Process Skew: Fingerprinting the Process for Anomaly Detection in Industrial Control Systems

Chuadhry Mujeeb Ahmed
SUTD Singapore
chuadhry@mymail.sutd.edu.sg

Jay Prakash
SUTD Singapore
jay_prakash@mymail.sutd.edu.sg

Rizwan Qadeer
GCL Technologies Luxembourg
rqadeer@gclinternational.com

Anand Agrawal
NYU Abu Dhabi
anand.agrawal@nyu.edu

Jianying Zhou
SUTD Singapore
jianying_zhou@sutd.edu.sg

ABSTRACT

In an Industrial Control System (ICS), its complex network of sensors, actuators and controllers have raised security concerns. In this paper, we proposed a technique called *Process Skew* that uses the small deviations in the ICS process (herein called as a process fingerprint) for anomaly detection. The process fingerprint appears as noise in sensor measurements due to the process fluctuations. Such a fingerprint is unique to a process due to the intrinsic operational constraints of the physical process. We validated the proposed scheme using the data from a real-world water treatment testbed. Our results show that we can effectively identify a process based on its fingerprint, and detect process anomaly with a very low false-positive rate.

CCS CONCEPTS

• **Security and privacy → Intrusion detection systems**;

KEYWORDS

Cyber Physical Systems, CPS Security, Critical Infrastructure, sensor attacks, sensor security

ACM Reference Format:
Chuadhry Mujeeb Ahmed, Jay Prakash, Rizwan Qadeer, Anand Agrawal, and Jianying Zhou. 2020. Process Skew: Fingerprinting the Process for Anomaly Detection in Industrial Control Systems. In *13th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '20), July 8–10, 2020, Linz (Virtual Event), Austria.* ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3395351.3399364

1 INTRODUCTION

An Industrial Control System (ICS) is composed of a set of sensors, actuators, controllers and communication networks [18]. Connectivity in an ICS provides improved monitoring and operation of a physical process. Such advancements are helpful but also bring up the challenge of secure operation of the connected devices [4].

WiSec '20, July 8–10, 2020, Linz (Virtual Event), Austria

ACM ISBN 978-1-4503-8006-5/20/07…$15.00
https://doi.org/10.1145/3395351.3399364

An ICS could be subject to cyber and/or physical attacks, which can be launched either remotely or locally. Attackers may tamper sensor reading or inject spoofing sensor data, and manipulate the actuators which, will cause anomaly of operations and eventually lead to physical damages to the system. Traditional intrusion detection methods based on network traffic cannot detect many low layer attacks originated in the physical domain, as there would be no abnormal network traffic [26].

Sensor data is transmitted to a Programmable Logic Controller (PLC) to take an appropriate action based on the sensor measurement. If an adversary can spoof sensor data in the digital or physical domain, it can derive a system to an unsafe state. The focus here is not on the confidentiality of the data as in legacy computer security but the integrity and trustworthiness of the data [15, 17]. Detection methods based on the physics of the process against attacks on sensor reading have been proposed in recent studies [2, 23, 25–27, 29, 31]. An attacker who tries to defy rules of physics would also expose itself. An understanding of the physics of the process can help to secure an ICS.

1.1 Proposed Technique

A novel technique is proposed to identify a physical process and detect data integrity attacks in an Industrial Control System (ICS). The proposed technique uses the small deviations in the process due to the deviations of the process (herein called process skews). The process skew is a noise that appears in sensor measurements due to the process fluctuations. Uniqueness in the skews is due to the specified operational constraints of the physical process. To create a process skew based fingerprints, it is challenging to extract process skew information from the sensor measurements. The proposed idea is inspired by the idea of *clock skew* in computers [16]. The concept of clock skew is that due to manufacturing inaccuracies, the clock of a computer will present a skew from its designed frequency. Similarly, for a process due to inaccuracies in the process, it would have a skew from what it is designed for. An example is that of a water pipe taking water to fill a tank. Pipes and tanks of two different sizes would take/store a different amount of water. Even if the pipes are of the same size, two different amounts of pumping force will result in a different amount of water flowing or being stored. The flow of water in a pipe and water storage in a tank are examples of the physical process. At the design stage, these processes are designed to meet certain operational requirements. However, when these processes are running they show small offsets from the designed parameters due to the physical inaccuracies in

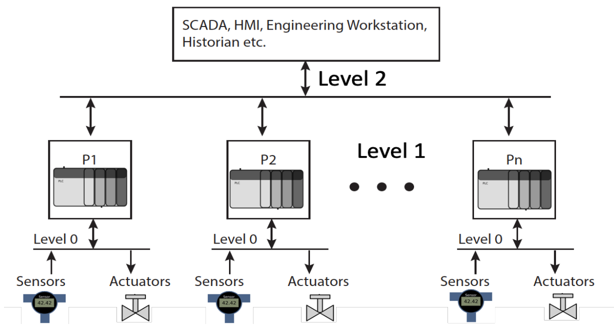

Figure 1: SWaT Test-bed Network Architecture.

the process, for example, no two water pipes can be same diameter at a micro-scale due to manufacturing imperfections.

1.2 Related Work

A closely related work proposed [21] to fingerprint sensors based on the measurement noise. However, the technique works only in specific states, for example, if the water in the tank is constant. To extract sensor noise for certain sensors (e.g. level sensors), one needs to wait for the process to be static. The work in [21] uses the noise from the sensor which a function of hardware of a device, while in our work we look at the inaccuracies in the physical process itself rather than the device. Moreover, our proposed technique does not depend on the specific state of the system and uses the dynamics of the process to create a system model. It uses process skews to create a fingerprint which is a novel idea.
CAN Bus Fingerprinting: In a particular type of ICS(automotive industry), researchers have tried to fingerprint devices in Controller Area Networks(CAN) bus [10–12, 22]. In [11] authors used clock skews from message arrival times as a fingerprint to detect intrusion for Electronic Control Units (ECUs) for a CAN bus based in-vehicle communication system. This approach is similar in essence to [16] as explained above and can not be used for sensors due to the lack of those physical components to generate particular features. In [10, 12, 22], output voltages on CAN bus are used to fingerprint the ECUs. For an electric grid system, the authors in[13] studied the opening and closing timing profiles of electric relays as fingerprints. Besides these techniques, other methods are proposed to fingerprint the devices in ICS. However, our proposed technique is a distinctive way of passively fingerprinting processes. To the best of our knowledge, this is the first attempt at using process skew as a process fingerprint to detect attacks.

Our Contributions: The main contributions of this work are,

- To propose a novel idea of process skew to fingerprint the physical processes.
- To detect sensor attacks under a multitude of adversarial scenarios.

2 MOTIVATION AND OVERVIEW

In this section, we will present details related to Secure Water Treatment Testbed (SWaT), which is used as a case study in this work. An overview of the proposed technique is also presented.

2.1 Industrial Control Systems

Industrial Control Systems (ICS) is a broad domain of connected industrial systems. A particular example of a water treatment industrial process is considered in this study. In particular, Secure Water Treatment Testbed (SWaT) at Singapore University of Technology and Design is being used as a motivating example in this paper. SWaT is a fully functional testbed and is open for researchers to use. A brief introduction is provided in the following, but an interested reader is referred to the testbed paper [19]. The SWaT testbed produces the purified water, and it is a scaled-down version of a real water treatment process. In Figure 1 it can be seen that the testbed is distributed and there are different stages, where each stage is labeled as P_n where n is the nth stage. There are six stages in the SWaT testbed P_1 through P_6. Each stage is equipped with a set of sensors and actuators. Sensors include water quantity measures such as level, flow, and pressure and water quality measures such as pH, ORP and conductivity. Actuators are different motorized valves and electric pumps. Stage 1 is the raw water stage to hold the raw water for the treatment and stage 2 is the chemical dosing stage to treat the water depending on the measurements from the water quality sensors. Stage 3 is the ultra-filtration stage. Stage 4 is composed of de-chlorinator and stage 5 is equipped with reverse osmosis filters. Stage 6 holds the treated water for distribution. Data from the sensors and actuators are communicated to the PLCs using a level 0 network and PLC communicates to each other over a level 1 network, as shown in Figure 1.

