State-Aware Anomaly Detection for Industrial Control Systems

Hamid Reza Ghaeini
Singapore University of Technology and Design
487372, Singapore
ghaeini@acm.org

Daniele Antonioli
Singapore University of Technology and Design
487372, Singapore
daniele_antonioli@mymail.sutd.edu.sg

Ferdinand Brasser
Technische Universitat Darmstadt
D-64293 Darmstadt, Germany
ferdinand.brasser@trust.tu-darmstadt.de

Ahmad-Reza Sadeghi
Technische Universitat Darmstadt
D-64293 Darmstadt, Germany
ahmad.sadeghi@trust.tu-darmstadt.de

Nils Ole Tippenhauer
Singapore University of Technology and Design
487372, Singapore
nils_tippenhauer@sutd.edu.sg

ABSTRACT

Anomaly detection for industrial control systems (ICS) can leverage process data to detect malicious derivations from expected process behavior. We propose state-aware anomaly detection that uses state dependent detection thresholds, which provide tighter constraints for an attacker trying to manipulate the process. In particular, our system provides: (i) estimation of system state from the knowledge of the network and the physical process (ii) a state-aware cumulative sum of residuals for monitoring the industrial control system (iii) and a novel state-aware anomaly detection technique. We implement and evaluate our anomaly detection technique on a real-world ICS. We pre-compute the process-state parameters using a big data framework for ICS and train the detector leveraging more than 120 GB of historical data from the ICS. The results show that the proposed method improves prior works by providing less time-to-detect of attacks while generating fewer false alarms.

CCS CONCEPTS

• **Security and privacy → Intrusion detection systems**; *Embedded systems security*; • **Computer systems organization →** *Embedded and cyber-physical systems*;

KEYWORDS

Industrial Control System; Anomaly Detection; Process State; Residual; CUSUM

ACM Reference Format:
Hamid Reza Ghaeini, Daniele Antonioli, Ferdinand Brasser, Ahmad-Reza Sadeghi, and Nils Ole Tippenhauer. 2018. State-Aware Anomaly Detection for Industrial Control Systems. In *SAC 2018: SAC 2018: Symposium on Applied Computing , April 9–13, 2018, Pau, France.* ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/3167132.3167305

SAC 2018, April 9–13, 2018, Pau, France

ACM ISBN 978-1-4503-5191-1/18/04…$15.00
https://doi.org/10.1145/3167132.3167305

1 INTRODUCTION

Industrial control systems (ICS) are complex systems able to autonomously monitor and control an industrial process. An ICS includes heterogeneous interconnected components such as: remote terminal unit (RTU), programmable logic controller (PLC), telemetry system, historian server, and human-machine interface (HMI). Those component are typically reachable over the Internet and connected to other embedded devices resulting in a setup known as the Industrial Internet of Things (IIoT). ICS are designed for safety and availability, however, security is recently being taken into consideration given the number of cyber and physical threats that are menacing the ICS space [11, 13].

There are promising proposals that try to perform stateful anomaly detection based on the state of the ICS physical process [3, 12, 19]. For example, in [19] a stateful detection mechanism based on the use of cumulative sum (CUSUM) of residuals is proposed. This detector raises the bar for a stealthy attacker. However, it suffers from calibration problems due to its lack of knowledge of the current system state. The main limitation of existing works is that an attacker will remain undetected below a threshold while leveraging on sensors and actuators variations due to the different system states.

As result, the attacker could control the process-state while remaining undetected which threatens the industrial control system. Our paper proposes a state-aware anomaly detection scheme based on CUSUM detection mechanism. The computation of the residual depends on the current system state and this will result in even tighter bound for the stealthy attacker. Furthermore, our proposed detection mechanism adds little pre-computation overhead in terms of computation with respect to the work [19] because we pre-compute the physical process state information using our big data framework, and then configure the detector accordingly.

We evaluate the performance of our detection mechanism against state-of-the-art stateful ones, such as [17], in a real water treatment testbed. We show that a stealthy attack that remains undetected by such detectors will be detected by our detector. This confirms our intuition about tighter constraints for a stealthy attacker who is trying to manipulate the ICS physical process.

