Secure Detection with Correlated Binary Sensors

Rohan Chabukswar[1] and Bruno Sinopoli[2]

Abstract— **Sensor networks use binary measurements and state estimations for several reasons, including communication and processing overheads. Such a state estimator is vulnerable to attackers that can hijack a subset of the sensors in an effort to change the state estimate. After exhibiting a simulation that demonstrates the possible effect of integrity cyberphysical systems, this paper extends the authors' methodology for designing the detectors resilient to integrity attacks, using the concept of invariant sets, to systems where the sensor measurements are not independent. In cyberphysical systems, the sensors in question monitor a system constrained to obey physical laws, so that physical quantities measured by and the noise in each sensor will be correlated to the sensors close to it. Further increase in the confidence of the estimate can be achieved by considering these correlations. This paper focuses on modeling the correlation between the sensors and its ramifications on the worst-case probability of detection.**

I. INTRODUCTION

Cyber-Physical systems (CPS) often employ distributed networks of embedded sensors and actuators [1] that interact with the physical environment, and are monitored and controlled by a Supervisory Control and Data Acquisition (SCADA) system. Distributed sensors and actuator networks are seen in applications like critical infrastructure monitoring, autonomous vehicle control, healthcare, etc.

Given the ubiquity of cyber-physical systems, and the importance their confidentiality, integrity, and availability, it is easy to see why they are a rich target for attacks. The incentives for attack could range from simple economic reasons and advantage over industrial competitors, to political espionage and sabotage and full-fledged terrorism. With the advent of increasingly "smart" CPS and deployment of an increasing number of sensors to remote locations where enforcing their security is infeasible, isolation of CPS networks and controllers from the Internet can only offer a limited amount of protection.

Additionally, in the recent past, human errors have helped attackers to introduce malware into heavily secured and isolated networks. For example, the Stuxnet worm, which was designed to secretly reprogram certain industrial centrifuges [2], was introduced by infected USB flash drives [3], and further used peer-to-peer calls to infect other computers inside private networks [4]. Clearly, isolation of networks and components, and in general, security with obscurity, is only a short-term solution. The Stuxnet worm has indubitably brought to light serious security susceptibilities in industrial control systems. This attack resonated with a recent concern in distributed control system security, whereby an attacker could modify the software or environment of some of the networked sensors and/or actuators, to launch a coordinated attack against the system infrastructure.

Another mitigating measure is the use of cryptography. Theft and reverse-engineering of cryptographic keys notwithstanding, an attacker could still attack the physical environment of the components, bypassing the communication network entirely. There are other methods of approaching CPS security, most of which rely either on the information content of the system or on the robustness of controllers and estimation and detection algorithms. Concentrating on the information content lacks a system model, blinding the detector to a wide variety of attacks (for example, lowering electricity bills by bypassing the meter). On the other hand, robust controllers and algorithms rely on outliers, whereas random, uncoordinated failures can hardly be assumed during an attack.

After briefly demonstrating the need to secure cyberphysical systems against integrity attacks, this paper looks at the problem of secure detection for a system with a binary state and correlated binary sensors. For systems using a multitude of distributed sensors for detecting a binary state, it is often superfluous to consider continuous readings from all sensors, and in fact, might prove to be infeasible for both sparse and low-powered communication networks, as well as small embedded processors. It is usual on such a platform for the sensors to be programmed to make a decision based on the information they have, and only communicate this decision over the network, reducing the communication overhead. The controller then makes a decision based on these preliminary decisions.

Considerable research, notably by Maronna et al. [5] and Huber and Ronchetti [6], has been devoted to constructing estimators that are not unduly affected by outliers or other small departures from model assumptions , which can be used to nullify the effect of outliers. However, the case of an attack is quite different from randomly occurring outliers, and such methods need to be reformulated for CPS. Bad data detection has been used in power grids for a long time as mentioned by Abur and Expósito [7]. Liu et al. [8] and

This research was supported in part by CyLab at Carnegie Mellon by grant DAAD19-02-1-0389 from the Army Research Office, grant NGIT2009100109 from the Northrop Grumman Information Technology, Inc. Cybersecurity Consortium, and grant 0955111 from the National Science Foundation. The views and conclusions contained here are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either express or implied, of ARO, CMU, CyLab, NSF, NGC, or the U.S. Government or any of its agencies.

