2019 IEEE 58th Conference on Decision and Control (CDC)
Palais des Congrès et des Expositions Nice Acropolis
Nice, France, December 11-13, 2019

Game Theoretical Approach to Sequential Hypothesis Test with Byzantine Sensors

Zishuo Li[1], Yilin Mo[2], and Fei Hao[1]

Abstract— **In this paper, we consider the problem of sequential binary hypothesis test in adversary environment based on observations from s sensors, with the caveat that a subset of c sensors is compromised by an adversary, whose observations can be manipulated arbitrarily. We choose the asymptotic Average Sample Number (ASN) required to reach a certain level of error probability as the performance metric of the system. The problem is cast as a game between the detector and the adversary, where the detector aims to optimize the system performance while the adversary tries to deteriorate it. We propose a pair of flip attack strategy and voting hypothesis testing rule and prove that they form an equilibrium strategy pair for the game. We further investigate the performance of our proposed detection scheme with unknown number of compromised sensors and corroborate our result with simulation.**

I. INTRODUCTION

Recent advancements in communication technology and sensing elements have made networked sensor system more readily available in control systems, performing the function of observation, detection and monitoring. However, the reliance on communication and sparsely spacial distribution make the sensor system vulnerable in the presence of various cyber attacks such as measurement manipulation, communication block, false data injection, etc. Since malicious attacks, such as Stuxnet [1] and BlackEnergy malware [2] may incur substantial damage on economy, ecosystem and even public safety, designing resilient networked system with secure detection, estimation and control algorithm has been recognized by both engineers and scholars as a significant research field.

In this paper we consider the problem of detecting a binary state θ with s sensors in adversarial environment. We assume c out of s sensors are compromised and their observations could be manipulated arbitrarily by the adversary. We introduce the Byzantine attack setting where system manager has no information about the exact set of corrupted sensors but only knows the cardinality of the set. The detection performance is evaluated by its Average Sample Number under prescribed level of significance (probability of error). We adopt a similar formulation as [3] where the problem is considered as a game between the detector and the attacker, in which the detector attempts to optimize the performance while the adversary intends to deteriorate it. A pair of strategy (attack strategy from the adversary and hypothesis testing scheme from the detector) is proposed and proved to be a Nash equilibrium pair for the game. Furthermore, scenario with unknown number of compromised sensors is investigated and choice of parameter in sequential test algorithm is discussed. Result of this paper is verified by numerical simulation.

Related Work: The study of sequential analysis (to the best of our knowledge) originated from Abraham Wald et al. [4][5] who proposed the Sequential Probability Ratio Test (SPRT) and proved its optimality in 1940s. Due to its wide applicability and optimality in hypothesis testing, sequential analysis has gained wide application in sensor network security design [6][7], change detection[8][9], signal anomaly detection [10][11], etc.

As threats to control systems from cyber attacks are increasing rapidly these days, studies about secure detection problem draw attention from researchers. The research efforts can be classified into two main directions: anomaly diagnose and resilient algorithm design. In the former one, anomaly diagnosis schemes are designed to reveal the existence of attack and trigger alarm and/or recovery mechanism. For example, the problem of revealing the existence of attacks and vulnerable part of the system that requires protection is considered in [12] and [13]. In the research about resilient algorithm design, researchers pursuit a scheme of secure system which has graceful performance degradation in the presence of attack. Since attacks may not be eliminated immediately even if we know its existence because of the concealment of attackers in cyberspace, resilient algorithm design is preferred in the sense of safety guarantee. We choose resilient testing algorithm design as our research goal in this paper.

The problem of resilient inference has been studied from various perspective recently including hypothesis testing [3][14], change detection [9][8], state estimation [15], etc. We focus on hypothesis testing problem. Similar formulation of detecting a binary state with multiple sensors under Byzantine attack is studied by Ren et al. [16] recently and the problem of security-efficiency trade-off is raised. Moreover, the model is extended to multi-hypothesis testing and heterogeneous sensor scenario where game theoretic approach is adopted [17] and sensor selection problem is investigated [18].

Main Innovation: We consider the problem of detecting a binary state using sequential analysis in the sense that stopping time is determined by observations while some other researches use a prescribed number of observed samples, e.g. one-shot scheme [19][20] and fixed time analysis [16]. By

[1]: Y. Mo and Z. Li are with the Department of Automation and BNRist Intelligence System Lab, Tsinghua University, China. Email: ylmo@tsinghua.edu.cn; lizs19@mails.tsinghua.edu.cn.

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

978-1-7281-1398-2/19/$31.00 ©2019 IEEE

making decision adapted to observations, Average Sample Number is saved (as can be seen in Remark 8) because sampling is stopped as soon as the existing observations possess enough preference on a certain hypothesis. The efficiency of detection sampling in our paper is evaluated and optimized by integrating ASN into performance metric (see definition of delay in equation 5). Similar methodology could be seen in the study of change detection (e.g. [8][21]).