2.2 Overview of the Proposed Technique

A major challenge is to extract the process skew from sensor data. An overview of the proposed technique is shown in Figure 2. The first step is to extract the measurements for a specific state of the process. It means that based on the actuator data, it is possible to determine the physical state of the process. For example, if the inlet pump is ON then the water is being filled in a tank, by knowing the state of the pump, it is possible to know the state of the physical process. However, such state information from the sensors and actuators might be spoofed by an attacker. Next, based on the state of each process a model along with the design parameters of the physical process is used to estimate the physical state of the process, for example, the water level in a tank. The difference between these estimates and real sensor measurements establishes an offset value, an amount by which the process is offset from what it should be, as per the design. These process offsets, when accumulated over time, reveals the process skew but still contain fluctuations due to the sensor noise. A linear regression model is used to obtain the best fit for each process skew. Process skew is obtained by calculating the rate of change of linear regression on offsets with respect to time. A theoretical proof based on the calculated entropy of the process skew is used to establish the uniqueness of process skews. A CUSUM detector is used to detect attacks based on the process skew. Details on the design of each block in Figure 2 are presented in Section 4.

3 THREAT MODEL

In an ICS, state of the physical process is known via sensors. System is kept in the normal operating bounds by the controllers based

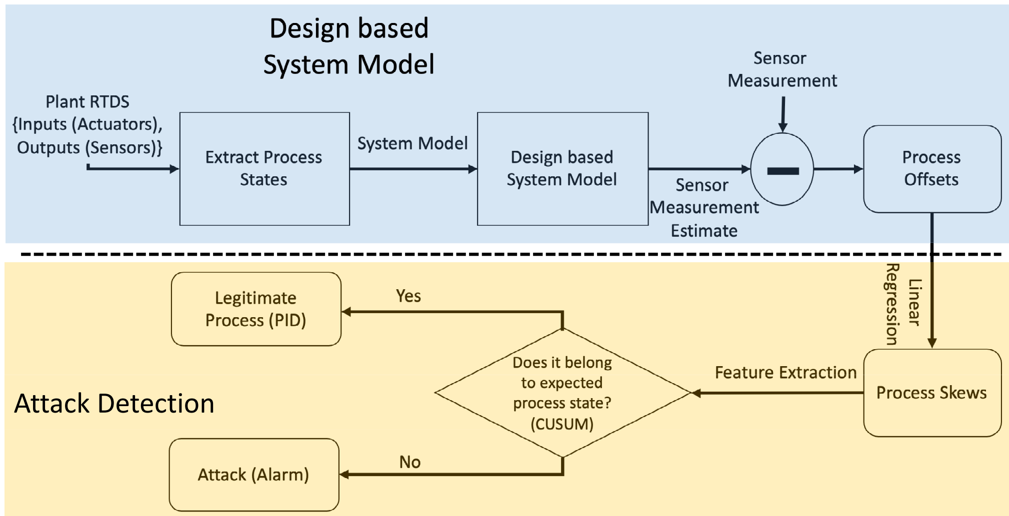

Figure 2: Overview of the proposed technique.

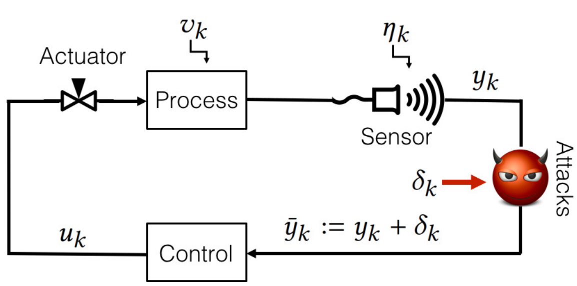

Figure 3: An abstraction of a Cyber Physical System (CPS). $\bar{y}_k$ may or may not be attacked sensor measurement [6].

on the sensor measurements. An adversary can spoof sensor measurements to deceive the controllers. It is important to authenticate whether the data is originating from the real physical process or being modified in some manner. Due to computational limitations and legacy compliant equipment it is not feasible to rely on cryptographic methods [8]. Therefore, we came up with the proposed novel idea of process skew based authentication of a physical process. The goal is to identify a process based on its physical dynamics. Specific cyber attacks are also considered on sensor measurements in a water treatment plant. In Figure 3, it can be seen that an attacker can modify a rightful sensor measurement by an attack value δ_k. In this section, we introduce the types of attacks launched on the secure water treatment testbed (SWaT). Essentially, the attacker model encompasses the attacker's intentions and capabilities. The attacker may choose its goals from a set of intentions [28], including performance degradation, disturbing a physical property of the system, or damaging a component. In our experiments, a range of attacks are considered from already published attack scenarios in the literature [9, 14].

3.1 Attacker Model

Assumptions on Attacker: It is assumed that the attacker has access to the sensor's measurements. A powerful attacker can arbitrarily change sensor measurements to the desired sensor value. We do not consider replay attack in this article because process skew profile for process would be preserved during a replay attack.

3.2 Attack Scenarios

Data Injection Attacks: For data injection attacks, it is considered that an attacker injects or modifies the real sensor measurement. In general, for a complex ICS, there can be many possible attack scenarios. We consider a generic attack to show the performance of the proposed technique. We evaluate the proposed technique for a range of network attack scenarios from benchmark attacks on SWaT testbed [14]. These attacks cover a wide range of 36 attacks on both sensors and actuators. Since the proposed technique extracts the process skew for the physical properties, thus chemical sensors are excluded from this study, leaving us with a total of 25 attacks as detailed in Table 5 in Appendix. In general, an attack vector can be defined as,

$$\bar{y}_k = y_k + \delta_k, \tag{1}$$

where y_k are the real sensor measurement, $\bar{y}_k$ is sensor measurement with a possible attack and δ_k is the data injected by an attacker at time step k. The detail about each δ_k (attack vector) is described in Table 5 in the Appendix where it can be seen that it ranges from an abrupt injection of data to more slow/stealthy change in sensor measurements.

3.3 Attack Execution

All the attacks which are taken from reference work [14], are executed by compromising the Supervisory Control and Data Acquisition (SCADA) system.

State (Inlet Flow | Outlet Flow[1])	Design Parameters	Process Details
S1 (0 | 1)	Outlet flow = 2.47m^3/hr	In this scenario, the water is being flown out of the tank 1 i.e., emptying process.
S2 (0 | 0)		In this scenario, the water level stays constant, i.e., static process.
S3 (1 | 0)	Inlet flow = 2.54m^3/hr	In this scenario, the water is being flown into the tank 1. i.e., filling process.
S4 (1 | 1)	Inlet flow = 2.54m^3/hr and Outlet flow = 2.47m^3/hr	In this scenario, the water is being flown out and in of the tank 1 at the same time, i.e., both filling and emptying process.

1. If flow present it is 1 else 0.

Table 1: The tank1 in stage1 of the SWaT testbed has one inlet valve labeled as MV-101 and one outlet pump labeled as P-101. Notice that there is a secondary backup pump also at the outlet labeled as P-102. Based on inflow and outflow there can be four possible states for the level in tank1 based on input and output flow process.

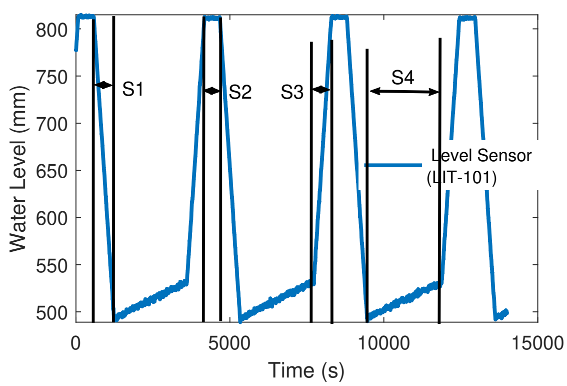

Figure 4: Level sensor in the SWaT testbed in stage 1 labelled as LIT-101 under the normal operation. This figure shows multiple runs of a physical process, e.g., water filling, water flowing out, both or none of the previous process. Each of these processes is labelled as S1 to S4, and the details are given in Table 1.