We summarize our contributions as follows:

- We design and implement a CUSUM-based state-aware anomaly detection scheme for industrial control systems.
- We propose a way to compute CUSUM residuals based on the current system state without incurring in major computation overhead by pre-computing the states' information.
- We evaluate our scheme against state-of-the-art stateful detection mechanism on a real water treatment testbed. We show that our detector provides tighter bounds for the stealthy attacker, and lower exposure time than the others.

The remainder of this paper organized as follows. Section 2 provides a context of the testbed, and the HAMIDS framework. In Section 3 we present our proposed framework. We describe our use-case in Section 4. Section 5 demonstrates the implementation and results of experimental validation. We summarize the related works at Section 6. Finally, the paper concludes with Section 7.

1(a) The SWaT, testbed of this paper.

1(b) Raspberry Pi devices next to the PLCs.

Figure 1: The ICS of this paper.

2 BACKGROUND

In this section, we introduce the relevant background about the Secure Water Treatment (SWaT), and the HAMIDS framework. We conclude the section with a discussion about stateful anomaly detection, and measurements of the water tank levels.

2.1 SWaT Testbed

The SWaT (Secure Water Treatment) [10] is a six-stage process plant of industrial water treatment systems, designed for cyber-physical security research. The general research goal of operating such plant is to advance the safety and security of critical infrastructures. In particular, it is intended to improve the safety and security of Cyber-Physical Systems (CPS) such as water treatment systems, power grids, and oil and natural gas refineries.

Initially, the SWaT plant receives the raw water in the first process, and it adds some chemicals to the received raw water. At the ultrafiltration process, the received water will filter, and then it will push to dechlorination by using UV lamps. Then, the water will be clean in the reverse osmosis process. Figure 1a shows the SWaT testbed.

2.2 HAMIDS framework

The HAMIDS (HierArchical Monitoring Intrusion Detection System) [6] is a framework that designed for security analysis and research in Industrial Control Systems field. This framework provides a device-level knowledge of the industrial applications by parsing industrial network protocols. In addition, it provides a platform for other researchers to perform industrial process analysis, safety or security analysis. The main component of packet parser of the HAMIDS framework is Bro that implemented to provide a high-level knowledge of industrial network traffic. We used a cluster setup of the Bro with cluster manager as depicted in Figure 4. By using the cluster, high-level knowledge of industrial network protocols will collect at a central server for further analysis and processing. The HAMIDS framework was designed to support CIP and EtherNet/IP traffic parsing, and traffic handlers will trigger on traffic using ports relating to both CIP and EtherNet/IP. The hierarchical aspect of the HAMIDS framework refers to the detection of several layers and segments of the ICS network, aggregated at the cluster manager. The visualization and data analysis component of this paper builds up at the top of the HAMIDS framework. The authors of [1] discussed the performance of the HAMIDS framework in a real intrusion test by invited intruders.

2.3 Stateful Anomaly Detection with CUSUM

The Cumulative Sum (CUSUM) algorithm was proposed in [18, 19] to offer a stateful aggregation and detection of anomalies based on residuals. These methods use the history of the system state for anomaly detection. Typically, they can limit the impact of stealthy attacks with better performance than stateless techniques that only consider the current state of the system.

Residuals. A stateless detection technique will raise an alarm if the absolute difference between the sensor reading and estimated system state was higher than a threshold. We call this absolute difference the residual estimation. The residual is defined as:

$$r_k = |y_k - \hat{y_k}| \tag{1}$$

CUSUM. The non-parametric CUmulative SUM (CUSUM) statistic is recursively computed as follows:

$$S_k = \begin{cases} 0 & \text{where } k = 0 \\ (S_{k-1} + r_k - \alpha)^+ & \text{where } k \neq 0 \end{cases} \tag{2}$$

where $(x)^+$ means $max(0, x)$ and α is the tuning value that selected to keep $|r_k| - \alpha < 0$ under a normal operation. However, we argue that this is not a perfect CUSUM computation as hypothesis H_0 contains different states of the system, and for each state there are different tuning parameters. The authors of [19] proposed a state-independent CUSUM computation. The anomaly detector raises an alarm when the CUSUM passes the threshold. Then the CUSUM test will be restarted after passing the threshold at time k, i. e., $S_{k-1} = 0$.