Organization: The rest of this paper is organized as follows: In Section II, we formulate the problem of binary hypothesis test and define the admissible attack and binary state detecting strategy as well as the performance metric. In Section III, we propose an attack strategy by flipping the distribution of observations from the compromised sensors and a resilient detection strategy by voting among all sensors. This pair of strategy is then proved to form an equilibrium pair for the game between attacker and detector. In Section IV, the scenario where actual number of compromised sensors is unknown is investigated and corresponding performance is quantified. Simulation result is provided in Section V, and Section VI finally concludes the paper.

Notations: We denote by $\mathbb{Z}^+$ the set of positive integers and by $\mathbb{R}$ the set of real numbers. We denote by $x \sim y$ when $x/y \to 1$. Cardinality of a finite set $\mathcal{S}$ is denoted as $|\mathcal{S}|$. Transpose of a vector or matrix is denoted by superscript T.

II. PROBLEM FORMULATION

A. Binary Hypothesis Testing

Suppose there is a binary state $\theta \in \{0,1\}$ detected by a group of s sensors. At each discrete time index k, the observation from each sensor $i \in \mathcal{S} \triangleq \{1,2,...,s\}$ is collected by a fusion center. Let row vector $\boldsymbol{x}_i = [x_i(1), x_i(2), x_i(3), ...]$ denote the sequence of observations from the ith sensor and column vector $\boldsymbol{x}(k) = [x_1(k), x_2(k), x_3(k), ..., x_s(k)]^T$ denote the observations at time k from all sensors. We assume that all observations from different sensors at different time are independently identically distributed for each θ. Simialr to notations in [16], when the hypothesis is false ($\theta = 0$), probability measure generated by $x_i(k)$ is denoted as ν and it is denoted as μ when the hypothesis is true ($\theta = 1$). In other words, for any Borel-measurable set $\mathscr{B} \subseteq \mathbb{R}$, the probability that $x_i(k) \in \mathscr{B}$ equals to $\nu(\mathscr{B})$ when $\theta = 0$ and equals to $\mu(\mathscr{B})$ when $\theta = 1$. We denote the probability space generated by all measurements $\boldsymbol{x}(1), \boldsymbol{x}(2), \ldots$ as $(\Omega, \mathscr{F}, \mathbb{P}_\theta)$, where for any $l \geq 1$

$$\mathbb{P}_\theta(x_{i_1}(k_1) \in \mathscr{B}_1, \ldots, x_{i_l}(k_l) \in \mathscr{B}_l) = \begin{cases} \nu(\mathscr{B}_1)\nu(\mathscr{B}_2)\ldots\nu(\mathscr{B}_l) & \text{if } \theta = 0 \\ \mu(\mathscr{B}_1)\mu(\mathscr{B}_2)\ldots\mu(\mathscr{B}_l) & \text{if } \theta = 1 \end{cases},$$

when $(i_j, k_j) \neq (i_{j'}, k_{j'})$ for all $j \neq j'$. The expectation taken with respect to $\mathbb{P}_\theta$ is denoted by $\mathbb{E}_\theta$.

We further assume that probability measure ν and μ are absolutely continuous with respect to each other. Therefore, the log-likelihood ratio $L_i(k)$ of $x_i(k)$ is well-defined as

$$L_i(k) \triangleq \log\left(\frac{\mathrm{d}\mu}{\mathrm{d}\nu}(x_i(k))\right), \tag{1}$$

where $\mathrm{d}\mu/\mathrm{d}\nu$ is the Radon-Nikodym derivative.

B. Byzantine Attack

Let the (manipulated) observation received by the fusion center at time k be

$$\boldsymbol{x}'(k) = \boldsymbol{x}(k) + \boldsymbol{x}^a(k), \tag{2}$$

where $\boldsymbol{x}^a(k) \in \mathbb{R}^s$ is the deflective vector injected by the attacker at time k. By adding values to the real observations $\boldsymbol{x}(k)$, the attacker can rewrite them to arbitrary value they assign. We have the following assumptions on the attacker.

***Assumption** 1 (Sparse Attack):* There exists an index set $\mathcal{C} \subseteq \mathcal{S}$ with $|\mathcal{C}| = c$ such that $\bigcup_{k=1}^{\infty} \mathrm{supp}\{\boldsymbol{x}^a(k)\} = \mathcal{C}$ where $\mathrm{supp}(\boldsymbol{x}) \triangleq \{i \in \mathcal{S} : x_i \neq 0\}$ is the support of vector $\boldsymbol{x}$. Furthermore, the system knows the cardinality c, but it does not know the set $\mathcal{C}$.

***Remark** 1:* It is conventional in the literature (e.g. [8] [22][23]) to assume that the attacker possesses limited resources, i.e., the number (or percentage) of compromised sensors is fixed and is known by the system manager. The value of c can also be seen as a design parameter representing the tolerance of sensor corruptions in the system.

We denote by $\mathcal{H} \triangleq \mathcal{S} \setminus \mathcal{C}$ the honest (not affected by attack) sensor. The information the attacker have access to is assumed as follows:

***Assumption** 2 (Attacker Knowledge):* (1) The attacker knows the probability measure, i.e. μ and ν; (2) The attacker knows the real system state θ; (3) The attacker knows the real observation from all compromised sensors from the beginning to the present time instant.

