Sequential Detection in Adversarial Environment

Jiaqi Yan, Xiaoqiang Ren, and Yilin Mo*

***Abstract*— In this paper, we consider the problem of sequential detection with m sensors in adversarial environment. An attacker intends to increase the detection error by modifying n out of m sensors' measurements. On the other hand, the detector needs to be designed to achieve the optimal performance during the attack. The problem is formulated as a game between detector and adversary in this paper. We study both cases where $m > 2n$ and $m \leq 2n$, and obtain an equilibrium strategy pair of detection rule and attack scheme for both cases. Furthermore, we investigate the efficiency of our proposed detection strategy in the absence of attacker.**

I. INTRODUCTION

Because of the ever-decreasing price, network embedded sensors have been widely used in critical infrastructures for the purpose of detection, monitoring and control. However, at the same time, the extensive use of sensors also makes the system more vulnerable to potential cyber attacks such as selective forwarding, message manipulation, false data injection, etc. [1]. Since the application of widespread sensors varies from aerospace, manufacturing, transportation, power grids, etc., which are always safety-critical: their failure can cause irreparable harm to economy, environment, and even public health, researcher have acknowledged the importance of designing the system with secure detection, estimation and control algorithm [2].

In this paper, we consider the problem of the sequential detection of a binary state θ with m sensors in adversarial environment. Inspired by the security concern of integrity attack on sensor measurements, we assume that an attacker intends to compromise n out of m sensors by modifying their measurements. The performance of the system is characterized by the probability of detection error in the worst case. We formulate this problem as a game between the detector and attacker, in which the detector attempts to minimize this probability, while the adversary intends to maximize it. We investigate both cases where $m > 2n$ and $m \leq 2n$ and propose optimal strategies for detector and attacker to achieve a Nash-equilibrium [3] for both cases. The efficiency of proposed strategy in the absence of attacker is further discussed.

Related Work

Recently, sequential tests have been widely applied in the detection problem (e.g., [4][5]), which is termed as *sequential detection*. Because of its optimum nature, sequential detection plays an important role in speeding up the detection process [6][7]. However, little of such work concerns cyber attacks and takes security as a goal.

The computer and sensor network security have focused on prevention mechanisms [2]. For example, in [8], secure routing protocols are proposed for designing a secure communication infrastructure. In [9][10], the false data filtering mechanisms are developed to prevent deceptive data injected into sensors network and decrease the energy waste. Although these security mechanisms can improve the security of system in practice, they can often be subverted: inevitable human errors, software bugs, and design flaws create many opportunities for adversary to launch successful attacks [11]. Therefore, it is desirable for a control system which could continue to function well even when under attack [2].

The robust secure detection problem has been extensively studied in recent years [12]). A classical approach is that, researchers first make some reasonable assumptions on the knowledge of attacker, and then propose a detector working against possible adversaries to achieve the optimal performance. In [13], Bayram et al. propose a restricted Neyman-Pearson approach for composite hypothesis testing in the presence of uncertainty in the prior probability distribution. They prove that the robust linear detector design problem can be formulated as a convex optimization problem. A lot of research formulates the detection problem as a minimax optimization (e.g., [14]), where one attempts to construct an optimal detector that minimizes the probability of detection error in the worst case. The main difference between them and this paper is that we intend to propose optimal strategies for not only detector but also attacker to obtain a Nash-equilibrium.

Some researches concerning adversarial environment also formulate the problem as a game. For example, in [15], Vamvoudakis et al. consider the problem of estimating a binary random variable based on sensor measurements that may have been corrupted by a cyber-attacker. The estimation problem is formulated as a zero-sum partial information game. Then new game theoretic approaches are applied to derive the optimal detector. However, these works mainly focus on the one-step situation, while in this paper, we talk about the sequential tests involving the interval from time 1 to time infinity.

The rest of this paper is organized as follows: In section II, we formulate the problem of sequential detection with n manipulated sensors from m total sensors as a game between the detector and attacker. In section III and IV, we propose the equilibrium strategy pair of detection rule and attack strategy for the case where $m > 2n$ and $m \leq 2n$, respectively. In section V, the efficiency of our proposed

*: The authors are with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore. Email: jyan004@e.ntu.edu.sg, xren@ntu.edu.sg, ylmo@ntu.edu.sg

Preprint submitted to 56th IEEE Conference on Decision and Control.
Received March 20, 2017.

detection strategy is investigated. Section VI provides some simulation results, and section VII finally concludes the paper.

Notations: For a vector x, we will denote by x^T as its transpose, and $||x||_0$ as the "zero norm" of x, which indicates the number of the nonzero elements in the vector x. For a scalar v, $\lceil v \rceil = \min\{p \in \mathbb{Z} | v \leq p\}$, and $\lfloor v \rfloor = \max\{p \in \mathbb{Z} | p \leq v\}$, where $\mathbb{Z}$ is the set of integers. We will use $\mathbb{P}_0(A)$ and $\mathbb{P}_1(A)$ to represent the probability of event A on the condition that $\theta = 0$ and $\theta = 1$, respectively.