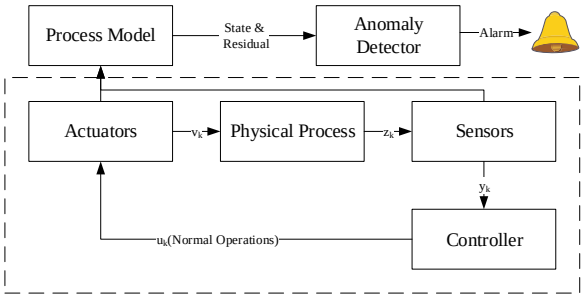


Figure 2: The framework structure.

2.4 Water Level Sensor

The demand for process control and stringent regulatory environment drive industrial control engineers to design more reliable level measurement systems. There are different proposals for water level sensors including (i) Floats, (ii) Hydrostatic Devices, (iii) Load Cells, (iv) Magnetic Level Gauges, (v) Capacitance Transmitters, (vi) Magnetostrictive Level Transmitters, (vii) Ultrasonic Level Transmitters, and (viii) Laser Level Transmitters.

In SWaT, the water tank level sensor is an ultrasonic level sensor that reliably and precisely measures the level of the water in the water tank. Table 1 describes features of the water tank level sensor of the SWaT testbed. The most important causes of noise in the water level measurement process are: (i) Accuracy level of the sensor (ii) Water movement in the tank

3 STATE-AWARE ANOMALY DETECTION

In this section, we describe our stateful process state-aware anomaly detection method for industrial control network traffic. In [19], CUSUM-based detectors for attacks on ICS are discussed. The authors note that the detector is mitigating the attack, but not entirely prevent it. In particular, attacks will remain undetected unless their impact passes a fixed threshold. As a result, an intelligent attacker might remain undetected while she is performing the attack. We note that the parametrization of the CUSUM-based detector is essential for the performance of such a countermeasure, which motivated this work. In particular, we consider the following questions:

1. How can we optimize the computation of the residual according to the state of the physical process?
2. Is it reasonable to use the process-states in overall CUSUM computation?

Table 1: Water tank level sensor specifications.

	Parameter	Specification
1	Name	Level Wizard II 10 DB
2	Accuracy	max(+/-0.25%, 6 mm)
3	Resolution	max(0.1%, 2 mm)
4	Maximum Range	10 meters
5	Operating frequency	41 kHz

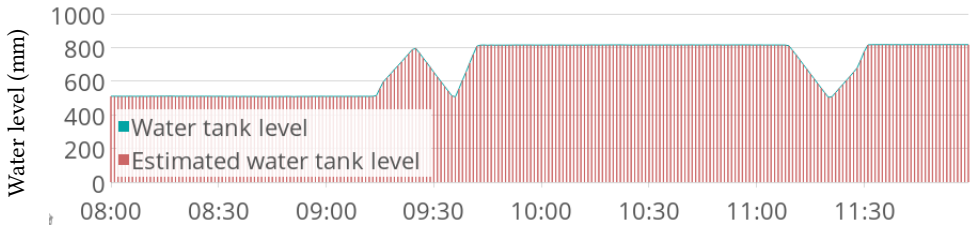
Attacker and System Model. The system under attack is an industrial process with automatic controls. A number of sensors are used to monitor the physical process. We assume that the sensors are not controlled by the adversary and they provide correct sensor readings. Those readings are then used for automatic control by local PLCs and the SCADA system. A detection system is used to mitigate the impact of an attack. The detection system could use data collected by the sensors directly, or obtain processed data from the PLCs or even from the SCADA and the historian server.

The attacker's goal is to manipulate the physical process to change its state to unsafe conditions (e.g., to damage the system), or to decrease the overall efficiency of the system. The attacker is able to manipulate network traffic of both the supervisory control network and the field communications network. The authors of [17] discussed the impact of the attacking Fieldbus communication. In [19] the authors proposed physical modeling to limit the impact of a Fieldbus attacks. To evaluate our proposed state-aware anomaly detection, we used the *intelligent attack against tank level* discussed in [18]. The attacker slowly changes the sensor reading of a tank level using a small constant increment trying to remain undetected.