[1]Rohan Chabukswar was with the Department of Electrical and Computer Engineering of Carnegie Mellon University, Pittsburgh, PA, United States when this work was done. rohanchabukswar@gmail.com

[2]Bruno Sinopoli is with the Department of Electrical and Computer Engineering of Carnegie Mellon University, Pittsburgh, PA, United States. brunos@ece.cmu.edu

Sandberg et al. [9] consider how an attacker can design and inject inputs into measurements to change state estimation results.

A system similar to the theoretical model in this paper has been previously studied by Agah et al. [10], Alpcan and Başar [11], Fuchs and Khargonekar [12], and later by Vamvoudakis et al. [13], by formulating the problem as a zero-sum partial information game in which a detector attempts to minimize the probability of error and an attacker attempts to maximize this probability. The optimal policy recommended by the authors in the latter work is a mixed strategy, where the detector chooses between two rules, based on the perceived probability of attack. This policy is dependent on the estimation of this probability of attack, which, for a lot of systems, is not only extremely difficult to analyze and estimate, but might also change widely based on several external factors.

Kodialam and Lakshman [14] also modeled intrusion detection as a zero-sum game, albeit between the service provider and the intruder. Other game-theoretical approach to solving the problem have been proposed by Bier et al. [15], who used the method increasing the attractiveness of some sensors to the attacker, while designating others as unimportant. The chief drawback of game-theoretical approaches is that the final detection output is possibly a mixed strategy, and not a function of just the inputs. That is, for the same inputs, the detector output can change randomly based on which policy is chosen, a behavior that may be undesirable in many systems.

Robust detection with minimax have been previously studied by Huber [16], Huber and Strassen [17] and Kasam and Poor [18], using uncertainty classes and the detector being designed as a naive-Bayes or Neymann-Pearson detector. the challenge in such an approach is constructing the least favorable distributions in the uncertainty classes, which are the classes that are supposed to be the hardest for the detector to distinguish.

Seeking a deterministic solution, we consider the behavior of such a system in the presence of a powerful attacker, without looking to estimate a probability that the adversary will attack. We consider an attack model where the adversary can attack up to a certain number of sensors, while remaining undetected. After reviewing some previous results, we will reformulate the system to consider correlated sensor measurements and explore in more detail the case where all the sensors are equivalent.

II. PAPER CONTRIBUTION

This paper extends the previous results of the authors [19] by considering the physical correlation between the binary sensors. The correlation causes a change in the expressions of the worst-case probabilities of false-alarm and detection. Considering the extra factor while constructing the detector improves the resilience of the detector when attacked by an intelligent attacker. The paper considers methods for including correlation coefficients in the detector formulation, and shortcomings of some correlation assumptions that are usually made in literature, that can make some calculated probabilites negative. The paper provides a new way to ensure non-negativity of these probabilities. We conclude with a simulation that verifies the computations laid out in the paper.

III. BINARY SENSORS

In this section, we look at the problem of secure detection for a system with a binary state and binary sensors. Although a sensor giving out just one bit of information seems a trivialization of the integrity attack of the previous section, it is more than just a simplified version. For systems using a multitude of distributed sensors for detecting a binary state, it is often superfluous to consider continuous readings from all sensors, and in fact, might prove to be infeasible for both sparse and low-powered communication networks, as well as small embedded processors. It is usual on such a platform for the sensors to be programmed to make a decision based on the information they have, and only communicate this decision over the network, reducing the communication overhead. The controller then makes a decision based on these preliminary decisions.

First, the previous results proposed by the authors [19] for non-correlated binary sensors are reviewed.

A. Original Problem

Consider a binary random variable X, with distribution

$$X = \begin{cases} 0 & \text{with probability } P_0 \\ 1 & \text{with probability } P_1 \end{cases}, \tag{1}$$

where $P_0, P_1 \geq 0$, and $P_0 + P_1 = 1$. Without loss of generality, let $P_1 \geq P_0$.