II. PROBLEM FORMULATION

In this paper, we consider the problem of detecting an unknown binary state $\theta \in \{0, 1\}$ with m sensors' measurements. At each time k, the measurement vector $y(k)$ is defined as:

$$y(k) \triangleq [y_1(k) \quad y_2(k) \quad \cdots \quad y_m(k)] \in \mathbb{R}^m, \tag{1}$$

where $y_i(k)$ is the scalar measurement from sensor i at time k. The following assumptions on sensor measurement $y_i(k)$ are made:

1) Given θ, all measurements $\{y_i(k)\}_{i=1,\ldots,m,k=1,\ldots}$ are independent and identically distributed (i.i.d.).

2) For any Borel-measurable set $S \subseteq \mathbb{R}$, the probability of $y_i(k)$ belongs to S satisfies the following equation:

$$\mathbb{P}(y_i(k) \in S) = \begin{cases} \nu(S) & \text{if } \theta = 0 \\ \mu(S) & \text{if } \theta = 1 \end{cases}, \tag{2}$$

where μ and ν are the probability measure on $\mathbb{R}$. We further assume that ν and μ are absolutely continuous with respect to each other. Hence, the log-likelihood ratio $\lambda : \mathbb{R} \to \mathbb{R}$ of $y_i(k)$ is well defined as

$$\lambda(y_i(k)) \triangleq \log\left(\frac{d\mu}{d\nu}(y_i(k))\right), \tag{3}$$

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

We denote by $Y(k)$ as the row vector of all measurements from time 1 to time k:

$$Y(k) \triangleq [y(1) \quad y(2) \quad \cdots \quad y(k)] \in \mathbb{R}^{mk}. \tag{4}$$

At time k, we define the detector $f_k : \mathbb{R}^{mk} \to [0, 1]$ as a mapping from the measurement space $Y(k)$ to the interval $[0, 1]$. The system follows the detection strategy like this: if $f_k(Y(k)) = \gamma \in [0, 1]$, the system decides the detection value $\hat{\theta}$ to be 1 with probability γ, and decides $\hat{\theta}$ to be 0 with probability $1 - \gamma$. The system's strategy $f \triangleq (f_1, f_2, \cdots)$ is defined as an infinite sequence of detectors from time 1 to time infinity.

A. Attack Model

We assume that an attacker intends to disturb the detection state of the system by modifying sensors' measurement. However, because of the limited resource, it can only compromise n out of m sensors in the system. The set of the compromised sensors is denoted as $\mathcal{I} = \{i_1, \cdots, i_n\}$, which is fixed over time. We assume that the system knows the number n, but it does not know the exact set $\mathcal{I}$.

To simplify notations, let us define:

$$y_{\mathcal{I}}(k) \triangleq [y_{i_1}(k) \quad y_{i_2}(k) \quad \cdots \quad y_{i_n}(k)] \in \mathbb{R}^n, \tag{5}$$

and

$$Y_{\mathcal{I}}(k) \triangleq [y_{\mathcal{I}}(1) \quad y_{\mathcal{I}}(2) \quad \cdots \quad y_{\mathcal{I}}(k)] \in \mathbb{R}^{nk}. \tag{6}$$

Now we consider the knowledge of the attacker. We assume that the attacker knows the probability measure ν and μ, the total number of sensors m, as well as the true state θ. We further characterize the attacker by its knowledge of the measurement vector:

1) An attacker is called a *weak* attacker if at any time k, it knows the measurement vector $Y_{\mathcal{I}}(k)$ from the compromised sensors;

2) An attacker is called a *strong* attacker if at any time k, it knows the measurement vector $Y(k)$ from all sensors.

Remark 1: In practice, if the channel between detector and sensors is not encrypted, then the attacker could potentially learn by eavesdropping the measurements $Y(k)$ from all sensors and thus is a strong attacker. On the other hand, if the communication channel is encrypted and the attacker cannot listen to the communication between the uncompromised sensors and detector, then it is more suitable to assume a weak attacker model.

For simplicity, let us denote by $\tilde{Y}(k)$ as the measurement vector known by the attacker at time k. From the above definition, we have

$$\tilde{Y}(k) \triangleq \begin{cases} Y_{\mathcal{I}}(k) & \text{for a weak attacker} \\ Y(k) & \text{for a strong attacker} \end{cases}.$$

At each time k, the attacker adds a *random* bias vector $y^a(k)$ according to its knowledge of the system $\tilde{Y}(k)$ to the true measurement $y(k)$. As a result, the system has to make its decision based on the manipulated measurement $y'(k)$ which can be defined as

$$y'(k) = y(k) + y^a(k) \triangleq [y'_1(k) \quad y'_2(k) \quad \cdots \quad y'_m(k)], \tag{7}$$

where $y'_i(k)$ is the manipulated measurement of sensor i at time k.Similar to (3), we define the log-likelihood ratio of $y'_i(k)$ as follows:

$$\lambda(y'_i(k)) \triangleq \log\left(\frac{d\mu}{d\nu}(y'_i(k))\right). \tag{8}$$

We further define

$$y^a(k) = [y^a_1(k) \quad y^a_2(k) \quad \cdots \quad y^a_m(k)] \triangleq g(\mathcal{I}, \theta, k, \tilde{Y}(k)), \tag{9}$$

where $y^a_i(k)_{i=1,\ldots,m}$ is the bias measurement vector added to sensor i at time k, and $y^a_i(k) = 0$ for $i \notin \mathcal{I}$. Obviously, g is a function of $\mathcal{I}, \theta, \tilde{Y}(k)$ and k. As a result, g characterizes the attacker's action for all possible scenarios. Hence, we can use g to denote the attacker's strategy. Similar to the definition of $Y(k)$, we further define the manipulated measurements from time 1 to k to be:

$$Y'(k) = [y'(1) \quad y'(2) \quad \cdots \quad y'(k)] \in \mathbb{R}^{mk}. \tag{10}$$

Preprint submitted to 56th IEEE Conference on Decision and Control.
Received March 20, 2017.