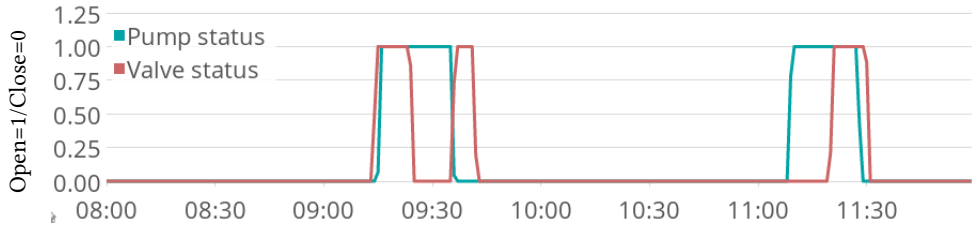
Framework Overview. The structure of the framework is summarized in Figure 2. A physical process is observed, in particular, the traffic containing control and sensor values, together with general traffic exchanged in the network. Those values are processed by the IDS to generate the required parameters for the anomaly detection. During the real-time detection, the anomaly detector determines the current state of the physical process and uses that input to choose appropriate parameters (e.g., mean of residuals in normal operation) for anomaly detection.

3.1 Physical Anomalies

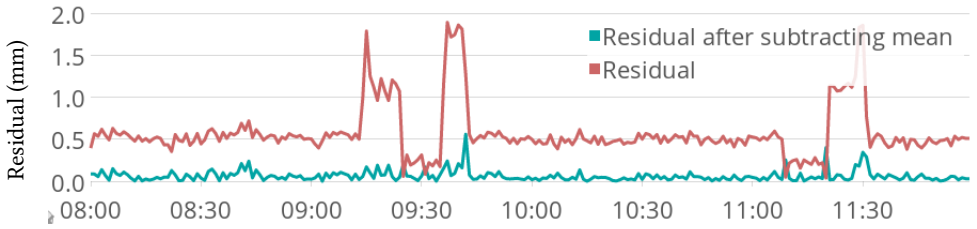
Physical Process Model. The physical system behavior model can be learned from observations through a technique called system identification. The most used models are Auto-Regressive (AR) models and Linear Dynamical State-space (LDS) models. We used



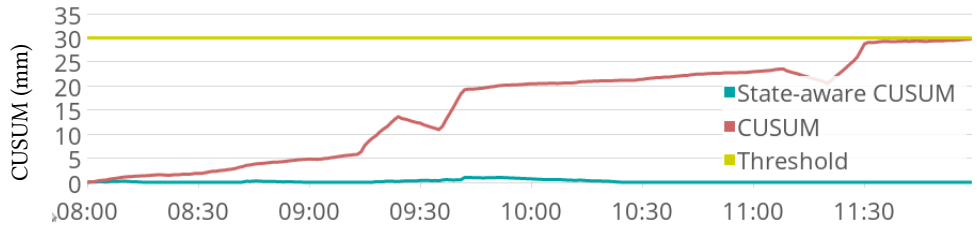
3(a) Water tank level reading and estimation.



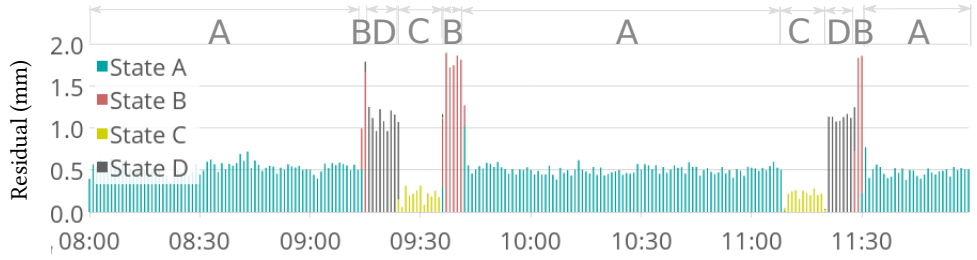
3(b) Pump and valve status.



3(c) Residual of water tank reading.



3(d) Cumulative sum of residuals.



3(e) Residuals of water tank reading and different states.

Figure 3: Sensor readings, estimates, and residuals in non-attack case.