4 DESIGN OF THE PROPOSED TECHNIQUE

In this section, all the components of the proposed technique are discussed in detail.

4.1 Extracting the Process States

We begin by considering an example from the SWaT testbed. In Figure 4, level sensor (LIT-101) measurements for a duration of normal process are shown. It can be seen that based on the inflow and outflow, there can be four possible process states, i.e., S1: outflow is present but no inflow, S2: neither inflow nor inflow, S3: inflow is present but no outflow, S4: both input and output flow processes are present. Table 1 shows a detailed description of the four possible process states in the water tank. Design parameters in Table 1 shows the design for the inflow and outflow process and which process is present in a particular state.

The water treatment plant is run for seven days continuously and the data for the normal operations of the plant is collected. In Figure 5 four possible process states for the water level in tank1 are shown. This data presents the particular states extracted from the seven days of the normal operation. There are hundreds of occurrences for each process state. Different colors in the plot represent different runs of the normal operation. The effects of the noise are evident from the variability of the process slope.

Each process is expected to behave according to the design parameters as shown in Table 1. However, as we can visually see in Figure 5 there are deviations due to the process noise. In Figure 5, the first state S1 shows different runs of the water emptying process from the tank1. We can see the variations in each process run due to the sensor noise. This is also evident from the static (S2) and water filling (S3, S4) processes. Having seen the deviations and noise in these physical processes, the next step is to figure out the variation due to the process offset from the design. To quantify the amount of skew, we need to learn the process dynamics for all these states under the designed set points.

4.2 Design based System Model

In Figure 7 the sensor measurements for the water filling process and estimated sensor value based on the design are shown. The accumulated offset is also labelled to make the visual sense of the idea. A physical system diagram for stage 1 is shown in Figure 6. Tank 1 in stage 1 of the SWaT testbed is being used as a running example to demonstrate the idea. In Figure 6, it is shown that the water level in the tank is measured using a level sensor and the inflow and outflow of the water is being controlled by the motorized valve (MV-101) at the input and pump (P-101) at the output respectively. The idea is to model this inflow and outflow by considering the physical principles and the design of the physical process. Process skew information is extracted by figuring out the process dynamics drift from the design due to the process noise. For a tank, we know that the rate of change of water inside the tank is equal to the difference between water flowing into the tank and water flowing out from the tank with respect to time. We can represent this using mass-balance equation [24] such as,

$$\frac{dV}{dt} = Q_{in} - Q_{out}$$

$$\frac{dh}{dt} = \frac{Q_{in} - Q_{out}}{A} \quad \text{since} \quad V = A \times h, \tag{2}$$

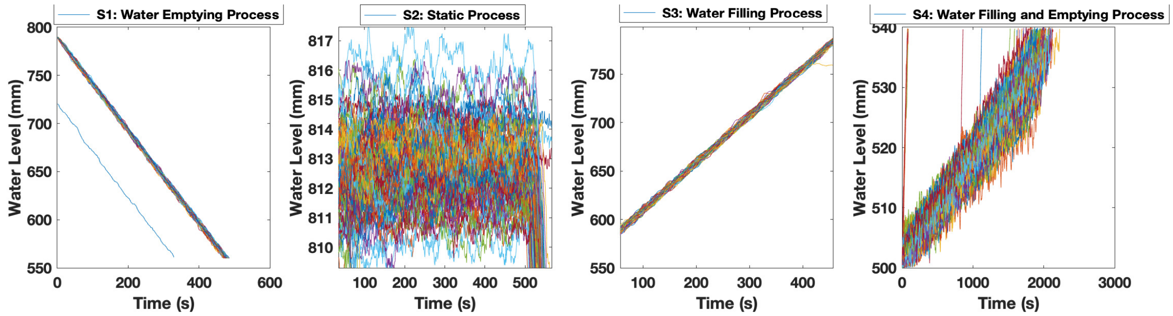

Figure 5: These sub-figures show four possible states of a physical process in a water tank, as described in Table 1. Level sensor in the SWaT testbed in stage 1 labelled as LIT-101 under the normal operation.

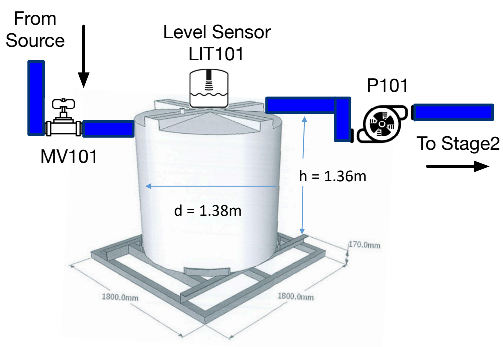

Figure 6: Modeling the process for the level sensor in Tank1.

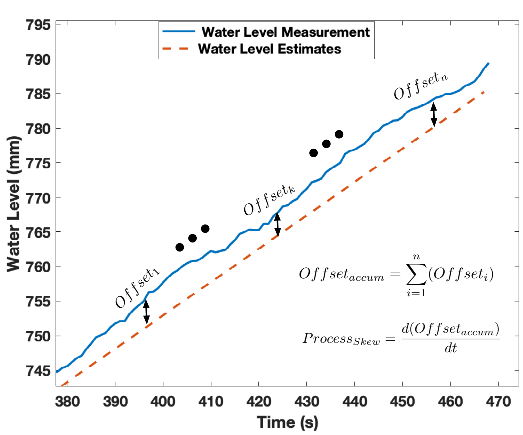

Figure 7: The idea of process skew. Water level sensor measurement and its estimates using the model are shown. The difference between both is defined as the offset.

where V represents the volume of the tank, A is the cross-sectional area of the tank, and h is the height of the water inside the tank, (2) provides a linear equation, we can see the term $[Q_{in} - Q_{out}]$ represents the water flow which depends upon the PLC control actions implemented via MV-101 and P-101. From Figure 6, it can be seen that using the height and diameter of the tank from design documents, it is possible to figure out the volume and the cross-sectional area of the tank. Let us consider that state of the physical process as the height of the water inside the tank. Then the solution of this equation gives us the following result.

$$x_{k+1} = x_k + u_k,$$

where u_k is the PLC control action. Here x_k represents water level in the tank at time k. The control action u_k can be an either open/close (for the motorized valve) or on/off (for the pump). Similarly, we can describe the sensor state and we can get the set of system equations.

$$\begin{cases} x_{k+1} = Ax_k + Bu_k, \\ y_k = Cx_k. \end{cases} \tag{3}$$

Where y_k is the sensor measurement driven by the control action u_k. Matrices A, B and C are the state-space matrices of appropriate dimensions. From (3), it can be seen that if we have a system state value at time k, then given the PLC control u_k we can predict the next state at time $k+1$. Table 1 shows a list of design parameters for each type of control action. For example, S4 has the MV-101 control as to open the valve and P-101 as turned on, given the information of this control from PLC, we know from the design of the physical process that how much the water level in the tank should increase. However, as we will see, due to the process noise, there would be deviations in the process states from what it was designed for.

4.3 Extracting the Process Offsets

Using the process design and the system of equations in (3), we could extract the process skews, i.e., how much the real process dynamics are offset from the designed physical process. In figure 8 we can see the offsets in the level of the water in tank1.

Definition 4.1. *Process Offset: Deviation of the process dynamics due to the process inaccuracies, from the design at each time step.*

The process offsets are calculated at each time step for the time while the process is active. All the process offsets are accumulated over time and then process skew is extracted.

Definition 4.2. *Process Skew: Slope of the accumulated process offsets for a process activity time frame.*

In Figure 8, we can see the accumulative offsets for the different process states. S1 represents the case of water outflow from the tank.