B. Asymptotic Detection Performance

Under attacks, the probability that the system makes a wrong decision at time k is

$$e(\theta, \mathcal{I}, k) \triangleq \begin{cases} \mathbb{E} f_k(Y'(k)) & \text{when } \theta = 0 \\ 1 - \mathbb{E} f_k(Y'(k)) & \text{when } \theta = 1 \end{cases}. \quad (11)$$

In this paper, we are concerned with the worst-case scenario. To this end, let us define

$$\epsilon(k) \triangleq \max_{\theta=0,1,|\mathcal{I}|=n} e(\theta, \mathcal{I}, k), \quad (12)$$

which denotes the worst-case probability of detection error considering all possible sets of compromised sensors and true state θ.

At each time k, we want to design a system strategy f_k to minimize $\epsilon(k)$. However, since the computation of expectation usually involves complicated integration, we consider the *asymptotic detection performance* instead. Define the rate function as

$$\rho \triangleq \liminf_{k\to\infty} -\frac{\log \epsilon(k)}{k}. \quad (13)$$

***Remark** 2:* ρ indicates the rate that the probability of detection error goes to 0, which represents the detection performance of the system. From the definition (11)-(13), one can prove that ρ is always nonnegative. If $\rho > 0$, then the probability of error will exponentially decay to 0, and a larger ρ indicates a shorter time for this convergence.

From (11), it is trivial to know that the worst-case rate ρ is a function of both detection strategy f and attacker's strategy g. Therefore, in the rest of this paper, we will use $\rho(f, g)$ instead to indicate this relationship. Clearly, the detector wants to maximize $\rho(f, g)$ to decrease the detection error, while the attacker wants to minimize it to make the error larger.

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:

$$\rho(f^*, g) \geq \rho(f^*, g^*) \geq \rho(f, g^*). \quad (14)$$

As a result, the pair of strategy (f^*, g^*) reaches a Nash-equilibrium [3]. In other words, if the detector implements f^*, then there is no incentive for the adversary to deviate from g^*, and vice versa.

***Remark** 3:* In this paper we only provide one pair of equilibrium strategies in each case we investigate. However, it is worth noticing that the equilibrium strategy pair satisfying (14) may not be unique.

C. Optimal Detection Rate for a Single Sensor in the Absence of Attacker

To simplify the presentation of the detection and attack strategies proposed later, in this subsection, we present the best rate can be achieved when only one sensor's measurements are used under the condition that the attacker is absent. We use C to denote this optimal rate.

From [16], this optimal decay rate is given by

$$C \triangleq \sup_{0<t<1} -\log\left[\mathbb{E}(e^{t\lambda(y_i(k))}|\theta = 0)\right], \quad (15)$$

where $\lambda(y_i(k))$ is the log-likelihood ratio defined in (3).

III. EQUILIBRIUM STRATEGIES FOR $m > 2n$

We first investigate the case when no more than half of the sensors are compromised by the attacker.

Before going on, we introduce the function $s(y, i, j) : \mathbb{R}^m \times \mathbb{N} \times \mathbb{N}$, where $1 \leq i \leq j \leq m$, which satisfies the following two conditions:

1) For any permutation matrix P, $s(Py^T, i, j) = s(y, i, j)$.
2) If $y_1 \leq y_2 \leq \cdots \leq y_m$, $s(y, i, j) = \sum_{l=i}^{j} y_l$.

***Remark** 4:* The function $s(y, i, j)$ can be interpreted as the summation from the ith element in vector y to the jth one after sorting in the ascending order.

From the definition of $s(y, i, j)$, we have the following proposition :

***Proposition** 1:* For $y,\ y' \in \mathbb{R}^m$, and $||y - y'||_0 \leq n$, the following inequalities holds:

1) If $j + n \leq m$, then $s(y', i, j) \leq s(y, i + n, j + n)$;
2) If $i - n \geq 1$, then $s(y', i, j) \geq s(y, i - n, j - n)$.