Linear Dynamical State-Space (LDS) model in our work. LDS models are a subset of state space models. Consider that the inputs (control commands u_k) and outputs (sensor measurements y_k) of the physical system are available. The dynamic modeling of the physical system will be:

$$x_{k+1} = Ax_k + Bu_k + \epsilon_k$$
$$y_k = Cx_k + Du_k + e_k \quad (3)$$

where A, B, C, and D are modeling metrics of the dynamics of the physical system, e_k and ϵ_k are sensor and perturbation noise. We will see in physical modeling part how we will use the LDS to model our physical system.

State observer. State observers are used to dynamically provide an estimation of the system with and without the noise. Industrial processes consist of a variety of states. Here, we consider the process states in our computation as an input of the anomaly detection system. There are many proposals for estimation of the state of a dynamic system such as Luenberger observers [16] and the Kalman filter [2]. Those techniques are used to dynamically estimate the system state with and without the noise, respectively. They provide a stateless detection and their drawbacks are discussed in [19]. Interested readers are encouraged to read [17, 18]. In this paper, we consider the sensor noise as a significant parameter for system state detection. In addition, we will consider the process state impact on the sensor noise model.

Process-State Dependent Residual Computation. Consider p as process state of the industrial component that we are modeling. Instead of computing the residual as defined before (i.e., $r = |y - \hat{y}|$), we now introduce a process state-dependent way to compute the residual. In particular, we normalize the residual with its historical average μ_p for the current process state p:

$$r[t,p] = ||y[t] - \hat{y}[t]| - \mu_p| \quad (4)$$

where y is the observed sensor value, and $\hat{y}$ is the output of the observer, i.e. the estimate sensor value computed by Equation 3.

Computation of μ_p. μ_p is computed from historical data of the ICS physical process while being in different process states. We assume that during data collection time, no attack was conducted. Then, we compute μ_p from the average of all residuals computed while the process was in state p:

$$\mu_p = \mathbb{E}(r[t,p])\ \forall t \text{ where process state } = p \quad (5)$$

Process-State Dependent CUSUM Parameters. Based on the process-state dependent residual as defined in Equation 4, we use the CUSUM computation as follows:

$$S_k = \begin{cases} 0 & \text{where } k = 0 \\ (S_{k-1} + |r_k - \mu_p| - \alpha)^+ & \text{where } k \neq 0 \end{cases} \quad (6)$$

where $(x)^+$ is the $max(0, x)$ and α is the tuning value that we selected to keep $|r_k - \mu_p| - \alpha < 0$ under a normal operation. We argue that this is a better CUSUM computation under hypothesis H_0 that consider states of the system and for each state, it uses μ_p as tuning parameter. The anomaly detector raises an alarm when the CUSUM passes the threshold. Then the CUSUM test will be restarted after passing the threshold at time k, i. e., $S_{k-1} = 0$.

4 USE CASE: WATER TANK IN SWAT

Process States for Water Tank Process. Consider the water tank filling of PLC1 as a process. It has two states for In-flow and Out-flow. As result, we have four distinct process states. Our model depends on the process states. Figure 3b depicts the process states based on the pump and valve status. In addition, Figure 3a demonstrates the tank level corresponding to the process state of Figure 3b. Figure 3c demonstrates level sensor residual imposed from different water tank process states. As we could see in Figure 3c when both pump and valve is closed the level sensor noise is low (State A). When the pump is open, and the valve is closed, the water tank level sensor residual will decrease as presented in Figure 3c (State C). This water tank level sensor residual decrement is caused by the placement of the pump and the decreasing water level. When the valve is open and the pump is closed, a volume of water that is pushed into the tank will cause water level distortion as depicted in Figure 3c (State B). Finally, when both valve and pump is open the residual would be as depicted in Figure 3c (State D). We extract the mean of water tank level residual for further processing of CUSUM. Table 2 present the computed mean of the residual of these four states as depicted in Figure 3c.