***Remark** 2:* The only restriction on the attack strategy is that the set of compromised sensors is fixed (from Assumption 1). The attacker have adequate knowledge about the system and can carry out complex attack strategies such as time-varying or probabilistic ones. This assumption is conventional in literature concerning the worst-case attacks (e.g. [24]). Nevertheless, assuming the adversary to be powerful when designing system would make sure its security and is in accordance with the Kerckhoffs's principle.

An admissible attack strategy is a mapping from attacker's information set to the bias vector that satisfies Assumption 1. Let the compromised sensor index set $\mathcal{C} = \{i_1, i_2, \cdots, i_c\}$. Define $\boldsymbol{X}_{\mathcal{C}}(k)$ as the matrix formed by true measurements from time 1 to k at compromised sensors:

$$\boldsymbol{X}_{\mathcal{C}}(k) \triangleq [\boldsymbol{x}_{\mathcal{C}}(1), \boldsymbol{x}_{\mathcal{C}}(2), \cdots, \boldsymbol{x}_{\mathcal{C}}(k)] \in \mathbb{R}^{c \times k} \tag{3}$$

with

$$\boldsymbol{x}_{\mathcal{C}}(k) \triangleq [x_{i_1}(k), x_{i_2}(k), \cdots, x_{i_c}(k)]^T \in \mathbb{R}^{c \times 1}.$$

Similar to definition in (3), $\boldsymbol{X}^a(k) \in \mathbb{R}^{s \times k}$ is defined as the matrix formed by bias vectors $\boldsymbol{x}^a(k) \in \mathbb{R}^{s \times 1}$ from time 1 to k. The injected bias vector is designed by the attacker based on its information set, i.e.

$$\boldsymbol{x}^a(k) = g\left(\boldsymbol{X}_{\mathcal{C}}(k), \boldsymbol{X}^a(k-1), \theta, k\right), \tag{4}$$

where g is a measurable function of accessible observations $\boldsymbol{X}_{\mathcal{C}}(k)$, history attacks $\boldsymbol{X}^a(k-1)$, real state θ and

time k such that $\boldsymbol{x}^a(k)$ satisfies Assumption 1. Denote the probability space generated by all manipulated observations $\boldsymbol{x}'(1),\boldsymbol{x}'(2),\dots$ as $(\Omega,\mathscr{F},\mathbb{P}_\theta^g)$ where θ is the real state. The corresponding expectation is denoted as $\mathbb{E}_\theta^g$.

C. Performance Metric

The detector at time k is defined as a mapping from the manipulated observation matrix to the set of decision:

$$f_k : \boldsymbol{X}'(k) \to \{continue, 0, 1\},$$

where *continue* denote taking next observation at time $k+1$ because existing knowledge is not enough to make a decision. Decision 0 and 1 denote stop taking observations and choose hypothesis H_0 and H_1 respectively. System's strategy $f \triangleq (f_1, f_2, \cdots)$ is defined as an infinite sequence of detectors from time 1 to ∞.

Based on the definition of detection strategies, the stopping time T representing the time that the test terminates is a $\{\mathscr{F}_t'\}$-stopping time, where $\mathscr{F}_t'$ is a σ-field of all the (manipulated) observations from time 1 to k: $\mathscr{F}_t' = \sigma\{\boldsymbol{X}'(k)\}$. Define the worst case Average Sample Number (detection delay) under attack g as

$$D(T) \triangleq \max_{\theta=0,1} \mathbb{E}_\theta^g[T]. \tag{5}$$

Denote the probability of Type-I and Type-II error[1] of the binary hypothesis testing problem as α and β respectively, e.g. $\alpha \triangleq \mathbb{P}_0^g[f_T = 1], \beta \triangleq \mathbb{P}_1^g[f_T = 0]$. As a detector needs to make decisions based on as few samples as possible under varying error probability constraints, we consider the asymptotic performance as error probability tends to zero:

$$\gamma(f,g) \triangleq \lim_{\alpha=\beta\to 0^+} \frac{\log(1/\alpha)}{D(T)}. \tag{6}$$

***Remark** 3:* By definition, $\gamma(f,g) \geq 0$ for any admissible f and g because $\alpha \leq 1$ and $D(T) > 0$. The performance integrates error probabilities α,β with detection delay $D(T)$ which we hope to be small at the same time. It means larger γ indicates better detection performance.

***Remark** 4:* The performance γ is determined by both the detection rule f and attack strategy g so it is denoted as $\gamma(f,g)$. The system manager intends to design a resilient detector f to maximize γ while the attacker needs malicious attack g to minimize γ.

In this paper, we intend to propose a pair of strategy (f^*,g^*), such that for any strategies f and g, the following inequality holds:

$$\gamma(f,g^*) \leq \gamma(f^*,g^*) \leq \gamma(f^*,g). \tag{7}$$

As a result, the pair of strategy (f^*,g^*) reaches a Nash equilibrium (which is not necessarily unique). In other words, given strategy of one player as f^* (or g^*), the other player do not have a strictly better strategy. We present the strategy pair in the next section.