To detect X, we have available a vector

$$y = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_m \end{pmatrix} \in \{0,1\}^m \tag{2}$$

of m binary sensor measurements, each of which is conditionally independent from the others given X. Let each sensor have a probability of false alarm (α)

$$P\left(y_i = 1 \middle| X = 0\right) = \alpha_i, \tag{3}$$
$$P\left(y_i = 0 \middle| X = 0\right) = 1 - \alpha_i, \tag{4}$$
$$i = 1, 2, \ldots, m,$$

and probability of detection (β)

$$P\left(y_i = 1 \middle| X = 1\right) = \beta_i, \tag{5}$$
$$P\left(y_i = 0 \middle| X = 1\right) = 1 - \beta_i, \tag{6}$$
$$i = 1, 2, \ldots, m.$$

If any of the sensors are actually such that $\alpha_i \geq \beta_i$ for some values of i, the measurements provided by those sensors can be inverted before being used, making $\alpha_i \leq \beta_i$. Thus, without a loss of generality, we can consider $\alpha_i \leq \beta_i \ \forall i$.

In the case where there is no attack, a Bayes detection algorithm suffices.

$$P_0 \prod_{i=1}^{m} \alpha_i^{y_i} (1-\alpha_i)^{(1-y_i)} \underset{H_0}{\overset{H_1}{\lessgtr}} P_1 \prod_{i=1}^{m} \beta_i^{y_i} (1-\beta_i)^{(1-y_i)} \quad (7)$$

where $H_0 \equiv \hat{X} = 0$ and $H_1 \equiv \hat{X} = 1$.

It is assumed that an attacker wants to increase the probability that the detector makes an error in detecting X. The attacker has the ability to flip up to l of the m sensor measurements, but the detector does not know which of the m measurements have been manipulated. While the detector knows that at most l measurements have been manipulated, the exact number is also unknown to the detector. This means that any detection scheme $\hat{X} = f(y)$ has to rely on the original measurement vector (y) manipulated by the attack vector (y^a)

$$y^c = y \oplus y^a, \quad (8)$$

where $y^a \in \{0,1\}^m$, and $\|y^a\| \leq l$. [1] Here $\oplus$ denotes the element-wise exclusive-or operation. By selecting which bits of y^a are 1, the attacker chooses which sensors to attack.

Remark 1: For the purposes of this paper, resiliency is defined as a low probability of error in the worst-case scenario. Thus, resiliency can be considered to be equivalent to the worst-case probability of detection.

The detection problem is formalized as a minimax problem where one wants to select an optimal detector

$$\hat{X} = f(y^c) = f(y \oplus y^a), \quad (9)$$

to minimize the probability of error (or maximize the worst-case probability of detection).

To have the detector follow the Kerckhoffs' Principle which states that, a cryptosystem should be secure even if everything about the system (except the key) is public knowledge, we assume that the attacker has full knowledge about f, the state of the system X, and all measurements $y_1, y_2, \ldots, y_m$.

Using the concept of imperturbable sets Y_0 and Y_1 (the sets of measurements y that, even when attacked, will not affect the output of the detection function f):

$$Y_0 = \left\{ y \middle| f(y \oplus y^a) = 0, \forall y^a \in \{0,1\}^m, \|y^a\| \leq l \right\}, \quad (10)$$

$$Y_1 = \left\{ y \middle| f(y \oplus y^a) = 1, \forall y^a \in \{0,1\}^m, \|y^a\| \leq l \right\}, \quad (11)$$

as derived in the previous work [19], the problem of finding the optimal detector can be formally stated as

$$\max_{Y_0, Y_1} \quad P_0 \sum_{y \in Y_0} \left(\prod_{i=1}^{m} \alpha_i^{y_i} \cdot \prod_{i=1}^{m} (1-\alpha_i)^{(1-y_i)} \right) + P_1 \sum_{y \in Y_1} \left(\prod_{i=1}^{m} \beta_i^{y_i} \cdot \prod_{i=1}^{m} (1-\beta_i)^{(1-y_i)} \right) \quad (12)$$

$$\text{subject to} \quad d(Y_0, Y_1) \geq 2l + 1, \quad (13)$$

[1] Since only binary states and sensor measurements are concerned, both the 0-norm and the 1-norm are equivalent. Hence, for legibility, the subscript is dropped with the understanding that it can be either the 0-norm or the 1-norm.

