

[11] F. S. Cattivelli and A. H. Sayed, "Distributed detection over adaptive networks using diffusion adaptation," *IEEE Transactions on Signal Processing*, vol. 59, no. 5, pp. 1917–1932, 2011.

[12] D. Jakovetić, J. M. Moura, and J. Xavier, "Distributed detection over noisy networks: Large deviations analysis," *IEEE Transactions on Signal Processing*, vol. 60, no. 8, pp. 4306–4320, 2012.

[13] F. Pasqualetti, A. Bicchi, and F. Bullo, "Consensus computation in unreliable networks: A system theoretic approach," *IEEE Transactions on Automatic Control*, vol. 57, no. 1, pp. 90–104, 2012.

[14] S. Liu, H. Zhu, S. Li, X. Li, and C. Chen, "An adaptive deviation-tolerant secure scheme for distributed cooperative spectrum sensing," 12 2012, pp. 603–608.

[15] B. Kailkhura, S. Brahma, and P. K. Varshney, "Data Falsification Attacks on Consensus-Based Detection Systems," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 3, no. 1, pp. 145–158, 2017.

[16] A. Wald, *Sequential Analysis*. New York: Wiley, 1947.

[17] B. Ghosh and P. Sen, *Handbook of Sequential Analysis*, ser. Statistics: A Series of Textbooks and Monographs. Taylor & Francis, 1991.

[18] A. Wald and J. Wolfowitz, "Optimum character of the sequential probability ratio test," *Annals of Mathematical Statistics*, vol. 19, 11 1947.

[19] Y. Mei, "Asymptotic optimality theory for decentralized sequential hypothesis testing in sensor networks," *IEEE Transactions on Information Theory*, vol. 54, no. 5, pp. 2072–2089, 2008.

[20] G. Fellouris and G. V. Moustakides, "Decentralized sequential hypothesis testing using asynchronous communication," *IEEE Transactions on Information Theory*, vol. 57, no. 1, pp. 534–548, 2011.

[21] K. S. Jithin and V. Sharma, "Novel algorithms for distributed sequential hypothesis testing," *2011 49th Annual Allerton Conference on Communication, Control, and Computing, Allerton 2011*, pp. 1529–1536, 2011.

[22] Z. Li, Y. Mo, and F. Hao, "Game theoretical approach to sequential hypothesis test with byzantine sensors," in *2019 IEEE 58th Conference on Decision and Control (CDC)*, 2019, pp. 2654–2659.

[23] S. Li and X. Wang, "Fully Distributed Sequential Hypothesis Testing: Algorithms and Asymptotic Analyses," *IEEE Transactions on Information Theory*, vol. 64, no. 4, pp. 2742–2758, 2018.

[24] V. V. Veeravalli, "Sequential decision fusion: Theory and applications," *Journal of the Franklin Institute*, vol. 336, no. 2, pp. 301–322, 1999.

[25] A. Wald, "Sequential tests of statistical hypotheses," *The Annals of Mathematical Statistics*, vol. 16, no. 2, pp. 117–186, 1945.

[26] G. Fellouris, E. Bayraktar, and L. Lai, "Efficient byzantine sequential change detection," *IEEE Transactions on Information Theory*, vol. 64, no. 5, pp. 3346–3360, May 2018.

[27] S. Marano, V. Matta, and L. Tong, "Distributed detection in the presence of byzantine attacks," *IEEE Transactions on Signal Processing*, vol. 57, no. 1, pp. 16–29, Jan 2009.

[28] A. K. Sahu and S. Kar, "Distributed sequential detection for gaussian shift-in-mean hypothesis testing," *IEEE Transactions on Signal Processing*, vol. 64, no. 1, pp. 89–103, 2016.

[29] K. Liu and Y. Mei, "Improved performance properties of the cisprt algorithm for distributed sequential detection," *Signal Processing*, vol. 172, p. 107573, 2020. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S016516842030116X

[30] L. Lamport, R. Shostak, and M. Pease, "The Byzantine Generals Problem," *ACM Transactions on Programming Languages and Systems (TOPLAS)*, vol. 4, no. 3, pp. 382–401, 1982.

[31] S. Boyd, A. Ghosh, B. Prabhakar, and D. Shah, "Randomized gossip algorithms," *IEEE Transactions on Information Theory*, vol. 52, no. 6, pp. 2508–2530, June 2006.

[32] H. Amini, M. Draief, and M. Lelarge, "Flooding in weighted sparse random graphs," *SIAM Journal on Discrete Mathematics*, vol. 27, no. 1, pp. 1–26, 2013.

[33] S. S. Pereira and A. Pages-Zamora, "Mean square convergence of consensus algorithms in random wsns," *IEEE Transactions on Signal Processing*, vol. 58, no. 5, pp. 2866–2874, 2010.

[34] R. Y. Rubinstein and D. P. Kroese, *Simulation and the Monte Carlo method*. John Wiley & Sons, 2016.

[35] A. M. Hussain, "Multisensor distributed sequential detection," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 30, no. 3, pp. 698–708, 1994.

[36] A. K. Sahu and S. Kar, "Distributed sequential detection for gaussian shift-in-mean hypothesis testing," *IEEE Transactions on Signal Processing*, vol. 64, no. 1, pp. 89–103, 2016.

[37] A. Gut, *Stopped Random Walks: Limit Theorems and Applications*. Springer, New York, NY, 2009. [Online]. Available: https://link.springer.com/book/10.1007/978-0-387-87835-5

[38] A. Tartakovsky, I. Nikiforov, and M. Basseville, *Sequential Analysis: Hypothesis Testing and Changepoint Detection*, 08 2014.

Zishuo Li (S'19) received the Bachelor of Engineering degree in 2019 from School of Automation Science and Electrical Engineering, Beihang University, Beijing, China. He is now working toward the Ph.D. degree in the Department of Automation, Tsinghua University. His research interests include secure control systems, networked control systems and signal processing with applications in sensor networks and intelligent robots.

Yilin Mo (S'08-M'13) is an Associate Professor in the Department of Automation, Tsinghua University. He received his Ph.D. In Electrical and Computer Engineering from Carnegie Mellon University in 2012 and his Bachelor of Engineering degree from Department of Automation, Tsinghua University in 2007. Prior to his current position, he was a postdoctoral scholar at Carnegie Mellon University in 2013 and California Institute of Technology from 2013 to 2015. He held an assistant professor position in the School of Electrical and Electronic Engineering at Nanyang Technological University from 2015 to 2018. His research interests include secure control systems and networked control systems, with applications in sensor networks and power grids.

Fei Hao received the M.S. degree in mathematics from Inner Mongolia University, Hohhot, China, in 1999, and the Ph.D. degree in dynamics and control from Peking University, Beijing, China, in 2002. From 2002 to 2004, he was a Postdoctoral Researcher with the Center for Systems and Control, Peking University. Since 2004, he has been with the Seventh Research Division, Beihang University, Beijing, where he is currently a Professor. His research interests include robust and optimal control, event-triggered control, hybrid systems, and networked control systems.