[1]In statistical hypothesis testing, a type-I error is rejection of a true null hypothesis H_0, while a type-II error is the failure to reject a false null hypothesis.

III. Equilibrium Strategy Pair

In this section we present an attack strategy and a detection scheme and prove that they can form a Nash equilibrium pair.

A. Preliminaries Results

Before we go on, we first present some basic results of hypothesis testing scheme without attack which will be helpful for future discussion. Denote the Kullback-Leibler (K–L) divergences between those two distribution we are trying to distinguish (i.e. μ and ν) as

$$I_1 \triangleq \int_{x\in\mathbb{R}} \log\left[\frac{\mathrm{d}\mu(\mathrm{x})}{\mathrm{d}\nu(\mathrm{x})}\right] \mathrm{d}\mu(x), I_0 \triangleq -\int_{x\in\mathbb{R}} \log\left[\frac{\mathrm{d}\mu(\mathrm{x})}{\mathrm{d}\nu(\mathrm{x})}\right] \mathrm{d}\nu(x)$$

To avoid degenerate problems, we adopt the following assumptions:

***Assumption** 3:* The K–L divergences are well-defined, i.e., $0 < I_0, I_1 < \infty$.

We introduce a more general sequential test strategy for multiple sensor based on Sequential Probability Ratio Test proposed by Wald [25]. We denote the cumulative log-likelihood ratio of sensor i at time n by $S_i(n)$ and the one summing over set $\mathcal{M}$ by $S_{\mathcal{M}}(n)$:

$$S_i(n) \triangleq \sum_{k=1}^{n} L_i(k), \quad S_{\mathcal{M}}(n) \triangleq \sum_{i\in\mathcal{M}} S_i(n), \tag{8}$$

where $\mathcal{M} \subseteq \mathcal{S}$. The decision is taken according to whether the prescribed threshold is crossed, i.e.

$$f_k = \begin{cases} 0, & S_{\mathcal{M}}(k) \leq -a \\ continue, & -a < S_{\mathcal{M}}(k) < b \\ 1, & S_{\mathcal{M}}(k) \geq b \end{cases}, \tag{9}$$

where $a,b > 0$ are chosen to regulate error probabilities α,β. Denote the defined detection rule based on summed log-likelihood ratio from sensors in $\mathcal{M}$ as $f_{\mathcal{M}}$. We have the following lemma quantifying performance of this test (called sum-SPRT) in the absence of attack. The proof is provided in Appendix A of [26] due to space limitation.

***Lemma** 1:* Define $I \triangleq \min\{I_0, I_1\}$, for all admissible test rule f based on sensor information in $\mathcal{M}$,

$$\gamma(f, g = \mathbf{0}) \leq \gamma(f_{\mathcal{M}}, g = \mathbf{0}) = |\mathcal{M}| \cdot I, \tag{10}$$

where $g = \mathbf{0}$ means the attacker is absent.

***Remark** 5:* The performance of $f_{\mathcal{M}}$ is proportional to the number of sensors $|\mathcal{M}|$ and the constant I defined by K-L divergence. Constant I who represents the "distance" of two distributions could be treated as a basic unit of performance.

Now we move on to consider the detection problem under attack. We assume $s > 2c$ to prevent trivial problems in the rest of paper if without further notice.

B. Attack Strategy

In this subsection we show an attack strategy where the attacker flips the distribution of the compromised sensor observations under different states to confuse the detector. We denote it as g^* (named flip attack) and it is defined in the following:

Denote sensor index set of the first c sensors as $\mathcal{O}_1 \triangleq \{1,2,\ldots,c\}$ and the set of last c sensors as $\mathcal{O}_2 \triangleq \{s-c+1, s-c+2, \ldots, s\}$. If $\theta = 0$, the adversary generates random observations $\tilde{x}_i(k)$ at time k for every sensor $i \in \mathcal{O}_1$ according to the opposite distribution μ, i.e. for any Borel-measurable set $\mathscr{B}$,

$$\mathbb{P}[\tilde{x}_i(k) \in \mathscr{B}] = \mu(\mathscr{B}),\ \theta = 0, i \in \mathcal{O}_1. \tag{11}$$

Then the malicious bias data is designed to make sure the final manipulated observations $x_i(k) + x_i^a(k)$ of sensors in $\mathcal{O}_1$ are the same as $\tilde{x}_i(k)$:

$$x_i^a(k) = \tilde{x}_i(k) - x_i(k),\ \theta = 0, i \in \mathcal{O}_1. \tag{12}$$

If $\theta = 1$, observations in $\mathcal{O}_2$ is manipulated in similar way.

$$\mathbb{P}[\tilde{x}_i(k) \in \mathscr{B}] = \nu(\mathscr{B}),\ \theta = 1, i \in \mathcal{O}_2. \tag{13}$$

$$x_i^a(k) = \tilde{x}_i(k) - x_i(k),\ \theta = 1, i \in \mathcal{O}_2. \tag{14}$$

For sensors not mentioned above, the bias value $x_i^a(k) = 0$. By this operation, the following inequality of performance holds.