where,

$$d(a,b) = \|a - b\|, \quad (14)$$

$$d(a,B) = \min_{b \in B} \|a - b\|, \quad (15)$$

$$d(A,B) = \min_{a \in A} \|a - B\| = \min_{a \in A, b \in B} \|a - b\|. \quad (16)$$

IV. MODELING THE CORRELATION

In cyberphysical systems, the sensors in question monitor a physical system — a system that is constrained to obey physical laws. In such a case, the physical quantities measured by all sensors can scarcely be independent of each other. The measurements and the noise of each sensor will be correlated to the sensors close to it. This section focuses on modeling the correlation between the sensors and its ramifications on the worst-case probability of detection.

Consider the same set of m binary sensors $y_1, y_2, \ldots, y_m$ as the previous section with probabilities of false alarm and detection. However, for the rest of the paper, the measurements from each of the sensors will not be considered to be independent.

It is safe to assume that the correlation coefficient between the sensors is constant, irrespective of the state of the system (X). In the cases where this assumption isn't true, the correlation of the sensor measurements could be considered separately when $X = 1$ and $X = 0$. Since the derivations are similar, for cleanliness of notation during the rest of the section, the value of the state X will not be specified. The probabilities will instead be denoted as

$$P(y_i = 1) = p_i, \quad (17)$$

$$P(y_i = 0) = 1 - p_i, \quad (18)$$

$$i = 1, 2, \ldots, m.$$

with the understanding that, if $X = 1$, $p_i = \beta_i$ and if $X = 0$, $p_i = \alpha_i$ for all $i = 1, 2, \ldots, m$.

Now, since the assumption is that the probabilities p_i need not be independent, for some $1 \leq i_1 < i_2 \leq m$, $E[y_{i_1} y_{i_2}] \neq E[y_{i_1}] E[y_{i_2}]$. In fact, since more than two variables can be interdependent, for some $1 \leq i_1 < i_2 < \ldots < i_k \leq m$, $1 < k \leq m$,

$$E[y_{i_1} y_{i_2} \ldots y_{i_k}] \neq E[y_{i_1}] E[y_{i_2}] \ldots E[y_{i_k}]. \quad (19)$$

The correlation coefficient r_{ij} is defined as

$$r_{ij} = \frac{E[y_i y_j] E[(1-y_i)(1-y_j)]}{\sqrt{E[y_i] E[1-y_i] E[y_j] E[1-y_j]}} - \frac{E[y_i (1-y_j)] E[(1-y_i) y_j]}{\sqrt{E[y_i] E[1-y_i] E[y_j] E[1-y_j]}}. \quad (20)$$

Using $E[y_i] = p_i$ and simplifying the expectations,

$$r_{ij} = \frac{E[y_i y_j] - p_i p_j}{\sqrt{p_i (1-p_i) p_j (1-p_j)}} = E[w_i w_j], \quad (21)$$

where

$$w_i = \frac{y_i - p_i}{\sqrt{p_i (1 - p_i)}}. \tag{22}$$

Similarly, the higher correlation coefficients can also be calculated as

$$r_{i_1 i_2 \ldots i_k} = E\left[w_{i_1} w_{i_2} \ldots w_{i_k}\right]. \tag{23}$$

As derived by Bahadur [20], the joint probability for a measurement vector $Y = (y_1, y_2, \ldots, y_m)$ can then be written as

$$P(y_1, y_2, \ldots, y_m) = \prod_{i=1}^{m} p_i^{y_i} (1 - p_i)^{1 - y_i} h(y_1, y_2, \ldots, y_m), \tag{24}$$

where

$$\begin{aligned} h(y_1, y_2, \ldots, y_m) = 1 &+ \sum_{j<k} r_{jk} w_j w_k \\ &+ \sum_{j<k<l} r_{jkl} w_j w_k w_l + \ldots \\ &+ r_{12\ldots m} w_1 w_2 \ldots w_m. \end{aligned} \tag{25}$$