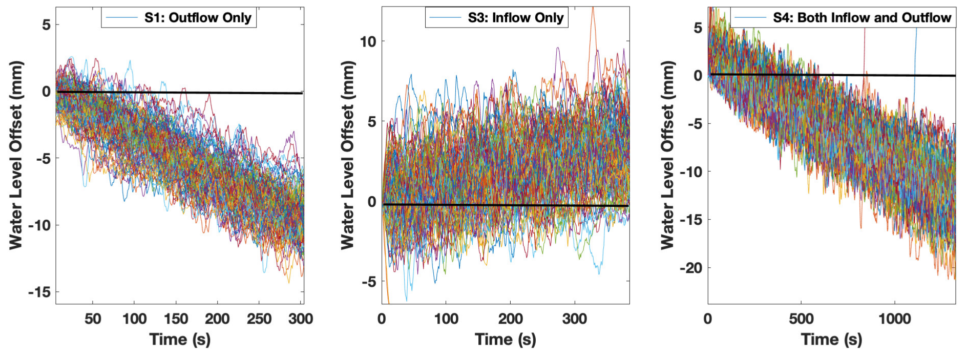

Figure 8: Water level offsets in the tank 1 for different states of the physical process.

A negative slope indicates that the real process is actually slower than the designed parameters. S2 is the case when the process is static and there is no inflow or outflow. Hence, the process is missing, so no process skew exists. For the case of S3, only the inflow is present and the positive slope shows that the real process is actually faster than the designed one. S4 is the case when both the inflow and outflow are present. In this case, it can be seen that the real process is actually slower than the design. Now all these physical state scenarios happen in the same physical process that is, the water tank in stage 1 of the SWaT testbed. Although it's the same process, it is observed that based on the process skew all the physical states of the process could be distinguished from each other. This establishes a process fingerprint. However, one important observation to make in Figure 8 is that the offsets are noisy due to the sensor noise. The challenge here is to remove the sensor noise effect without disturbing the process offsets. In the following, a mathematical expression is derived for the process skew. Consider the linear time-invariant model of the system with sensor and process noise as

$$\begin{cases} x^*_{k+1} = Ax^*_k + Bu_k + v_k, \\ y^*_k = Cx^*_k + \eta_k, \end{cases} \tag{4}$$

where y^*_k is the sensor measurement with the measurement noise η_k and x^*_{k+1} is the system state.

Proposition 4.1. *At each time step, the difference between sensor measurements given by* (4) *and sensor measurement estimate (by design) given by* (3) *is calculated to obtain the process offset as,* $y_{k+1} - y^*_{k+1} = CA[O_k] - Cv_k - \eta_{k+1}$, *where* $O_k = x_k - x^*_k$ *is the offset.*

Proof. The difference between (4) and (3)is given as,

$$y_{k+1} - y^*_{k+1} = Cx_{k+1} - Cx^*_{k+1} - \eta_{k+1}, \tag{5}$$

$$y_{k+1} - y^*_{k+1} = CAx_k + CBu_k - CAx^*_k - CBu_k - Cv_k - \eta_{k+1}, \tag{6}$$

$$y_{k+1} - y^*_{k+1} = CA(x_k - x^*_k) - Cv_k - \eta_{k+1}. \tag{7}$$

As the offset is defined as the difference the real system state and the estimated state of the system ($x_k - x^*_k$), it produces,

$$y_{k+1} - y^*_{k+1} = CA[O_k] - Cv_k - \eta_{k+1} \tag{8}$$

From (8) that the offset (O_k) can be extracted at each time step. ■

From (8), it is observed that the process offset contains the noise from the sensor; therefore, it is important to fit a straight line to data to get the process skew. Since the process skew is the slope of the accumulated process offsets, we need a straight line to represent each of the above physical states. Towards that end, we resort to the linear regression model for each process offset as evidently, the offsets are linear in time.

4.4 Process Skew

To establish the linearity between the time and the progression of the process, correlation coefficients are used. Correlation calculates the level of the linear relationship between variables. If we have a high correlation between two variables, then it means that the values for those increase or decrease in a linear relationship. However, uncorrelated variables might still be dependent on each other it is just that the relationship might be nonlinear. For N scalar values of two variables, the Pearson correlation coefficient is defined as,

$$\rho(X, Y) = \frac{\sum_{i=1}^{N}(X_i - \bar{X})(Y_i - \bar{Y})}{\sqrt{\sum_{i=1}^{N}(X_i - \bar{X})^2}\sqrt{\sum_{i=1}^{N}(Y_i - \bar{Y})^2}} \tag{9}$$

where $\bar{X}$ is the mean of the variable X and $\bar{Y}$ is the mean of the variable Y. We have found that the process data is linearly correlated with the time as the process is linearly increasing or decreasing in time. Linear regression approach is adopted to get the data models describing the relationship between the variable in a mathematical form. Least squares fit is used to obtain the model. For a set of n observed values of X and Y given by $X = (x_1, x_2, ..., x_n)$ and $Y = (y_1, y_2, ..., y_n)$ respectively. These values for a system of linear equations which can be represented in matrix form as,

$$\begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix} = \begin{bmatrix} 1 & x_1 \\ 1 & x_2 \\ \vdots & \vdots \\ 1 & x_n \end{bmatrix} \begin{bmatrix} \beta_0 \\ \beta_1 \end{bmatrix}$$

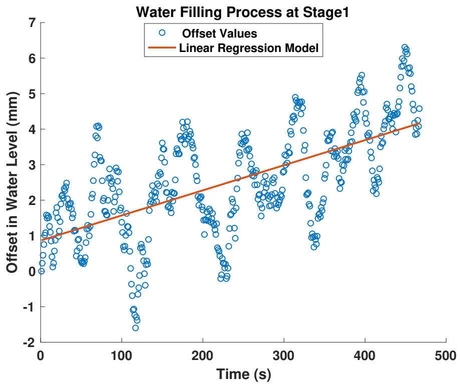

Figure 9: Linear regression model fit for the process skew for a water filling process in Stage1 of the water treatment system.

which can be simplified to,

$$Y = \beta_0 + \beta_1 X + \epsilon, \tag{10}$$

where β_0 is the y-intercept, β_1 is the slope/regression coefficient and ϵ is the model error.

Figure 9 shows a linear model fitting through the process skew data. This linear model is used to find the slope that defines the process skew. Figure 9 shows a visual idea regarding the accuracy of the linear model. To quantify the goodness of a system model, mean square error (MSE) is used as a metric. In particular, one minus the root mean square error (RMSE) defines the estimation accuracy or best fit of a model,

$$RMSE = \sqrt{\frac{\sum_{i=1}^{n}(y_i - \hat{y}_i)^2}{n}} \tag{11}$$

MSE is the difference between sensor measurement and sensor measurement estimate squared and essentially gives the distance between measured and estimated value or in other words, how far the estimated value from the measured value is. The model accuracies for the three stages of SWaT and corresponding process states used in this study (from SWaT testbed) are shown in Table 2. It can be seen that the obtained system model is very accurate, with almost zero mean error for all the runs of a process. Table 2 shows the mean of models created for all the runs of the process. The process offsets are accumulated for the run of a process,

$$O_{accum} = \sum_{k=1}^{n}(O_k) \tag{12}$$

and the corresponding process skew is given as,

$$Process_{skew} = \frac{d(O_{accum})}{dt}. \tag{13}$$

4.5 Skew Uniqueness

In Figure 10, process skew distribution for all the eight physical processes in the three stages of the SWaT testbed is shown. It can be observed that all the processes can be uniquely distinguished

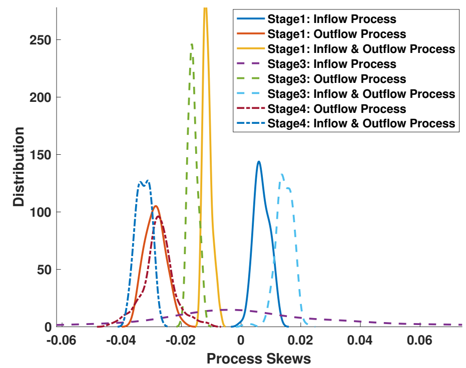

Figure 10: Process skew distribution for all the eight physical processes in the three stages of SWaT testbed.

based on the process skew profile. Figure 10 shows a visual analysis for process skew uniqueness; however, we will see a mathematical proof for the skew uniqueness. It is imperative to study that fingerprints are information-theoretically unique in order to negate the possibility of impersonation attacks. An attacker can use skews of her processes to design compromises. Let $w(t)$ be the signal corresponding to a process skew. In order to present an information-theoretic analysis on the top, we study justification of two important criteria:

(1) mutual information between skews as recorded for the same process, i.e., in successive operations should be high, ≈ 1, and
(2) conditional entropy of skews with other process skews should be very low, «1.