To simplify notation, let us further define

$$\min_{m-2n}(y) \triangleq s(y, 1, m - 2n), \quad (16)$$

$$\operatorname*{med}_{m-2n}(y) \triangleq s(y, n + 1, m - n), \quad (17)$$

$$\max_{m-2n}(y) \triangleq s(y, 2n + 1, m). \quad (18)$$

Then we have the following lemma:

***Lemma** 1:* For $y,\ y' \in \mathbb{R}^m$, and $||y - y'||_0 \leq n$, the following inequalities hold:

$$\min_{m-2n}(y) \leq \operatorname*{med}_{m-2n}(y') \leq \max_{m-2n}(y). \quad (19)$$

Proof: The proof of Lemma 1 can be immediately achieved from Proposition 1 by substituting $n + 1$ to i, and $m - n$ to j. ■

We are now ready to prove the main theorems of this section. We first derive a detection strategy which achieves the detection rate $\rho \geq m - 2n$ against any possible attack. After that, we propose an attack strategy and further prove that the rate for any detector cannot exceed $m - 2n$ against this attack. Therefore, the Nash-equilibrium is established.

A. Optimal Detection Strategy

At each time k, consider the following detection strategy f_k^*:

1) Compute the sum of log-likelihood ratio from time 1 to time k for each sensor i:

$$\Lambda_i'(k) = \sum_{t=1}^{k} \lambda(y_i'(t)), \quad (20)$$

where $\lambda(y_i'(t))$ is the log-likelihood ratio defined in (8).

Denote

$$\Lambda'(k) \triangleq [\Lambda_1'(k) \quad \Lambda_2'(k) \quad \cdots \quad \Lambda_m'(k)]. \quad (21)$$

Preprint submitted to 56th IEEE Conference on Decision and Control.
Received March 20, 2017.

2) Compute $\text{med}_{m-2n}(\Lambda'(k))$, and compare it to 0 to generate $\hat{\theta}$ as follows:

$$\hat{\theta} = \begin{cases} 0 & \text{if } \underset{m-2n}{\text{med}}\,(\Lambda'(k)) < 0 \\ 1 & \text{if } \underset{m-2n}{\text{med}}\,(\Lambda'(k)) \geq 0 \end{cases}. \tag{22}$$

The system's strategy is defined as $f^* \triangleq (f_1^*, f_2^*, \cdots)$.

***Remark** 5:* If (20) is done in a recursive fashion, then the computational complexity incurred at each k is $O(m)$. The computational complexity for (22) is $O(m\log(m))$, which can be achieved by first sorting $\Lambda_i(k)$ in the ascending order and then summing the middle $m-2n$ elements. Therefore, the total computational complexity at each time step k is $O(m\log(m))$.

We now have the first theorem:

***Theorem** 1:* For any attack strategy g, the following inequality holds:

$$\rho(f^*, g) \geq (m-2n)C.$$

Proof: Define

$$\Lambda_i(k) = \sum_{t=1}^{k} \lambda(y_i(t)), \tag{23}$$

and

$$\Lambda(k) \triangleq [\Lambda_1(k) \quad \Lambda_2(k) \quad \cdots \quad \Lambda_m(k)], \tag{24}$$

where $\Lambda_i(k)$ is defined in (23). Since the attacker can only manipulate up to n sensors, $||\Lambda(k) - \Lambda'(k)||_0 \leq n$. From Lemma 1, we have

$$\min_{m-2n}(\Lambda(k)) \leq \underset{m-2n}{\text{med}}\,(\Lambda'(k)) \leq \max_{m-2n}(\Lambda(k)). \tag{25}$$

Consider the situation when the true state $\theta = 0$. Following the above strategy f^*, the system will make a wrong decision if $\text{med}_{m-2n}(\Lambda'(k)) \geq 0$. As a result,

$$\begin{aligned} e(\theta=0, \mathcal{I}, k) &= \mathbb{P}_0(\underset{m-2n}{\text{med}}\,(\Lambda'(k)) \geq 0) \\ &\leq \mathbb{P}_0(\max_{m-2n}(\Lambda(k)) \geq 0), \end{aligned}$$

where the inequality comes from (25).

Notice that $\max_{m-2n}(\Lambda(k)) \geq 0$ if and only if there exists an index set $\mathcal{K}$ with cardinality $m-2n$, i.e., $|\mathcal{K}| = m-2n$ such that

$$\sum_{i\in\mathcal{K}} \Lambda_i(k) \geq 0.$$

As a result,

$$\begin{aligned} e(\theta=0, \mathcal{I}, k) &\leq \mathbb{P}_0\left(\bigcup_{|\mathcal{K}|=m-2n} \left\{\sum_{i\in\mathcal{K}} \Lambda_i(k) \geq 0\right\}\right) \\ &\leq \sum_{|\mathcal{K}|=m-2n} \mathbb{P}_0\left(\sum_{i\in\mathcal{K}} \Lambda_i(k) \geq 0\right) \\ &= \binom{m}{2n} \mathbb{P}_0\left(\sum_{i=1}^{m-2n} \Lambda_i(k) \geq 0\right), \end{aligned}$$

where the last equality holds because of the symmetry between sensors.