This is the probability, calculated by substituting α_1 and β_i for p_i, that causes the manifestation of the factor $h(y_1, y_2, \ldots, y_m)$ in the worst-case probability of detection P of Equation (12):

$$\begin{aligned} P = P_0 \sum_{y \in Y_0} \left(h_\alpha (y_1, y_2, \ldots, y_m) \prod_{i=1}^{m} \alpha_i^{y_i} (1 - \alpha_i)^{(1 - y_i)} \right) \\ + P_1 \sum_{y \in Y_1} \left(h_\beta (y_1, y_2, \ldots, y_m) \prod_{i=1}^{m} \beta_i^{y_i} (1 - \beta_i)^{(1 - y_i)} \right). \end{aligned} \tag{26}$$

It can be seen that the correlation factor can significantly affect the worst-case probability of detection, and hence the solution of the optimization problem. Even when the solution remains unchanged, the correlations r between the sensors will increase the worst-case probability of detection, improving the detector performance.

For m greater than 4 or 5, computing this distribution can become infeasible. One of the assumptions that are usually made (Emrich and Piedmonte [21]), is that some of the higher order correlation coefficients $r_{jkl\ldots}$ are zero. The problem with this assumption is that since $r_{jkl\ldots}$ need to satisfy linear inequalities determined by the marginal expectations, they are not free to vary over $[-1, 1]$. Thus by assuming $r_{jkl\ldots}$ are zero, the values of h at some measurement vectors might be negative.

In the next section we propose a method to overcome this problem by using a different assumption.

V. CORRELATION ASSUMPTIONS

Zero is as arbitrary a value for the correlation coefficient as any. In fact, assuming $r_{jkl\ldots}$ are zero could potentially make $h(y_1, y_2, \ldots, y_m)$ negative for some values of $y_1, y_2, \ldots, y_m$. In order to avoid this, we propose that the correlation coefficient be set in the following roundabout manner, such that $h(y_1, y_2, \ldots, y_m)$ is guaranteed to be non-negative.

Remark 2: If the problem specifies as many values of $r_{jkl\ldots}$ as are possible, the remaining values can be made to be consistent. It is easy to see that if all values of $r_{jkl\ldots}$ are not specified, the parameter space is incomplete, and can be filled in many ways. Several methods have been proposed to generate binary random variables that have the given correlation values — for example, Emrich and Piedmonte [21], and Lunn and Davies [22]. A method that generates random variables of given 2-correlations by using Poisson processes is proposed by Park et al. [23]. Intuitively, if a large number of random variables of the given 2-correlations are generated, consistent higher order correlations can be accrued by calculating the higher order correlations of these generated samples. The accuracy of the calculated correlations depends on the size of the sample — for true values, an infinite sample size would be needed.

The key idea behind the paper is that such a sample does not need to be generated. If an appropriate method to generate the samples is chosen, the characteristics the method can be used to generate the higher-order correlation values algebraically. The actual calculated value will depend on the exact generation method used, but this roundabout manner assures us that any calculated value will be consistent with the specified values. The quality and characteristics of the calculated value, then, are equivalent to those of the generation method used. The comparison of the different methods is beyond the scope of this paper, however, it can be assumed that the method that generates samples with parameters closest to the sensor correlation values will be better suited for constructing the detector.

A. Example

Consider $m = 3$ with $p_1 = 0.9$, $p_2 = 0.8$, $p_3 = 0.7$, and the 2-correlation coefficients are given as $r_{12} = 0.1$, $r_{13} = 0.5$ and $r_{23} = 0.5$. Given the 2-correlations, the generation method by Park et al. [23] can be chosen.[2] Applying the method, we get

$$z_1 = \mathcal{P}_1 + \mathcal{P}_2 + \mathcal{P}_3 \tag{27}$$

$$z_2 = \mathcal{P}_1 + \mathcal{P}_4 + \mathcal{P}_5 \tag{28}$$

$$z_3 = \mathcal{P}_1 + \mathcal{P}_2 + \mathcal{P}_4 + \mathcal{P}_6, \tag{29}$$