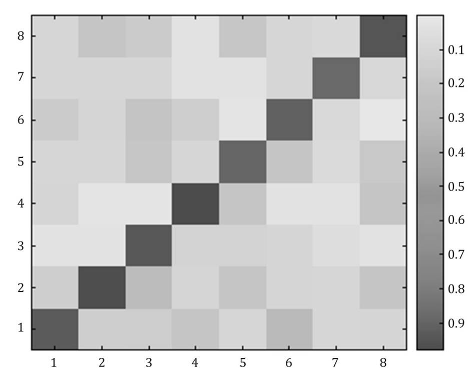

Figure 11: Mutual information across eight process skews.

In order to investigate these relations mutual information, $I(\cdot)$, for process i is defined as

$$I(w_{ij}, w_{ik}) = H(w_{ij}) - H(w_{ij}|w_{ik})$$

where $i \in 1:S, j \in 1:N, H(w_{ij})$ is the entropy of jth attempt by a process i and $H(w_{ij}|w_{ik})$ is conditional entropy of ith process for jth attempt, given the features of kth attempt. For high recall, mutual information for each of the process skew should be close

Table 2: Validation of the linear regression model to find a good fit for the process offset to find the process skew.

Metric	Stage 1			Stage 3			Stage 4[2]	
	I.F. Only	O.F. Only	I.F. and O.F.[3]	I.F. Only	O.F. Only	I.F. and O.F.	O.F. Only	I.F. and O.F.
Avg. [RMSE]	8.6e-15	2.9e-14	1.09e-13	3.33e-15	1.56e-14	6.37e-14	2.31e-14	2.05e-13
Avg. [(1 - RMSE)*100%]	100%	100%	100%	100%	100%	100%	100%	100%

2. Stage4 process outlet is always active, therefore, no I.F. only case.
3. I.F. stands for inflow and O.F. for outflow.

to 1 (normalized). Similarly, an ICS process i should not have access to any extra information about process t given observations of its own. Mathematically this can be quantified in conditional entropy as $H(w_{ij}|w_{tk}) \rightarrow 0$ for $i, t \in 1 : S$ and $j, k \in 1 : N$. We evaluated entropy measure and mutual information for each of the process skews as proposed in [7]. As can be seen in Figure 11, mutual information across 8 process skews are fairly low, < 0.1, which supports the use case. The entropy of each of the skews was recorded to be ≥ 0.94 . Further, the investigation of conditional entropy across different processes of the ICS system reveals that features are independent.

4.6 Cumulative Sum (CUSUM) Detector

The process skews for different runs of a particular process; for example, a water filling process is accumulated. The process skew vector is given as an input to the CUSUM procedure, also known as the stateful detector. The input to the CUSUM procedure can be considered as a *distance measure*, i.e., a measure of how far the estimate is from the expected measurements. A dedicated detector for each process is designed. The index i denotes the process, $i \in \mathcal{I} := \{1, 2, \ldots, m\}$, where m is the number of processes in each stage of the plant. Process skew is labelled as $r_{k,i}$ here for easy reference, where k is the time step. The standard CUSUM [20] procedure is explained using the following equations.

CUSUM: $S^-_{0,i} = \bar{T}_i,\ \ S^+_{0,i} = \bar{T}_i,\ \ \tilde{k}^+_i = 0,\ \ \tilde{k}^-_i = 0,$

$$\begin{cases} S^+_{k,i} = \max(\bar{T}_i, S^+_{k-1,i} + r_{k,i} - \bar{T}_i - \kappa_i), & \text{if } S^+_{k-1,i} \leq \tau^+_i, \\ S^+_{k,i} = \bar{T}_i \ \text{ and } \ \tilde{k}^+_i = \tilde{k}^+_i + 1, & \text{if } S^+_{k-1,i} > \tau^+_i. \end{cases} \quad (14)$$

$$\begin{cases} S^-_{k,i} = \min(\bar{T}_i, S^-_{k-1,i} + r_{k,i} - \bar{T}_i + \kappa_i), & \text{if } S^-_{k-1,i} \geq \tau^-_i, \\ S^-_{k,i} = \bar{T}_i \ \text{ and } \ \tilde{k}^-_i = \tilde{k}^-_i + 1, & \text{if } S^-_{k-1,i} < \tau^-_i. \end{cases} \quad (15)$$

Design parameters: Bias $\kappa_i > 0$; threshold $\tau_i > 0$.
Output: $Alarm(s) = \tilde{k}^+_i + \tilde{k}^-_i$.

From (14)-(15), it can be observed that $S^+_{k,i}$ and $S^-_{k,i}$ accumulate the distance measure $r_{k,i}$ over time to measure how far are the values of the residual from the target mean ($\bar{T}_i$). To tune the CUSUM detector there is also a slack variable κ chosen to be $\frac{1}{2} * \sigma_i$ in this study. $\tau_i = \pm\Gamma * \sigma_i$, where Γ is a multiplier to the standard deviation (σ) and usually taken between 3 and 5 [20]. An alarm is raised when this accumulation becomes greater or less than a chosen threshold τ_i. The sequence $S_{k,i}$ is reset to the target mean value each time it becomes negative or larger than τ_i. If r_k, i is tightly bounded and κ_i is not sufficiently large, the CUSUM sequence $S_{k,i}$ grows unbounded until the threshold τ_i is reached, no matter how large τ_i is set. In order to prevent such drifts, the slack variable κ_i must be selected properly based on the statistical properties of the distance measure. Once κ is chosen, the threshold τ_i must be selected to achieve a required false alarm rate $\mathcal{A}^*_i$. $\mathcal{A}_i \in [0, 1]$ denotes the *false alarm rate* for the CUSUM procedure defined as the expected proportion of observations which are false alarms [1, 30].

5 EVALUATION

The proposed technique is evaluated in a real water treatment testbed. The following metrics are used for performance evaluation. We define TP_i as true positive for class c_i when it is rightly classified based on the ground truth. False-negative FN_i is defined as the wrongly rejected, and False positive FP_i as wrongly accepted. True negative TN_i is the rightly rejected class. The True Positive Rate (TPR) and False Positive Rate (FPR) are defined as follows:

$$\text{True Positive Rate (TPR)} = \frac{TP}{TP + FN} = 1 - FNR, \quad (16)$$

$$\text{False Positive Rate (FPR)} = \frac{FP}{FP + TN} = 1 - TNR. \quad (17)$$

Ideally, FPR should be as small as possible and TPR as high as possible. Both TPR and FPR being ratios range between 0 and 1.