By Cramer's theorem [17],

$$-\limsup_{k\to\infty} \frac{\log \mathbb{P}_0(\sum_{i=1}^{m-2n} \Lambda_i(k) \geq 0)}{k} = (m-2n)C.$$

Therefore,

$$-\limsup_{k\to\infty} \frac{\log e(\theta=0, \mathcal{I}, k)}{k} \geq (m-2n)C. \tag{26}$$

Similarly, one can prove that

$$-\limsup_{k\to\infty} \frac{\log e(\theta=1, \mathcal{I}, k)}{k} \geq (m-2n)C. \tag{27}$$

Combining the two inequalities (26) and (27), we get the conclusion that

$$\rho(f^*, g) \geq (m-2n)C.$$

■

B. Optimal Attack Strategy

We consider the attack strategy g^* which flips the distribution of the compromised sensor measurements. Formally it is defined as follows:

1) The attacker generates i.i.d. random variables $y_i'(k)$, where $i = 1, \cdots, m$ and $k = 1, \cdots$, such that the distribution of $y_i'(k)$ satisfies

$$\mathbb{P}(y_i'(k) \in S) = \begin{cases} \mu(S) & \text{if } \theta = 0 \\ \nu(S) & \text{if } \theta = 1 \end{cases}. \tag{28}$$

2) Compute $y_i^a(k)$ as follows:

$$y_i^a(k) = \begin{cases} y_i'(k) - y_i(k) & \text{if } i \in \mathcal{I} \\ 0 & \text{if } i \notin \mathcal{I} \end{cases}. \tag{29}$$

***Theorem** 2:* For any detection strategy f, the following inequality holds:

$$\rho(f, g^*) \leq (m-2n)C.$$

Proof: Consider the following two cases:

1) True state $\theta = 0$ and sensor $1, 2, ..., n$ are compromised. In this case, at each time k, the sensor measurement $y(k)$ follows the following distribution:

$$y(k) \sim \underbrace{\mu \times \cdots \times \mu}_{n} \times \underbrace{\nu \times \cdots \times \nu}_{n} \times \underbrace{\nu \times \cdots \times \nu}_{m-2n}.$$

2) True state $\theta = 1$ and and sensor $n+1, n+2, ..., 2n$ are compromised. In this case, at each time k, the sensor measurement $y(k)$ follows the following distribution:

$$y(k) \sim \underbrace{\mu \times \cdots \times \mu}_{n} \times \underbrace{\nu \times \cdots \times \nu}_{n} \times \underbrace{\mu \times \cdots \times \mu}_{m-2n}.$$

We use the probability measure μ_a and ν_a to denote the distribution of $y(k)$ in above two cases, respectively. Notice that for both cases, sensor 1 to sensor n will follow the distribution μ, and sensor $n+1$ to sensor $2n$ will follow the distribution ν.

Preprint submitted to 56th IEEE Conference on Decision and Control.
Received March 20, 2017.

Now we consider the following optimization problem which intends to minimize the probability of error in the above two cases:

$$\min \ \ \mathbb{P}_{\mu_a}(\hat{\theta}=1)+\mathbb{P}_{\nu_a}(\hat{\theta}=0), \tag{30}$$

where the first term indicates the probability of detection error in the first case, and the second term denotes this probability in the second case.

It is well known optimal solution for (30) is the Bayes detector which is defined as follows [18]:

$$f_{\mathrm{B}}(Y'(k))=\begin{cases}0 & \text{if } \sum_{i=2n+1}^{m}\Lambda_i'(k)<0\\ 1 & \text{if } \sum_{i=2n+1}^{m}\Lambda_i'(k)\geq 0\end{cases}.$$

Furthermore,

$$\begin{aligned}&\liminf_{k\to\infty}\frac{\log(\mathbb{P}_{\mu_a}(\hat{\theta}=1)+\mathbb{P}_{\nu_a}(\hat{\theta}=0))}{k}\\ =&\liminf_{k\to\infty}\frac{\log(e(\theta=0,\mathcal{I},k)+e(\theta=1,\mathcal{I},k))}{k}\\ =&\liminf_{k\to\infty}\log\frac{\log(\max_\theta(e(\theta,\mathcal{I},k)))}{k}.\end{aligned}$$

As a result, Bayes detector is also optimal in the sense that the rate $\rho(f,g^*)$ is maximized. Notice that this optimal detector only relies on the measurements from sensor $2n+1$ to sensor m for its decision. From Cramer's theorem [17],

$$-\limsup_{k\to\infty}\frac{\log\mathbb{P}_0(\sum_{i=2n+1}^{m}\Lambda_i'(k)\geq 0)}{k}=(m-2n)C,$$

and

$$-\limsup_{k\to\infty}\frac{\log\mathbb{P}_1(\sum_{i=2n+1}^{m}\Lambda_i'(k)<0)}{k}=(m-2n)C,$$

Therefore, Bayes detector will distinguish the above two cases with the rate $(m-2n)C$. Because of its optimality, no detector can distinguish the above two cases with better than this rate against g^*. In other words, for any detection strategy f,

$$\rho(f,g^*)\leq(m-2n)C.$$

■

One can further prove that under such attacks, the best rate $(m-2n)C$ can also be achieved by the optimal detection strategy f^* defined in (20)-(22). As a result, from Theorem 1 and Theorem 2, we can immediately derive the following theorem:

***Theorem** 3:* The strategy pair (f^*,g^*) forms a Nash-equilibrium such that

$$\rho(f,g^*)\leq\rho(f^*,g^*)\leq\rho(f^*,g),$$

where f^* is the optimal detection strategy defined in (20)-(22), g^* is the optimal attack strategy defined in (28)-(29), and $\rho(f^*,g^*)=(m-2n)C$.