where

$$\mathcal{P}_1 = \text{Poisson}(\theta_1 = 0.0165), \tag{30}$$

$$\mathcal{P}_2 = \text{Poisson}(\theta_2 = 0.0870), \tag{31}$$

$$\mathcal{P}_3 = \text{Poisson}(\theta_3 = 0.0018), \tag{32}$$

$$\mathcal{P}_4 = \text{Poisson}(\theta_4 = 0.1350), \tag{33}$$

$$\mathcal{P}_5 = \text{Poisson}(\theta_5 = 0.0716), \tag{34}$$

$$\mathcal{P}_6 = \text{Poisson}(\theta_6 = 0.1181), \tag{35}$$

where $\text{Poisson}(\theta)$ denotes a Poisson process of intensity θ.

[2]The values are chosen to match one of the examples used by Park et al. [23].

The binary random variables y_1, y_2, and y_3 can be generated from z_1, z_2, and z_3:

$$y_i = \begin{cases} 1 & \text{if } z_i = 0 \\ 0 & \text{otherwise.} \end{cases} \tag{36}$$

This is the prescribed method for generation of the y_is. However, the y_is need not be actually generated to calculate the unspecified coefficients of correlation (in this case, only r_{123}). Using the definition of r_{123} from Equation (23),

$$r_{123} = \frac{E[y_1y_2y_3] - p_1p_2p_3}{\sqrt{p_1p_2p_3(1-p_1)(1-p_2)(1-p_3)}} - \sqrt{\frac{p_1}{1-p_1}}r_{23} - \sqrt{\frac{p_2}{1-p_2}}r_{13} - \sqrt{\frac{p_3}{1-p_3}}r_{12} \tag{37}$$

The value of $E[y_1y_2y_3]$ can be computed given the forms of y_1, y_2, and y_3. Since $y_1y_2y_3 = 1 \iff y_1 = y_2 = y_3 = 1 \iff z_1 = z_2 = z_3 = 0 \iff \mathcal{P}_1 = \mathcal{P}_2 = \ldots = \mathcal{P}_6 = 0$,

$$E[y_1y_2y_3] = \prod_{i=1}^{l} e^{-\theta_i}. \tag{38}$$

Performing the computations, $E[y_1y_2y_3] = e^{-0.4300} = 0.6505$, giving $r_{123} = 0.0109$.

Thus, if these processes were to generate y_1, y_2, and y_3, then the value of r_{123} would not be zero. Although assigning the computed value of 0.0109 to r_{123} of our sensors is exactly as arbitrary as assigning 0, the advantage here lies in the fact that as long as the 2-correlations are consistent, the higher correlations will also be consistent, enough to guarantee the non-negativity of $h(y_1, y_2, \ldots, y_m)$. All that remains is to use the higher correlation values to figure out the worst-case detection probability.

Given r_{123}, it's easy to compute h for different values of y_1, y_2 and y_3, which in turn can be used to calculate the joint probability of each measurement vector $P(y_1, y_2, y_3)$ of equation (24).

Y			h	Uncorrelated Probability	Correlated Probability
y_1	y_2	y_3			
0	0	0	5.3189	0.0060	0.0319
0	0	1	0.0062	0.0140	0.0001
0	1	0	2.7844	0.0240	0.0668
0	1	1	0.0210	0.0560	0.0012
1	0	0	2.2174	0.0540	0.1197
1	0	1	0.3830	0.1260	0.0483
1	1	0	0.3774	0.2160	0.0815
1	1	1	1.2906	0.5040	0.6505

TABLE I
JOINT PROBABILITY FOR MEASUREMENT VECTOR $Y = (y_1, y_2, y_3)$

Table I shows the calculation of h, and the uncorrelated and correlated probabilities. It can be seen that the change caused by h can be as high as a factor of 5. This will translate to a higher confidence in the sensor readings in the event of an integrity attack.