5.1 Normal Operation

For the normal operation data from the SWaT testbed is collected for a period of seven days. During the normal operation, the plant was run continuously under the normal conditions and as it was designed to operate. The operating conditions from the design was already presented in Table 1. For all the possible process states, data is extracted. Process offsets are extracted for each process in Stage1, Stage3 and Stage4 of the SWaT testbed. Stage2 and Stage5 is constituted of chemical sensors and reverse osmosis process respectively; therefore, those two stages are not considered in this study. This work is focused on studying the physical properties of the process. Studying the chemical properties of the process is out of the scope of this work. During seven days, water filling or the emptying process happened hundred of times. Process offsets are calculated for each of these process runs. Process offsets are noisy due to the noise from the sensors. A linear regression model is fit to handle the noise in the signal. After the linear model is fitted, we obtain a straight line for accumulated process offsets over process time frame. The rate of change of these process offsets is defined as the process skew. Figure 8 shows process offsets for different process states of the Stage1 of the SWaT testbed. Figure 9 shows an example of linear model fitting for the process offsets. The obtained linear model can be used to calculate process skews. Normal process skews are used with a CUSUM detector to establish

Table 3: Design and performance of CUSUM detector on the normal data. μ and σ are mean and standard deviation of the process skews.

Parameters	Stage 1			Stage 3			Stage 4	
	I.F. Only	O.F. Only	I.F. and O.F.	I.F. Only	O.F. Only	I.F. and O.F.	O.F. Only	I.F. and O.F.
κ	0.0013	0.0017	7.27e-04	0.0217	7.90e-04	0.0014	0.0027	0.0012
τ	0.0102	0.0219	0.0073	0.1083	0.0126	0.0199	0.0277	0.0148
μ	0.0070	-0.0288	-0.0113	0.0082	-0.0161	0.0146	-0.0277	-0.0327
σ	0.0026	0.0034	0.0015	0.0433	0.0016	0.0028	0.0054	0.0025
TNR	96.04%	97.46%	97.10%	96.99%	96.97%	96.38%	97.39%	95.31%
FPR	3.96%	2.54%	2.90%	3.01%	3.03%	3.62%	2.61%	4.69%

a fingerprint for each process. The detailed CUSUM parameters for all the stages in SWaT are shown in Table 3. All the thresholds and other parameters are designed to have a desired false alarm rate of less than 5%. Table 3 shows bias parameter κ, threshold τ, mean μ and standard deviation σ for the process skews. In the last two rows of the Table 3 performance of the CUSUM under the normal operating conditions are shown using the design parameters specified. It can be observed that for all the casesthe the desired false alarm rate is below 5%.

RQ1: Can process skews be used to fingerprint each process state? Table 3 shows a high true negative rate meaning it is possible to identify each process state with a high accuracy based on the process skew fingerprint. A physical process goes through different process states during the operation of the process plant. For example, for the process of a fluid tank, either fluid is flowing out, flowing in, both or in a static state. Since different process states have different skews, it is possible to uniquely identify each process state based on its process skew fingerprint.

RQ2: Does a process skew depends on the initial conditions of a process dynamics? This means that, does it matter at what initial state the process starts. For example, does it matter if the water filling process starts at 500 mm or 800 mm water levels? In this study, a particular process, for example, a water filling process started at different initial states depending on the control logic. The results presented in Table 3 is a combination of all possible initial conditions of a particular process and a fingerprint is created for all the runs of the process taken together. It can be seen from Table 3 that the process skew based fingerprint is stable over a range of process start and end conditions, making it robust to use in a real-world system.

5.2 Attack Detection

RQ3: Can the proposed process skew based fingerprint be used as an attack detection method? The performance of the proposed technique as an attack detection method is evaluated under a range of attack data collected from SWaT testbed. SWaT was subject to different attack scenarios for four days. This is to say that for four days there were a lot of runs of normal operation and then there were attack instances in between. A complete list of attacks is shown in Table 5 in the Appendix. An example of process skews for the process of tank4 in stage4 is shown in Figure 12. From Figure 12 it is evident that using process offsets and skews, it is easy to detect attacks. The attack scenarios deviate from the normal process offsets. Note that there are attack start and attack stop markers. In some cases when the attack was stopped the slope of the process offset, which is

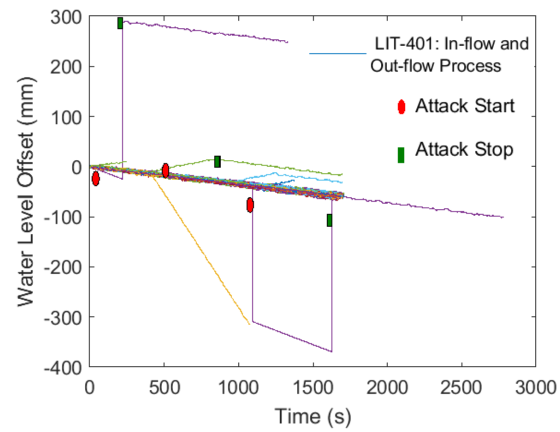

Figure 12: LIT-401 Process Offsets under attacks. This is a mix of normal process and few attacks. Normal offsets are close together and follow the normal profile of the process. However, there are clear deviations for the attacks as labeled in the figure.

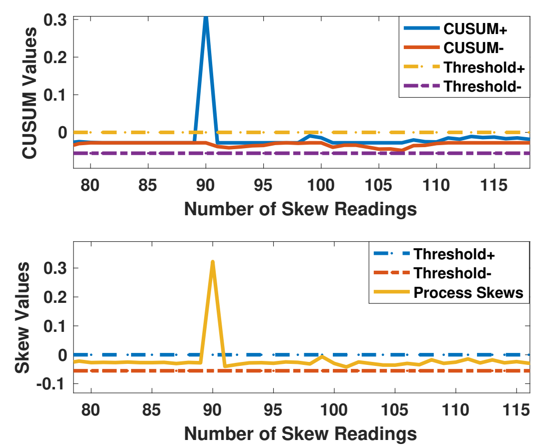

Figure 13: Attack detection example for LIT-401, outflow process. Using the CUSUM detector on process skews, the attacks are evident.

Table 4: Evaluation of the proposed technique on the attack data from SWaT testbed. TPR presents the attacks which were detected accurately as percentage (attacks-detected/total-attacks-executed).

Metrics	Stage 1			Stage 3			Stage 4	
	I.F. Only	O.F. Only	I.F. and O.F.	I.F. Only	O.F. Only	I.F. and O.F.	O.F. Only	I.F. and O.F.
TPR	100%(3/3)	100%(4/4)	100%(1/1)	100% (1/1)	100%(3/3)	100%(7/7)	100(2/2)%	100(5/5)%
FPR	3.2%(4/125)	1.65%(2/121)	8.06%(10/124)	5.08% (9/177)	4.58%(7/153)	6.04% (13/215)	0.92%(2/217)	10.70%(23/215)

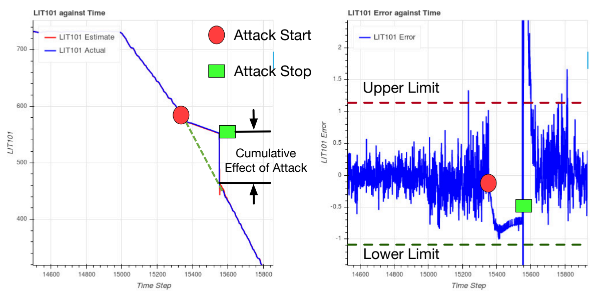

Figure 14: Stealthy attack on the level sensor in Stage1 of the SWaT testbed. The Stealthy attack is designed to spoof the values of the level sensor measurements so that the residual shown on the right does not surpass the threshold.

process skew tends to go back to normal as expected, but the whole offset has deviated for the overall process. Figure 13 shows the CUSUM detector for the same process. From Figure 13, we can see that it is easy to see how process skews can enable attack detection. However, a detailed analysis is carried out for all the three stages and corresponding processes in the SWaT testbed and results are presented in Table 4. We can see that all the attacks are detected in all the scenarios with 100% TPR. FPR is close to the desired 5% false alarm rate except for two instances. Process skew has shown perfect performance on attack detection.

6 DISCUSSION

6.1 A Comparison with Model based Detectors

Can process skew fingerprint be used to detect attacks those are stealthy for the model based detectors [3, 5, 6]?