***Remark** 6:* Since f^* in (20)-(22) does not depend on the knowledge of the attacker, and g^* in (28)-(29) only requires the attacker's knowledge of the compromised sensors' measurements. Hence, equilibrium strategy pair in Theorem 3 can be achieved by even the weak attacker.

IV. EQUILIBRIUM STRATEGIES FOR $m\leq 2n$

In this section, we consider the case when more than half of the sensors are compromised.

We begin with the attack strategy g^* defined as below:

1) The attacker generates i.i.d. random variables $y_i'(k)$, where $i=1,\cdots,m$ and $k=1,\cdots$, such that

$$\mathbb{P}(y_i'(k)\in S)=\begin{cases}\mu(S) & \text{if } \theta=0\\ \nu(S) & \text{if } \theta=1\end{cases}. \tag{31}$$

2) Compute $y_i^a(k)$ as follows:

If $\theta=0$,

$$y_i^a(k)=\begin{cases}y_i'(k)-y_i(k) & \text{if } i\in\mathcal{J}_1\\ 0 & \text{if } i\notin\mathcal{J}_1\end{cases}; \tag{32}$$

If $\theta=1$,

$$y_i^a(k)=\begin{cases}y_i'(k)-y_i(k) & \text{if } i\in\mathcal{J}_2\\ 0 & \text{if } i\notin\mathcal{J}_2\end{cases}, \tag{33}$$

where $\mathcal{J}_1,\mathcal{J}_2$ are the subsets of the compromised sensors set when $\theta=0$ and $\theta=1$, respectively, with $|\mathcal{J}_1|=\lceil\frac{m}{2}\rceil$, and $|\mathcal{J}_2|=\lfloor\frac{m}{2}\rfloor$.

In other words, under g^*, the attacker will flip the measurements' distribution of sensors in set $\mathcal{J}_1,\mathcal{J}_2$, when $\theta=0$ and 1, respectively.

***Remark** 7:* The reason why the adversary will not implement the same strategy as (28)-(29) in the situation $m\leq 2n$ is that under such attacks, the detector can easily figure it out by simply flipping the compromised sensors' measurements back if it knows the strategy of the adversary. Thus, the detection rate ρ would not be minimized.

***Theorem** 4:* For any detection strategy f, the following inequality holds:

$$\rho(f,g^*)=0.$$

Proof: Consider the following two cases:

1) True state $\theta=0$, $\mathcal{I}=\{1,\ \cdots,\ n\}$, and $\mathcal{J}_1=\{1,\ \cdots,\ \lceil m/2\rceil\}$, then the distribution of the sensor measurement $y(k)$ at each time k is as follows:

$$y(k)\sim\underbrace{\mu\times\mu\times\cdots\times\mu}_{\lceil\frac{m}{2}\rceil}\times\underbrace{\nu\times\nu\times\cdots\times\nu}_{m-\lceil\frac{m}{2}\rceil}.$$

2) True state $\theta=1$, $\mathcal{I}=\{m-n+1,\ \cdots,\ m\}$, and $\mathcal{J}_2=\{\lceil m/2\rceil+1,\ \cdots,\ m\}$, then the distribution of the sensor measurement $y(k)$ at each time k is as follows:

$$y(k)\sim\underbrace{\mu\times\mu\times\cdots\times\mu}_{\lceil\frac{m}{2}\rceil}\times\underbrace{\nu\times\nu\times\cdots\times\nu}_{m-\lceil\frac{m}{2}\rceil}.$$

Since the distribution of $y(k)$ is identical, no detector can distinguish the above two cases. Therefore, Theorem 4 follows immediately.

■

From Theorem 4, we have the next theorem:

Preprint submitted to 56th IEEE Conference on Decision and Control.
Received March 20, 2017.

***Theorem** 5:* For any detection strategy f, the strategy pair (f, g^*) forms a Nash-equilibrium such that

$$\rho(f, g^*) = 0 \leq \rho(f, g),$$

where g^* is the attack strategy defined in (31)-(33).

Proof: The proof of Theorem 5 is obvious since ρ is always nonnegative. ■

V. EXTENSION

In practice, the attacker may not present consistently. Thus, the system with all sensors uncompromised may operate for some time. As a result, we are interested in what the performance, i.e., detection rate, of the system will be under proposed detection strategy when there are no sensors being compromised.

***Theorem** 6:* Under the detection rule (20)-(22), when all the sensors are benign, the detector will achieve the detection rate of $(m-n)C$.

Proof: Since there is no attacker in this situation, we will use $\rho(f^*)$ rather than $\rho(f^*, g)$ to denote the detection rate.

Consider the situation when $\theta = 0$. Notice that

$$\begin{aligned} e(\theta = 0, \mathcal{I} = \emptyset, k) &= \mathbb{P}_0(\operatorname*{med}_{m-2n}(\Lambda'(k)) \geq 0) \\ &= \mathbb{P}_0(\operatorname*{med}_{m-2n}(\Lambda(k)) \geq 0) \\ &= \mathbb{P}_0(s(\Lambda(k), n+1, m-n) \geq 0). \end{aligned}$$

Hence, we are interested in the probability of the event $\{s(\Lambda(k), n+1, m-n) \geq 0\}$.