***Theorem** 1:* For any admissible detection strategy f we have

$$\gamma(f, g^*) \leq (s-2c)I. \tag{15}$$

***Remark** 6:* The coefficient $(s-2c)$ indicates that the detector will have positive performance when less than half of the sensors are compromised. It also implies every increase of number of compromised sensor will incur two units of performance decrease. The result follows from Theorem 3 (2) in [16].

Proof: Under attack g^*, for either $\theta = 0$ or $\theta = 1$, sensors in $\mathcal{O}_1$ will follow distribution μ and sensors in $\mathcal{O}_2$ will follow distribution ν. In other words, only sensors in $\mathcal{S} \setminus (\mathcal{O}_1 \cup \mathcal{O}_2)$ have different distributions under different θ. Since we assume $s > 2c$, $\mathcal{S} \setminus (\mathcal{O}_1 \cup \mathcal{O}_2) \neq \emptyset$. If we define $\mathcal{M} = \mathcal{S} \setminus (\mathcal{O}_1 \cup \mathcal{O}_2)$, according to Lemma 1:

$$\gamma(f, g^*) \leq \gamma(f_{\mathcal{M}}, g = \mathbf{0}) = |\mathcal{S} \setminus (\mathcal{O}_1 \cup \mathcal{O}_2)|I = (s-2c)I.$$

Thus, equation (15) is obtained. ■

C. Detection Strategy

In this section we present a detection strategy that could form a Nash equilibrium pair with flip attack g^*. Before we present the detection rule, we first define some notations.

First we define the stopping time of single threshold test for each sensor i in the following two equations. Similar to basic SPRT, those two thresholds are denoted as $-a < 0 < b$:

$$\tau_i^+(b) \triangleq \inf_{k \in \mathbb{Z}^+} \{S_i(k) \geq b\}. \tag{16}$$

$$\tau_i^-(a) \triangleq \inf_{k \in \mathbb{Z}^+} \{S_i(k) \leq -a\}. \tag{17}$$

Then sort those stopping time of the same threshold in an ascending order and denote them as $\tau_{(i)}^-(a), \tau_{(i)}^+(b)$:

$$\tau_{(1)}^-(a) \leq \tau_{(2)}^-(a) \leq \cdots \leq \tau_{(s)}^-(a),$$
$$\tau_{(1)}^+(b) \leq \tau_{(2)}^+(b) \leq \cdots \leq \tau_{(s)}^+(b).$$

Define r as the parameter of decision rules with $s/2 < r \leq s$ and the voting rule $f^{(r)}$ is defined as taking corresponding hypothesis the first time when there have been r crossing of the same threshold. The rule is showed formally in the following. For each time k,

$$f_k^{(r)} = \begin{cases} \textit{continue}, & k < min\{\tau_{(r)}^-(a), \tau_{(r)}^+(b)\} \\ 0, & k = \tau_{(r)}^-(a) < \tau_{(r)}^+(b) \\ 1, & k = \tau_{(r)}^+(b) < \tau_{(r)}^-(a) \\ 0 \textit{ or } 1, & k = \tau_{(r)}^+(b) = \tau_{(r)}^-(a) \end{cases}. \tag{18}$$

The decision 0 *or* 1 means stop sampling and take H_0 or H_1 with the same probability 0.5. Denote the detection strategy defined above as $f^{(r)} \triangleq \{f_1^{(r)}, f_2^{(r)}, \ldots\}$. We denote the stopping time of detection rule $f^{(r)}$ as $T^{(r)}$.

Before we show the performance of detection strategy, we provide some preliminary results of stopping times and error probabilities in absence of attack whose proof is provided in Appendix B of [26] because of space limitation.

***Theorem** 2:*

$$(1) \lim_{a=b\to\infty} \mathbb{E}_0 \left| \frac{\tau_{(r)}^-(a)}{a} - \frac{1}{I_0} \right| = 0, \lim_{a=b\to\infty} \mathbb{E}_1 \left| \frac{\tau_{(r)}^+(b)}{b} - \frac{1}{I_1} \right| = 0 \tag{19}$$

$$(2) \lim_{a=b\to\infty} \frac{\mathbb{E}_0[T^{(r)}]}{a} \leq \frac{1}{I_0},\ \lim_{a=b\to\infty} \frac{\mathbb{E}_1[T^{(r)}]}{b} \leq \frac{1}{I_1} \tag{20}$$

$$(3) \lim_{a=b\to\infty} \frac{1}{b} \log \mathbb{P}_0[\tau_{(r)}^+(b) \leq \tau_{(r)}^-(a)] \leq -r \tag{21}$$

$$\lim_{a=b\to\infty} \frac{1}{a} \log \mathbb{P}_1[\tau_{(r)}^-(a) \leq \tau_{(r)}^+(b)] \leq -r \tag{22}$$

Based on Theorem 2 we are ready to show the performance of our detection rule with carefully designed r.