Figure 14 shows the execution of such an attack on the SWaT testbed. On the left-hand plot, actual measurements and sensor estimates obtained from level sensor, LIT-101, using the system model have been plotted. On the right-hand side, respective residual (measured - estimated) values for the level sensor are shown. Upper and lower limits for a statistical detector can be seen. On the left-hand plot, the dotted green line shows the ground truth for the process state, while the attacker spoofed the sensor values and managed to derive the system away from the normal operation overtime during the attack period. The spoofed values are chosen such that the residual values never grow bigger than a model-based detector threshold and hence, could not get detected. But from the ground truth, we know that the process dynamics are not what the attacker is making PLC to believe. Using process skew, it is possible to detect the presence of such an attacker. The idea is if an attacker wants to deviate the process from its desired operation, it must defy the process dynamics and expose itself to process skew. In comparison, it can be concluded that the proposed process skew based technique can detect attacks that are stealthy for the system model based detectors.

6.2 Scalability

This case study is carried out on a water treatment plant but we believe that the technique itself is generalizable. The physical process discussed in this work is water/fluid dynamics, but there are other similar processes, e.g., gas or other chemical fluids where the same techniques should work. Moreover, in this work, a range of different processes and process states are considered that points towards its scalability. On the top of it, the demonstration on a real system highlights its applicability in real-world applications.

7 CONCLUSIONS

We demonstrated that indeed a process skew exists for each process due to the deviations in the process from the design. The proposed technique can be used to fingerprint the different process states, for example, filling, emptying, or a combination of these process dynamics in a water treatment system. Hence, it is possible to detect attacks on the processes. An extensive evaluation of the proposed technique on a real-world water treatment system validates its applicability and practicality.

While carrying out this study, some useful observations have been made regarding the process transients. When a process changes from one state to another, the process dynamics are said to be in a transient state and it takes time to reach a steady-state. In the future, we would like to explore this transient feature of the processes for attack detection.

ACKNOWLEDGEMENT

This work was supported by the SUTD start-up research grant SRG-ISTD-2017-124.

REFERENCES

[1] B.M. Adams, W.H. Woodall, and C.A. Lowry. 1992. The use (and misuse) of false alarm probabilities in control chart design. *Frontiers in Statistical Quality Control 4* (1992), 155–168.

[2] Anand Agrawal, Chuadhry Mujeeb Ahmed, and Ee-Chien Chang. 2018. Poster: Physics-based attack detection for an insider threat model in a cyber-physical system. In *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*. 821–823.

[3] C. M. Ahmed, S. Adepu, and A. Mathur. 2016. Limitations of state estimation based cyber attack detection schemes in industrial control systems. In *2016 Smart City Security and Privacy Workshop (SCSP-W)*. 1–5. https://doi.org/10.1109/SCSPW.2016.7509557

[4] Chuadhry Mujeeb Ahmed and Jianying Zhou. 2020. Challenges and Opportunities in CPS Security: A Physics-based Perspective. arXiv:cs.CR/2004.03178

[5] Chuadhry Mujeeb Ahmed, Jianying Zhou, and Aditya P. Mathur. 2018. Noise Matters: Using Sensor and Process Noise Fingerprint to Detect Stealthy Cyber Attacks and Authenticate Sensors in CPS. In *Proceedings of the 34th Annual*

Computer Security Applications Conference (ACSAC '18). ACM, New York, NY, USA, 566–581. https://doi.org/10.1145/3274694.3274748

[6] Mujeeb Ahmed, Carlos Murguia, and Justin Ruths. 2017. Model-based Attack Detection Scheme for Smart Water Distribution Networks. In *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security (ASIA CCS '17)*. ACM, New York, NY, USA, 101–113. https://doi.org/10.1145/3052973.3053011

[7] Gavin Brown, Adam Pocock, Ming-Jie Zhao, and Mikel Luján. 2012. Conditional likelihood maximisation: a unifying framework for information theoretic feature selection. *Journal of machine learning research* 13, Jan (2012), 27–66.

[8] John Henry Castellanos, Daniele Antonioli, Nils Ole Tippenhauer, and Martín Ochoa. 2017. Legacy-compliant data authentication for industrial control system traffic. In *International Conference on Applied Cryptography and Network Security*. Springer, 665–685.

[9] Yuqi Chen, Christopher M. Poskitt, and Jun Sun. 2018. Learning from Mutants: Using Code Mutation to Learn and Monitor Invariants of a Cyber-Physical System. *IEEE Security and Privacy 2018* abs/1801.00903 (2018). arXiv:1801.00903 http://arxiv.org/abs/1801.00903

[10] Kyong-Tak Cho and Kang G. Shin. 2017. Viden: Attacker Identification on In-Vehicle Networks. *CoRR* abs/1708.08414 (2017). arXiv:1708.08414 http://arxiv.org/abs/1708.08414

[11] Kyong-Tak Cho and Kang G. Shin. 2016. Fingerprinting Electronic Control Units for Vehicle Intrusion Detection. In *25th USENIX Security Symposium (USENIX Security 16)*. USENIX Association, Austin, TX, 911–927. https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/cho

[12] Wonsuk Choi, Hyo Jin Jo, Samuel Woo, Ji Young Chun, Jooyoung Park, and Dong Hoon Lee. 2016. Identifying ECUs Using Inimitable Characteristics of Signals in Controller Area Networks. *CoRR* abs/1607.00497 (2016). arXiv:1607.00497 http://arxiv.org/abs/1607.00497

[13] David Formby, Preethi Srinivasan, Andrew Leonard, Jonathan Rogers, and Raheem Beyah. 2016. Who's in Control of Your Control System? Device Fingerprinting for Cyber-Physical Systems. In *NDSS*.

[14] Jonathan Goh, Sridhar Adepu, Khurum Nazir Junejo, and Aditya Mathur. 2017. A Dataset to Support Research in the Design of Secure Water Treatment Systems. In *Critical Information Infrastructures Security*, Grigore Havarneanu, Roberto Setola, Hypatia Nassopoulos, and Stephen Wolthusen (Eds.). Springer International Publishing, Cham, 88–99.

[15] Dieter Gollmann and Marina Krotofil. 2016. *Cyber-Physical Systems Security*. Springer Berlin Heidelberg, Berlin, Heidelberg, 195–204. https://doi.org/10.1007/978-3-662-49301-4_14

[16] Tadayoshi Kohno, Andre Broido, and KC Claffy. 2005. Remote physical device fingerprinting. *IEEE Transactions on Dependable and Secure Computing* 2, 2 (April 2005), 93–108. https://doi.org/10.1109/TDSC.2005.26

[17] Marina Krotofil, Alvaro A. Cárdenas, Bradley Manning, and Jason Larsen. 2014. CPS: Driving Cyber-physical Systems to Unsafe Operating Conditions by Timing DoS Attacks on Sensor Signals. In *Proceedings of the 30th Annual Computer Security Applications Conference (ACSAC '14)*. ACM, New York, NY, USA, 146–155. https://doi.org/10.1145/2664243.2664290

[18] Edward A. Lee. 2008. Cyber Physical Systems: Design Challenges. In *2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC)*. 363–369. https://doi.org/10.1109/ISORC.2008.25

[19] Aditya P. Mathur and Nils O. Tippenhauer. 2016. SWaT: a water treatment testbed for research and training on ICS security. In *2016 International Workshop on Cyber-physical Systems for Smart Water Networks (CySWater)*. 31–36. https://doi.org/10.1109/CySWater.2016.7469060

[20] D.C. Montgomery. 2009. *Introduction to Statistical Quality Control*. Wiley.