We first prove that $\rho(f^*)$ is lower bounded by the rate $(m-n)C$.

Notice that

$$\begin{aligned} e(\theta = 0, \mathcal{I} = \emptyset, k) &= \mathbb{P}_0(s(\Lambda(k), n+1, m-n) \geq 0) \\ &\leq \mathbb{P}_0(s(\Lambda(k), n+1, m) \geq 0) \\ &\leq \binom{m}{n} \mathbb{P}_0\left(\sum_{i=1}^{m-n} \Lambda_i(k) \geq 0\right). \end{aligned}$$

From Cramer's theorem [17],

$$-\limsup_{k\to\infty} \frac{\log \mathbb{P}_0(\sum_{i=1}^{m-n} \Lambda_i(k) \geq 0)}{k} = (m-n)C.$$

As a result,

$$-\limsup_{k\to\infty} \frac{\log e(\theta = 0, \mathcal{I}, k)}{k} \geq (m-n)C.$$

The similar result can also be get under the condition that $\theta = 1$. Therefore,

$$\rho(f^*) \geq (m-n)C. \tag{34}$$

Then we further prove that $\rho(f^*)$ is also upper bounded by the rate $(m-n)C$.

We assume $\mathbb{P}_0(\Lambda_i(k) \geq 0) = M$. From Cramer's theorem [17], we have

$$-\limsup_{k\to\infty} \frac{\log M}{k} = C. \tag{35}$$

Notice that if $\Lambda_1(k) < 0, \cdots, \Lambda_n(k) < 0$, and $\Lambda_{n+1}(k) \geq 0, \cdots, \Lambda_m(k) \geq 0$, then the considered event $\{s(\Lambda(k), n+1, m-n) \geq 0\}$ will happen. Therefore, the probability of this event is lower bounded by $\binom{m}{n} M^{m-n}(1-M)^n$. As a result,

$$\begin{aligned} &-\limsup_{k\to\infty} \frac{\log e(\theta = 0, \mathcal{I} = \emptyset, k)}{k} \\ &\leq -\limsup_{k\to\infty} \frac{\log\left(\binom{m}{n} M^{m-n}(1-M)^n\right)}{k} \\ &= (m-n)C. \end{aligned}$$

Similarly, one can prove that

$$\limsup_{k\to\infty} \frac{\log e(\theta = 1, \mathcal{I} = \emptyset, k)}{k} \leq (m-n)C.$$

As a result,

$$\rho(f^*) \leq (m-n)C. \tag{36}$$

Combining inequalities (34) and (36), one can immediately get

$$\rho(f^*) = (m-n)C.$$

■

***Remark** 8:* We notice that the rate in Theorem 6 is not optimal because $\rho(f)$ is not maximized, since one can prove that if the attacker is absent, then the Bayes detector [18] will achieve the best rate of mC. Usually, the performance of the detection rule when there is no attacker at all is referred to by efficiency, while the performance when the attacker is present is referred to by security. Therefore, in order to increase the security of the system, we sacrifice the system's efficiency to some degree. The parameter n can be interpreted as how many bad sensors can the system tolerate, which is a design parameter. One can further derive that the larger the n is, the more resilient the detector will be under attacks, but at the same time, the more performance degradation will occur during normal operation when the attacker is absent. Therefore, there exists a trade-off between security and efficiency, which can be tuned by choosing a suitable parameter n.

VI. SIMULATION

In this section, we provide numerical examples to verify the theoretical results established in the previous sections. We assume that the sensor's measurement $\{y_i(k)\}_{i=1,\ldots,m,k=1,\ldots}$ follows the distribution $\mathcal{N}(-1,1)$[1] when $\theta = 0$, and follows $\mathcal{N}(1,1)$ when $\theta = 1$. From (15), one can derive that the optimal decay rate of a single sensor is $C = 0.5$.

Since the situation when $m \leq 2n$ is trivial, we only focus on the case where $m > 2n$. We first assume $m = 7$, and n varies from 0 to 3. Fig. 1 shows that under the detection strategy f^* defined in (20)-(22) and attack strategy g^* defined in (28)-(29), the detection rate $\rho(f^*, g^*)$ finally approaches $0.5(m-2n)$, i.e., $(m-2n)C$, which are consistent with our result.

[1] $\mathcal{N}(a, b)$ represents the Gaussian distribution with mean equals to a, and variance equals to b.

Preprint submitted to 56th IEEE Conference on Decision and Control.
Received March 20, 2017.

If the detector adopts the detection rule (20)-(22) and is designed to tolerate n bad sensors, but the attacker is absent in practice, then the system's performance is further studied. Specifically, we assume $m = 7$, $n = 3$. Fig. 2 indicates that the system will eventually achieve the rate of $(m-n)C = 2$, which is proved in Theorem 6.