***Theorem** 3:* For any admissible attack strategy g, fix $r = s-c$ and denote $f^* \triangleq f^{(s-c)}$. We have

$$\gamma(f^*, g) \geq (s-2c)I.$$

Proof: We show the following inequalities for arbitrary attack g (notice that $\mathbb{P}_\theta^g$ and $\mathbb{E}_\theta^g$ denote probability and expectation under attack g)

$$\mathbb{E}_1^g[\tau_{(r)}^+(b)] \leq \mathbb{E}_1[\tau_{(r+c)}^+(b)]. \tag{23}$$

$$\mathbb{E}_0^g[\tau_{(r)}^-(a)] \leq \mathbb{E}_0[\tau_{(r+c)}^-(a)]. \tag{24}$$

$$\mathbb{P}_1^g[\tau_{(r)}^-(a) \leq \tau_{(r)}^+(b)] \leq \mathbb{P}_1[\tau_{(r-c)}^-(a) \leq \tau_{(r-c)}^+(b)]. \tag{25}$$

$$\mathbb{P}_0^g[\tau_{(r)}^-(a) \geq \tau_{(r)}^+(b)] \leq \mathbb{P}_0[\tau_{(r-c)}^-(a) \geq \tau_{(r-c)}^+(b)]. \tag{26}$$

Due to space limitations, the proof of these four inequalities above is shown in Appendix C of [26]. They are obtained considering cumulative log-likelihood ratio and threshold-reached time in the worst case given all admissible attacks.

We are ready to quantify the performance under attack with the help of inequalities (23) to (26). On one hand, detection delay can be upper bounded based on (19) and (23):

$$\mathbb{E}_1^g[T^{(r)}] \leq \mathbb{E}_1^g[\tau_{(r)}^+(b)] \leq \mathbb{E}_1[\tau_{(r+c)}^+(b)] \sim \frac{b}{I_1}.$$

in which the first inequality comes from definition of voting rule (18). On the other hand, error probability can be

quantified based on (22) and (25):

$$\begin{aligned}\beta \leq & \mathbb{P}_1^g[\tau_{(r)}^-(a) \leq \tau_{(r)}^+(b)] \\ \leq & \mathbb{P}_1[\tau_{(r-c)}^-(a) \leq \tau_{(r-c)}^+(b)] \leq Ce^{-(r-c)a},\end{aligned}$$

where C is a constant term. Those two inequalities imply

$$\begin{aligned}\lim_{\alpha=\beta\to 0^+} \frac{\log(1/\beta)}{\mathbb{E}_1^g[T^{(r)}]} &= \lim_{a=b\to\infty} \frac{\log(1/\beta)}{\mathbb{E}_1^g[T^{(r)}]} \\ &\geq \lim_{a=b\to\infty} \frac{(r-c)\cdot a}{b/I_1} = (r-c)I_1.\end{aligned}$$

When $\theta = 0$, similar results could be derived from equation (24) and (26). Thus, by replacing r with $s-c$, the final result is obtained:

$$\gamma(f^*, g) \geq (s-c-c)\min\{I_0, I_1\} = (s-2c)I.$$

The proof is completed. ■

Combining Theorem 1 and 3, we are ready to show the Nash equilibrium pair of strategies.

***Theorem** 4:* Detection strategy f^* defined in (18) with $r = s-c$ and attack strategy g^* defined in (11) to (14) form a Nash equilibrium, i.e. for any admissible detection rule f and attack g,

$$\gamma(f, g^*) \leq \gamma(f^*, g^*) = (s-2c)I \leq \gamma(f^*, g).$$

Proof: Set the detector in Theorem 1 as f^* and attack in Theorem 3 as g^* and we can obtain $\gamma(f^*, g^*) \geq (s-2c)I$ and $\gamma(f^*, g^*) \leq (s-2c)I$ at the same time. Substituting $(s-2c)I$ with $\gamma(f^*, g^*)$ in theorem 1 and 3 leads to the result. ■

***Remark** 7:* The payoffs for players of the game are $\gamma(f, g)$ (for detector f) and $-\gamma(f, g)$ (for attacker g). Notice that the strategy set for this game is non-compact, the Nash equilibrium does not necessarily exist. Our result actually proved the existence of Nash equilibrium in addition to a pair of specific strategy.

***Remark** 8:* Since the definition of $\gamma(f, g)$ can also be used to evaluate non-sequential detection schemes, we are able to compare their performance with ours. We define

$$\tilde{I} \triangleq -\log\left[\inf_{w\in\mathbb{R}}\left\{\int_{x\in\mathbb{R}}\left(\frac{\mathrm{d}\mu(x)}{\mathrm{d}\nu(x)}\right)^w \mathrm{d}\nu(x)\right\}\right].$$

It has been shown in [16] Theorem 2 that $0 < \tilde{I} < I$. The detector performance defined in [16] is the same as ours for fixed sample detecting scheme. However, the value of detector performance in that paper is $(s-2c)\tilde{I}$ which is smaller than ours. In this sense, our scheme is more sample-efficient because the sampling is terminated as soon as there is enough statistical information indicating the real hypothesis.