VI. SIMULATION

In our example system consisting of only three sensors, the number of sensors attacked can only be 1, constraining the sets Y_0 and Y_1 severely to $Y_0 = \{(0,0,0)\}$ and $Y_1 = \{(1,1,1)\}$, irrespective of the probabilities in question. Thus, the inclusion of h cannot change the detector. What does change in our system, however, is the confidence of the detector. Looking at the correlated and uncorrelated probabilities in table I, the probability that a measurement lies in $Y_0 \cup Y_1$ changes from 0.51 (almost half) to 0.6824 (better than 2/3), making the detector more resilient to attacks that change 1 measurement.

To verify this, N sets of 3 sensor measurements were generated. An intelligent attacker was assumed, who flips one sensor measurement if and only if it is going to cause a change in the detector output. Table II shows the results of the simulation, under the cases where the sensors are correlated and uncorrelated.

Sensors	N	Successful Attacks	Correct Detection Rate
Uncorrelated	1000	492	0.5080
Correlated	1000	319	0.6810
Uncorrelated	1000000	489757	0.5102
Correlated	1000000	317574	0.6824

TABLE II
SIMULATION RESULTS

It can be seen from table II that the rate of correct detection is higher in case of correlated sensors, using a detector that uses the fact that the sensors are correlated.

VII. ALL SENSORS EQUIVALENT

As was done in the previous work [19] with the case of uncorrelated sensors, this section focuses on the case where all sensors are equivalent, and all 2-correlations are the same.

If all sensors and 2-correlations are equivalent,

$$p_i = p,\ 1 \le i \le m, \tag{39}$$

$$r_{i,j} = r,\ 1 \le i < j \le m. \tag{40}$$

This uses a special case of the method given by Park et al. [23]. Using the simplification,

$$z_i = \mathcal{P} + \mathcal{P}_i, \tag{41}$$

where

$$\mathcal{P} = \text{Poisson}(\mu), \tag{42}$$

$$\mathcal{P}_i = \text{Poisson}(\nu - \mu), \tag{43}$$

where $\mu = \log\left(1 + r\frac{1-p}{p}\right)$ and $\nu = -\log p$. Thus, for $1 \le i_1, i_2, \ldots, i_k \le m$, where $1 < k \le m$, simplifying like the example in the last section,

$$E[y_{i_1}y_{i_2}\ldots y_{i_k}] = \frac{p^{2k-1}}{(p + r(1-p))^{k-1}}. \tag{44}$$

Thus, $E\left[y_{i_1} y_{i_2} y_{i_3}\right] = \frac{p^5}{(p+r(1-p))^2}$ can be used to generate the 3-correlations r_3 as

$$r_3 = \frac{\frac{p^5}{(p+r(1-p))^2} - p^3}{p^3 (1-p)^3} - 3r\frac{p}{1-p}. \tag{45}$$

These 3-correlations and $E\left[y_{i_1} y_{i_2} y_{i_3} y_{i_4}\right] = \frac{p^7}{(p+r(1-p))^3}$ can be further used to compute r_4, and so on.

VIII. CONCLUSIONS AND FUTURE WORK

The allowance of correlation among sensors allows for a more accurate modeling of a physical SCADA system, where the sensors are connected through measuring the same physical system, causing their outputs to be non-independent. This interdependence of the sensor values can be leveraged to improve the resilience of the detector in the event of an integrity attack on the system.

The increase in detection rate by considering the effects of correlation will boost the security of distributed sensor networks that employ binary variables. Future work will involve simulating or implementing such a SCADA system in order to demonstrate the effectiveness of the detector, and possibly implementing these methodologies on a simulation or implementation of a power grid. Future work will also involve reducing the search space for two classes of detectors to make higher number of sensors tractable, and extending the results to sensors with integer outputs instead of binary outputs.

REFERENCES

[1] E. A. Lee, "Cyber Physical Systems: Design Challenges," in *Object Oriented Real-Time Distributed Computing (ISORC), 2008 11th IEEE International Symposium on DOI - 10.1109/ISORC.2008.25*. IEEE, 2008, pp. 363–369.

[2] J. Markoff, "A Silent Attack, But Not A Subtle One," *New York Times*, vol. 160, no. 55176, p. 6, 2010.