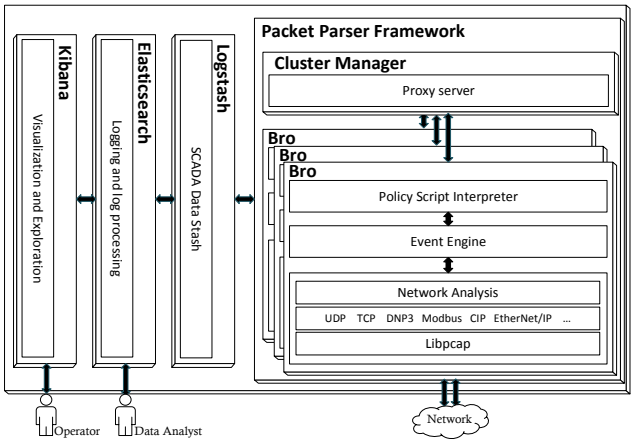


Figure 4: Implemented big data framework.

Table 2: Computed mean of water tank level residuals, P is the pump status and V is the valve status, P means that the pump is on and $\neg P$ means the pump is off.

State	Boolean Algebra	Mean
A	$\neg P \wedge \neg V$	0.48
B	$\neg P \wedge V$	1.65
C	$P \wedge \neg V$	0.25
D	$P \wedge V$	1.15

4.1 Residuals in non-attack case

System Model of Water Tank.

Consider the tank level h concerning incoming Q^{in} and outgoing Q^{out} volume of water. Then, the cross-sectional area of the base of the tank will be:

$$Area\frac{dh}{dt} = Q^{in} - Q^{out} \quad (7)$$

By performing a discretization the time with a period of one second, the physical model of the tank level will be [18]:

$$h_{k+1} = h_k + \frac{Q_k^{in} - Q_k^{out}}{Area} \tag{8}$$

Note that Equation 8 represents an LDS model because the input $Q_k^{in} - Q_k^{out}$ changes over time [18]. To detect anomalies in the reported tank level, our system continuously models the current state of each tank with such a linearized stateful model. Thus, we are able to obtain an estimate of the tank level for each time step. Deducting the estimated tank level from the reported value, we obtain a residual which is then used for the anomaly detection.

In Figure 3, we show example values for normal systems operations with high water movement. The provided example is not occurring frequently during the water treatment process, and the intuition behind this case is to provide a clear differentiation between the proposed method and [19] under a system with normal operation. In particular, we compared the observed and estimated tank level, the states of valves and pumps (to derive component states), the related residuals (r and $r[p]$), and CUSUM computations. It can be noted that for the provided example sequence of operations, the CUSUM with static α is increasing over time, and would eventually cross any threshold.

4.2 Residuals in attack case

We consider that the attacker knows our detection strategy and tries to avoid detection. An optimal greedy attacker (y^{a*}) at time t will try to maximize the residual while remaining below the threshold.

$$y_{k+1}^{a*} = \begin{cases} \arg\max_{y_{k+1}}^{a} |y_{k+1} - y_{k+1}^{a}| \\ \arg\min_{y_{k+1}}^{a} |y_{k+1} - y_{k+1}^{a}| \end{cases} \tag{9}$$

The attacker goal in stateless detection techniques will be:

$$y_{k+1}^{a*} = \hat{y_{k+1}} \pm \tau \tag{10}$$

Discussion about the stateless techniques is out of the scope of this paper. The attacker goal in stateful detection techniques will be:

$$y_{k+1}^{a*} = \max\{y_{k+1} : S_{k+1} \leq \tau\} \tag{11}$$

The CUSUM computed by Equation 2. A greedy optimal attacker tries to not pass the threshold of CUSUM, i. e., $S_K = \tau$. Hence, the attacker goal will be:

$$y_{k+1}^{a*} = \hat{y_{k+1}} \pm (\tau + \alpha - S_k) \tag{12}$$

As proposed in Section 3.1 by using Equation 6 the attacker goal while the system process is in state p will be:

$$y_{k+1}^{a*} = \hat{y_{k+1}} \mp \mu_p \pm (\tau + \alpha - S_k) \tag{13}$$

As depicted in Figure 5 the attacker try to remain beyond the threshold while performing the attack. As the attacker knows our attack detection model the optimal attack could be performed when the process has lowest μ_p or highest μ_p, depending whether she choose arg min or arg max in Equation 9.