***Remark** 9:* Single time step computation complexity of our detection scheme is $O(s)$ as computing $S_i(k)$ and voting among sensors both have a complexity of $O(s)$. Therefore, the computational complexity is lower than the result in [16] where the sorting algorithm cause a computational complexity of $O(s\log s)$. Moreover, voting detection algorithm is more easily applied to distributed computing because the sensors do not need to send the actual observations to the control center but only need to inform whether the threshold is crossed. System based on our detection algorithm have less information transmission pressure and is more likely to achieve better efficiency and resilience.

IV. Extensions

In the previous section, we assume the number of compromised sensors c is known to the system manager. However, in practice the real value may be unknown and what we have is a estimation of its upper bound. It can be seen as a design parameter denoting how many sensor corruptions the system can tolerate. In this section, we study the condition where we have an upper bound $\bar{c}$ and the actual number of compromised sensors c can take value in $\{0, 1, 2, \ldots, \bar{c}\}$.

We denote the voting detection rule with $r = s-\bar{c}$ as $\tilde{f} \triangleq f^{(s-\bar{c})}$. We have the following Theorem revealing the lower bound of its performance.

***Theorem** 5:* Given detector $\tilde{f}$, assume c is the actual number of compromised sensors and $c \leq \bar{c} < s/2$. Under any admissible attack, we have

$$\gamma(\tilde{f}, g) \geq (s-\bar{c}-c)I.$$

Proof: In this setting, Theorem 3 still holds true and the only difference is the choice of r. Thus, the result is obtained by substituting $s-c$ with $s-\bar{c}$. ■

***Remark** 10:* The performance loss is in proportional to the sum of estimation number of corruption $\bar{c}$ and the actual number of corruption c. If c is fixed, excessive $\bar{c} > c$ will cause unnecessary performance loss.

The result in Theorem 5 implies the performance lower bound is $(s-\bar{c})I$ when all sensors are benign. We present it in the following Corollary formally.

***Corollary** 1:* When there is no attack, i.e. $c = 0$, performance is lower bounded:

$$\gamma(\tilde{f}, g = \mathbf{0}) \geq (s-\bar{c})I.$$

***Remark** 11:* $\gamma(\tilde{f}, g = \mathbf{0})$ could be seen as the detection efficiency of voting rule at normal operation (attacker is absent). The increasing of $\bar{c}$ will sacrifice detection performance in absence of attack while gaining better system resilience. Thus, sufficient knowledge about the attacker (e.g. how many sensors will be compromised) will be helpful for system efficiency-security trade off. Since the equilibrium strategy pair is not unique, questing for a detection rule who can achieve maximum performance when the attack is present and absent simultaneously is meaningful and could be our future work.

V. Simulation

In this section, we provide some numerical examples to verify the results established in the previous sections. We assume the observations of sensors follow i.i.d. distribution of $N(-1,1)$[2] when $\theta = 0$ and $N(1,1)$ when $\theta = 1$. In this case $I = I_0 = I_1 = 2$.

We set $s = 10$ and c varies from 0 to 4. In Fig. 1, detection and attack strategy are f^* and g^* respectively. We calculate

[2] $N(p, q^2)$ represent Normal distribution with mean p and variance q^2.

detection delay $D(T)$ and error probability α with threshold $a = b$ vary from 5×10^0 to 1×10^5 for each fixed c. The result $\frac{\log(1/\alpha)}{D(T)}$ is normalized by I and should tend to $s - 2c$ according to Theorem 4. To simulate the error probability with higher accuracy, we adopt the importance sampling approach [27].

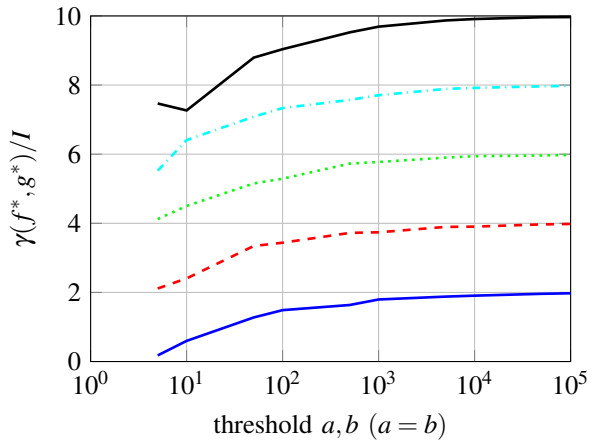

Fig. 1. Normalized performance of equilibrium strategy pair (f^*, g^*) when $s = 10$ for $c = 0$ (black solid line), $c = 1$ (cyan dash dot line), $c = 2$ (green dot line) , $c = 3$ (red dash line) and $c = 4$ (blue solid line).