[21] Mujeeb Ahmed, Aditya Mathur, and Martin Ochoa. 2017. NoiSense: Detecting Data Integrity Attacks on Sensor Measurements using Hardware based Fingerprints. *ArXiv e-prints* (Dec. 2017). arXiv:cs.CR/1712.01598

[22] P. S. Murvay and B. Groza. 2014. Source Identification Using Signal Characteristics in Controller Area Networks. *IEEE Signal Processing Letters* 21, 4 (April 2014), 395–399. https://doi.org/10.1109/LSP.2014.2304139

[23] Youngseok Park, Yunmok Son, Hocheol Shin, Dohyun Kim, and Yongdae Kim. 2016. This Ain't Your Dose: Sensor Spoofing Attack on Medical Infusion Pump. In *10th USENIX Workshop on Offensive Technologies (WOOT 16)*. USENIX Association, Austin, TX. https://www.usenix.org/conference/woot16/workshop-program/presentation/park

[24] Qadeer R., Murguia C.and Ahmed C.M., and Ruths J. 2017. Multistage Downstream Attack Detection in a Cyber Physical System. In *CyberICPS Workshop 2017, in conjunction with ESORICS 2017*.

[25] Hocheol Shin, Yunmok Son, Youngseok Park, Yujin Kwon, and Yongdae Kim. 2016. Sampling Race: Bypassing Timing-based Analog Active Sensor Spoofing Detection on Analog-digital Systems. In *Proceedings of the 10th USENIX Conference on Offensive Technologies (WOOT'16)*. USENIX Association, Berkeley, CA, USA, 200–210. http://dl.acm.org/citation.cfm?id=3027019.3027037

[26] Yasser Shoukry, Paul Martin, Yair Yona, Suhas Diggavi, and Mani Srivastava. 2015. PyCRA: Physical Challenge-Response Authentication For Active Sensors Under Spoofing Attacks. In *Proceedings of the 22Nd ACM SIGSAC Conference on Computer and Communications Security (CCS '15)*. ACM, New York, NY, USA, 1004–1015. https://doi.org/10.1145/2810103.2813679

[27] Yunmok Son, Hocheol Shin, Dongkwan Kim, Youngseok Park, Juhwan Noh, Kibum Choi, Jungwoo Choi, and Yongdae Kim. 2015. Rocking Drones with Intentional Sound Noise on Gyroscopic Sensors. In *Proceedings of the 24th USENIX Conference on Security Symposium (SEC'15)*. USENIX Association, Berkeley, CA, USA, 881–896. http://dl.acm.org/citation.cfm?id=2831143.2831199

[28] A. Sridhar and M. Aditya. 2016. Generalized Attacker and Attack Models for Cyber Physical Systems. In *40th IEEE COMPSAC*.

[29] Timothy Trippel, Ofir Weisse, Wenyuan Xu, Peter Honeyman, and Kevin Fu. 2017. WALNUT: Waging Doubt on the Integrity of MEMS Accelerometers with Acoustic Injection Attacks. In *2017 IEEE European Symposium on Security and Privacy (EuroS P)*. 3–18. https://doi.org/10.1109/EuroSP.2017.42

[30] C.S. van Dobben de Bruyn. 1968. *Cumulative sum tests : theory and practice*. London : Griffin.

[31] Shoukry Yasser, Martin Paul, Tabuada Paulo, and Srivastava Mani. 2013. Non-invasive Spoofing Attacks for Anti-lock Braking Systems. In *CHES, Springer Link*, Vol. 8086. 55–72.

Table 5: Executed Attacks on SWaT Testbed from reference [14]

Attack Sequence Number	Start Time	End Time	Attack Point	Start State	Attack	Expected Impact or Attacker Intent
1	28/12/2015 10:29:14	10:44:53	MV-101	MV-101 is closed	Open MV-101	Tank overflow
2	28/12/2015 10:51:08	10:58:30	P-102	P-101 is on where as P-102 is off	Turn on P-102	Pipe bursts
3	28/12/2015 11:22:00	11:28:22	LIT-101	Water level between L and H	Increase by 1 mm every second	Tank Underflow; Damage P-101
7	28/12/2015 12:08:25	12:15:33	LIT-301	Water level between L and H	Water level increased above HH	Stop of inflow; Tank underflow; Damage P-301
8	28/12/2015 13:10:10	13:26:13	DPIT-301	Value of DPIT is <40kpa	Set value of DPIT as >40kpa	Backwash process is started again and again; Normal operation stops; Decrease in water level of tank 401. Increase in water level of tank 301
10	28/12/2015 14:16:20	14:19:00	FIT-401	Value of FIT-401 above 1	Set value of FIT-401 as <0.7	UV shutdown; P-501 turns off; UV did not shutdown; P-501 did not turn off
11	28/12/2015 14:19:00	14:28:20	FIT-401	Value of FIT-401 above 1	Set value of FIT-401 as 0	UV shutdown; P-501 turns off
13	29/12/2015 11:11:25	11:15:17	MV-304	MV-304 is open	Close MV-304	Halt of stage 3 because change in the backwash process
14	29/12/2015 11:35:40	11:42:50	Mv-303	MV-303 is closed	Do not let MV-303 open	Halt of stage 3 because change in the backwash process
16	29/12/2015 11:57:25	12:02:00	LIT-301	Water level between L and H	Decrease water level by 1mm each second	Tank Overflow
17	29/12/2015 14:38:12	14:50:08	MV-303	MV-303 is Closed	Do not let MV-303 open	Halt of stage 3 because change in the backwash process
21	29/12/2015 18:30:00	18:42:00	MV-101, LIT-101	MV-101 is open; LIT-101 between L and H	Keep MV-101 on continuously; Value of LIT-101 set as 700 mm	Tank overflow
22	29/12/2015 22:55:18	23:03:00	UV-401, AIT-502, P-501	UV-01 is on; AIT-502 is <150; P-501 is open	Stop UV-401; Value of AIT502 set as 150; Force P-501 to remain on	Possible damage to RO
25	30/12/2015 10:01:50	10:12:01	LIT-401, P-401	Value of LIT-401 <1000; P-402 is on	Set value of LIT-401 as 1000; P402 is kept on	Tank underflow
26	30/12/2015 17:04:56	17:29:00	P-101, LIT-301	P-101 is off; P-102 is on; LIT-301 is between L and H	P-101 is turned on continuously; Set value of LIT-301 as 801 mm	Tank 101 underflow; Tank 301 overflow
27	31/12/2015 01:17:08	01:45:18	P-302, LIT-401	P302 is on, LIT401 Is between L and H	Keep P-302 on continuously; Value of LIT401 set as 600 mm till 1:26:01	Tank overflow
30	31/12/2015 15:47:40	16:07:10	LIT-101, P-101, MV-201	P-101 is off; MV-101 is off; MV-201 is off; LIT-101 is between L and H; LIT-301 is between L and H	Turn P-101 on continuously; Turn MV-101 on continuously; Set value of LIT-101 as 700 mm; P-102 started itself because LIT301 level became low	Tank 101 underflow; Tank 301 overflow
31	31/12/2015 22:05:34	22:11:40	LIT-401	Water level between L and H	Set LIT-401 to less than L	Tank overflow
32	1/01/2016 10:36:00	10:46:00	LIT-301	Water level between L and H	Set LIT-301 to above HH	Tank underflow; Damage P-302
33	1/01/2016 14:21:12	14:28:35	LIT-101	Water level between L and H	Set LIT-101 to above H	Tank underflow; Damage P-101
35	1/01/2016 17:18:56	17:26:56	P-101; P-102	P-101 is on; P-102 is off	Turn P-101 off; Keep P-102 off	Stops outflow
36	1/01/2016 22:16:01	22:25:00	LIT-101	Water level between L and H	Set LIT-101 to less than LL	Tank overflow
39	2/01/2015 11:43:48	11:50:28	FIT-401, AIT-502	In Normal Range	Set value of FIT-401 as 0.5; Set value of AIT-502 as 140 mV	UV will shut down and water will go to RO UV did not shutdown
40	2/01/2015 11:51:42	11:56:38	FIT-401	In Normal Range	Set value of FIT-401 as 0	UV will shut down and water will go to RO P-402 did not close, both should be interlinked
41	2/01/2015 13:13:02	13:40:56	LIT-301	Water level between L and H	decrease value by 0.5 mm per second	Tank overflow Rate of decrease in water level reduced after 1:33:25 PM