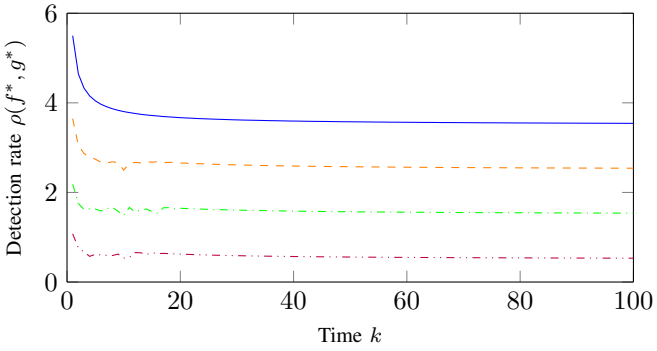

Fig. 1. Detection rate under optimal strategy pair when $m = 7$ and $m > 2n$ for $n = 0$ (blue solid line), $n = 1$ (red dashed line), $n = 2$ (green dash dot line) and $n = 3$ (purple dash dot dot line).

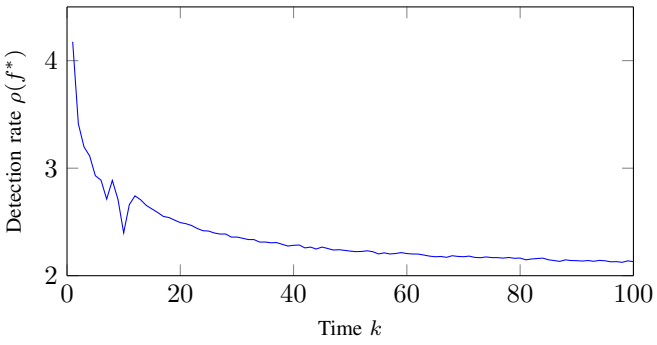

Fig. 2. Detection rate under optimal detection strategy when $m = 7, n = 3$, and all sensors are benign.

VII. CONCLUSION

In this paper, we consider the equilibrium strategy of sequential detection in adversarial environment. In our problem, the attacker intends to deteriorate the detection performance, and the detector needs to be designed to minimize the probability of detection error. We study both cases where $m > 2n$ and $m \leq 2n$, and obtain an equilibrium strategy pair of detection rule and attack scheme for both cases. Furthermore, the system's performance of our strategy when all sensors are benign is investigated. The future work involves the trade-off between system's security and efficiency.

REFERENCES

[1] J.-Y. Ding, K. You, S. Song, and C. Wu, "Likelihood ratio based scheduler for secure detection in cyber physical systems," *IEEE Transactions on Control of Network Systems*, vol. PP, 2017.
[2] A. A. Cardenas, S. Amin, and S. Sastry, "Secure control: Towards survivable cyber-physical systems," in *Distributed Computing Systems Workshops, 2008. ICDCS'08. 28th International Conference on*. IEEE, 2008, pp. 495–500.
[3] R. Gibbons, *A primer in game theory*. Harvester Wheatsheaf, 1992.
[4] D. Reinhard, M. Fauß, and A. M. Zoubir, "An approach to joint sequential detection and estimation with distributional uncertainties," in *Signal Processing Conference (EUSIPCO), 2016 24th European*. IEEE, 2016, pp. 2201–2205.
[5] F. Bayat and S. Wei, "Sequential detection of disjoint subgraphs over boolean mac channels: A probabilistic approach," in *Globecom Workshops (GC Wkshps), 2016 IEEE*. IEEE, 2016, pp. 1–6.
[6] A. Wald and J. Wolfowitz, "Optimum character of the sequential probability ratio test," *The Annals of Mathematical Statistics*, pp. 326–339, 1948.
[7] S. R. G. C. University, *Sequential analysis of statistical data: Applications*. Columbia University Press, 1963.
[8] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," *Ad hoc networks*, vol. 1, no. 2, pp. 293–315, 2003.
[9] R. Lu, X. Lin, H. Zhu, X. Liang, and X. Shen, "Becan: a bandwidth-efficient cooperative authentication scheme for filtering injected false data in wireless sensor networks," *IEEE transactions on parallel and distributed systems*, vol. 23, no. 1, pp. 32–43, 2012.
[10] F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical en-route filtering of injected false data in sensor networks," *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 4, pp. 839–850, 2005.
[11] J. H. Marburger, E. F. Kvamme, G. Scalise, and D. A. Reed, "Leadership under challenge: Information technology r&d in a competitive world. an assessment of the federal networking and information technology r&d program," DTIC Document, Tech. Rep., 2007.
[12] R. Chabukswar and B. Sinopoli, "Secure detection with correlated binary sensors," in *American Control Conference (ACC), 2015*. IEEE, 2015, pp. 3874–3879.
[13] S. Bayram and S. Gezici, "On the restricted neyman–pearson approach for composite hypothesis-testing in presence of prior distribution uncertainty," *IEEE Transactions on Signal Processing*, vol. 59, no. 10, pp. 5056–5065, 2011.
[14] 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, 2014.
[15] 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, 2014.
[16] H. Chernoff, "A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations," *The Annals of Mathematical Statistics*, pp. 493–507, 1952.
[17] U. SCHMOCK, "Large deviations techniques and applications," *Journal of the American Statistical Association*, vol. 95, no. 452, pp. 1380–1380, 2000.
[18] J. O. Berger, "Statistical decision theory and bayesian analysis," 1985.

Preprint submitted to 56th IEEE Conference on Decision and Control.
Received March 20, 2017.