VI. Conclusion

In this paper, we formulate the problem of binary sequential detection in adversarial environment as a game between the detector and the attacker. Detection performance is defined asymptotically by both error probability and Average Sample Number as error probability tends to zero and this value is integrated in the game as payoff which the detector intends to maximize while the attacker intends to minimize. We propose a pair of detection rule and attack strategy and prove them to be an equilibrium pair of the game. Furthermore, the performance in condition where number of compromised sensor is unknown and where all sensors are benign is quantified. The choice of detection rule parameter r is discussed and result is corroborated by numerical simulations. The future work includes the trade-off between system's security and efficiency as well as discussion about (simultaneous) achievability of optimal security and efficiency.

References

[1] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Security Privacy*, vol. 9, no. 3, pp. 49–51, May 2011.

[2] G. Salles-Loustau, L. Garcia, P. Sun, M. Dehnavi, and S. Zonouz, "Power grid safety control via fine-grained multi-persona programmable logic controllers," in *2017 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Oct 2017, pp. 283–288.

[3] J. Yan, X. Ren, and Y. Mo, "Sequential detection in adversarial environment," in *2017 IEEE 56th Annual Conference on Decision and Control (CDC)*, Dec 2017, pp. 170–175.

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

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

[6] J. Ho, "Distributed detection of replica cluster attacks in sensor networks using sequential analysis," in *2008 IEEE International Performance, Computing and Communications Conference*, Dec 2008, pp. 482–485.

[7] J. Ho, M. Wright, and S. K. Das, "Fast detection of mobile replica node attacks in wireless sensor networks using sequential hypothesis testing," *IEEE Transactions on Mobile Computing*, vol. 10, no. 6, pp. 767–782, June 2011.

[8] 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.

[9] H. Wang, D. Zhang, and K. G. Shin, "Change-point monitoring for the detection of dos attacks," *IEEE Transactions on Dependable and Secure Computing*, vol. 1, no. 4, pp. 193–208, Oct 2004.

[10] D. Li, M. Zhang, Z. Lai, and Y. Shen, "Sequential probability ratio test based fault detection method for actuators in gnc system," in *Proceedings of the 32nd Chinese Control Conference*, July 2013, pp. 6324–6327.

[11] D. Yuan, H. Li, and M. Lu, "A method for gnss spoofing detection based on sequential probability ratio test," in *2014 IEEE/ION Position, Location and Navigation Symposium - PLANS 2014*, May 2014, pp. 351–358.

[12] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "Revealing stealthy attacks in control systems," in *2012 50th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, Oct 2012, pp. 1806–1813.

[13] L. Hu, Z. Wang, Q.-L. Han, and X. Liu, "State estimation under false data injection attacks: Security analysis and system protection," *Automatica*, vol. 87, pp. 176 – 183, 2018.

[14] B. Kailkhura, Y. S. Han, S. Brahma, and P. K. Varshney, "Asymptotic analysis of distributed bayesian detection with byzantine data," *IEEE Signal Processing Letters*, vol. 22, no. 5, pp. 608–612, May 2015.

[15] H. Fawzi, P. Tabuada, and S. Diggavi, "Secure estimation and control for cyber-physical systems under adversarial attacks," *IEEE Transactions on Automatic Control*, vol. 59, no. 6, pp. 1454–1467, June 2014.

[16] 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.

[17] X. Ren and Y. Mo, "Multiple hypothesis testing in adversarial environments: A game-theoretic approach," in *2018 Annual American Control Conference (ACC)*, June 2018, pp. 967–972.

[18] ——, "Secure detection: Performance metric and sensor deployment strategy," in *IEEE Transactions on Signal Processing*, vol. 66, no. 17, Sep. 2018, pp. 4450–4460.

[19] K. G. Vamvoudakis, J. P. Hespanha, B. Sinopoli, and Y. Mo, "Detection in adversarial environments," *IEEE Transactions on Automatic Control*, vol. 59, no. 12, pp. 3209–3223, Dec 2014.

[20] Y. Mo, J. P. Hespanha, and B. Sinopoli, "Resilient detection in the presence of integrity attacks," *IEEE Transactions on Signal Processing*, vol. 62, no. 1, pp. 31–43, Jan 2014.

[21] V. V. Veeravalli and T. Banerjee, "Quickest change detection," *Mathematics*, vol. 33, no. 14, pp. 4434–4457, 2012.

[22] E. Soltanmohammadi, M. Orooji, and M. Naraghi-Pour, "Decentralized hypothesis testing in wireless sensor networks in the presence of misbehaving nodes," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 1, pp. 205–215, Jan 2013.

[23] B. Kailkhura, Y. S. Han, S. Brahma, and P. K. Varshney, "Asymptotic analysis of distributed bayesian detection with byzantine data," *IEEE Signal Processing Letters*, vol. 22, no. 5, pp. 608–612, May 2015.

[24] 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.

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

[26] Z. Li, Y. Mo, and F. Hao, "Game theoretical approach to sequential hypothesis test with byzantine sensors." [Online]. Available: https://arxiv.org/abs/1909.02909

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