4.3 State-Aware Detector

The authors of [17–19] used a constant threshold CUSUM to detect the attacks in Fieldbus. Alongside the static threshold, we use the process state to determine the effect of the sensor and water movement in computed residual. As Figure 3c shows our proposed state aware residual will remain smooth during a normal operation of the industrial control system. Hence, it will not increase the CUSUM to generate a false alarm (Figure 3d). During the attack (as depicted in Figure 5c) our proposed method will react to anomalies and it will increase the CUSUM similar to the work [19](Figure 5d).

5 IMPLEMENTATION AND EVALUATION

We now present the implemented proposed framework, which is continuously monitoring the operations of the SWaT system. The HAMIDS framework is used to process the industrial network traffic, and detect events (see Section 2). Those detected events are then stored in a central cluster. We now provide further details on the central cluster, and the distributed IDS components used.

5.1 Implementation Challenges

The proposed method need handling a huge amount of data to produce our detection model. These data will be collected from the history of the normal operation of the plant. Overall, our distributed framework generates about 4000 log entries per minute depending on the running physical process, with a size of between 20 GB to 50 GB per day after compression. We used data recorded for three days. Our big data framework processed about 120 GB of data to produce the detection model.

5.2 IDS components

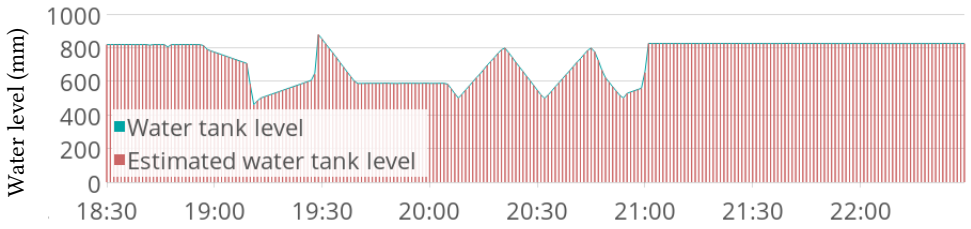
Traffic Collection and Analysis. We leveraged six Raspberry Pi 3 devices to collect and analyzed the industrial traffic in the different network segments. Those Raspberry Pi devices are placed in the PLCs (Figure 1b) and pass the useful data from PLCs to our central cluster.

5.3 Big-Data Framework

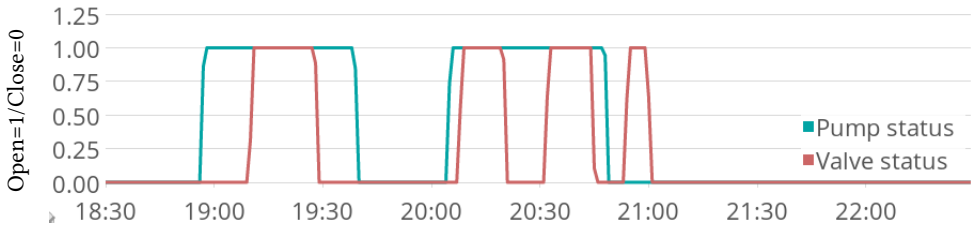
The central cluster is running on a machine with 12 (logical) CPU cores and 20GB of RAM, running Ubuntu server 16.04. In the central cluster, we use the Elastic stack to provide real-time log recording and processing (see Figure 4). This is the heart of our big data processing framework. It will store more than seven days history of the industrial control process.

Logstash. Logstash is an open-source data collection and log parsing engine that used as an interface between the HAMIDS framework and Elasticsearch. The Logstash parser was designed to extract the industrial network protocol commands like EtherNet/IP commands. It intended to parse the packets containing the states and values of industrial sensors and actuator. We used Ruby scripting to provide processed data for log recording and processing at the Elasticsearch.

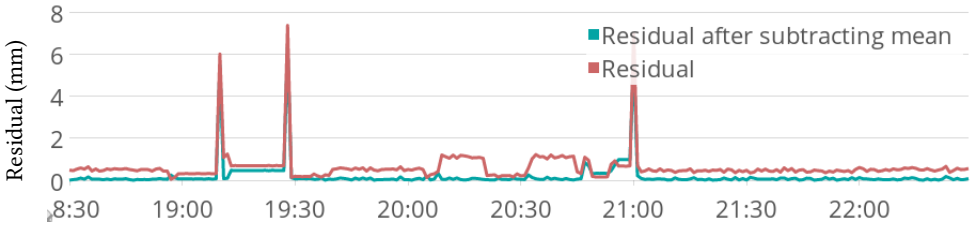
Elasticsearch. Elasticsearch is an open-source search engine that provides a distributed full-text search engine with JSON documents and an HTTP web interface. Its compatibility with other log processing software offers a broad range of functionalities for Elasticsearch.