[3] N. Falliere, L. Ó Murchú, and E. Chien. (2011) W32. Stuxnet Dossier. [Online]. Available: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

[4] A. Matrosov, E. Rodionov, D. Harley, and J. Malcho, "Stuxnet under the microscope," *ESET*, 2010.

[5] R. A. Maronna, D. R. Martin, and V. J. Yohai, *Robust Statistics*, ser. Theory and Methods. Wiley, 2006.

[6] P. J. Huber and E. M. Ronchetti, *Robust Statistics*. Wiley, 2011.

[7] A. Abur and A. G. Expósito, *Power System State Estimation*, ser. Theory and Implementation. CRC Press, 2004.

[8] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 1, pp. 1–33, 2011.

[9] H. Sandberg, A. Teixeira, and K. H. Johansson, "On Security Indices for State Estimators in Power Networks," in *First Workshop on Secure Control Systems, Cyber Physical Systems Week 2010*, 2010.

[10] A. Agah, S. K. Das, K. Basu, and M. Asadi, "Intrusion detection in sensor networks: a non-cooperative game approach," in *Network Computing and Applications, 2004. (NCA 2004). Proceedings. Third IEEE International Symposium on*. IEEE, 2004, pp. 343–346.

[11] T. Alpcan and T. Başar, "A game theoretic approach to decision and analysis in network intrusion detection," in *Decision and Control, 2003. Proceedings. 42nd IEEE Conference on*. IEEE, 2003, pp. 2595–2600 Vol.3.

[12] Z. E. Fuchs and P. P. Khargonekar, "Games, deception, and Jones' Lemma," in *American Control Conference (ACC), 2011*. IEEE, 2011, pp. 4532–4537.

[13] K. G. Vamvoudakis, J. P. Hespanha, B. Sinopoli, and Y. Mo, "Adversarial detection as a zero-sum game," in *Decision and Control and European Control Conference (CDC-ECC), 2011 50th IEEE Conference on*, 2012, pp. 7133–7138.

[14] M. Kodialam and T. V. Lakshman, "Detecting network intrusions via sampling: a game theoretic approach," in *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*, 2003, pp. 1880–1889.

[15] V. Bier, S. Oliveros, and L. Samuelson, "Choosing What to Protect: Strategic Defensive Allocation against an Unknown Attacker," *Journal of Public Economic Theory*, vol. 9, no. 4, pp. 563–587, 2007.

[16] P. J. Huber, "A Robust Version of the Probability Ratio Test," *The Annals of Mathematical Statistics*, vol. 36, no. 6, pp. 1753–1758, 1965.

[17] P. J. Huber and V. Strassen, "Minimax Tests and the Neyman-Pearson Lemma for Capacities," *The Annals of Statistics*, vol. 1, no. 2, pp. 251–263, 1973.

[18] S. A. Kassam and H. V. Poor, "Robust techniques for signal processing: A survey," *Proc. IEEE*, vol. 73, no. 3, pp. 433–481, 1985.

[19] R. Chabukswar, Y. Mo, and B. Sinopoli, "Secure Detection Using Binary Sensors," in *4th IFAC Workshop on Distributed Estimation and Control in Networked Systems*, Koblenz, Germany, 2013.

[20] R. R. Bahadur, "A Representation of the Joint Distribution of Responses to n Dichotomous Items," in *Studies in Item Analysis and Prediction (Stanford Mathematical Studies in Social Sciences VI)*, H. Solomon, Ed. Stanford University Press, 1961, pp. 158–168.

[21] L. J. Emrich and M. R. Piedmonte, "A Method for Generating High-Dimensional Multivariate Binary Variates," *The American Statistician*, vol. 45, no. 4, pp. 302–304, 1991.

[22] A. D. Lunn and S. J. Davies, "A note on generating correlated binary variables," *Biometrika*, vol. 85, no. 2, pp. 487–490, 1998.

[23] C. G. Park, T. Park, and D. W. Shin, "A Simple Method for Generating Correlated Binary Variates," *The American Statistician*, vol. 50, no. 4, pp. 306–310, 1996.