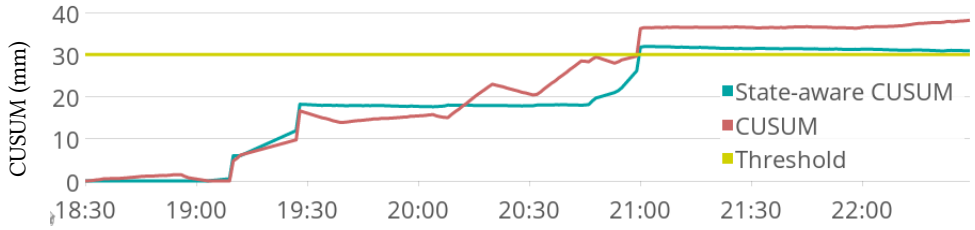
5(a) Water tank level reading and estimation.



5(b) Pump and valve status.



5(c) Residual of water tank reading.



5(d) Cumulative sum of residuals.

Figure 5: Sensor readings, estimates, and residuals in non-attack case.

The distribution feature of the Elasticsearch enables it to process an enormous amount of data and also the capability of stream processing that is the fundamental necessity of on-line intrusion detection systems.

Kibana. Kibana is an open-source analysis and visualization platform of the Elastic stack that is used in most of data and security analysis projects. Kibana visualizes the indexed content on the Elasticsearch cluster and provides a fantastic dashboard for its user so that they could quickly analyze the data. In our proposed framework we provide a dashboard for the industrial operator to monitor the industrial control system securely and have an in-depth knowledge of the ongoing industrial process directly both in the PLCs and at the level 1 of the industrial control network. Figure 4 depicts the elements of the implemented framework.

5.4 Evaluation

Scenario. To evaluate the proposed framework we performed cyber and physical attacks in the SWaT. The network-based intrusion detection system discussed in [6] is out of the scope of this paper. To evaluate our proposed detection technique, we perform three cyber-physical attacks that intercept the industrial control traffic and manipulate the traffic to change the sensor reading values. In this scenario, we assume that the adversary mounts a man-in-the-middle attack in the Fieldbus network with the following goals:

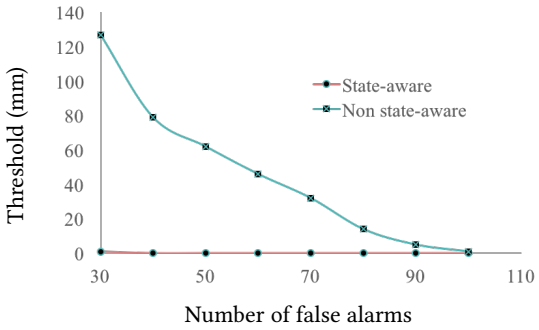
- *Goal 1 (MitM)* Intercept the industrial process network traffic.
- *Goal 2 (Manipulation)* Change the tank level while it remains beyond the threshold of both stateless and stateful detection techniques.

In other words, the attacker will launch the attack at certain points of the process state that have high or low residuals. The attacker tries to change the values in a way that the caused residual will not pass *three times of the residuals seen in normal operation* after removing the attack. In this way stateless or the stateful detection techniques are not able to detect the attack.

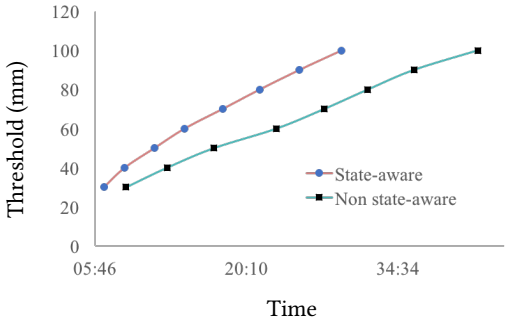
Physical anomaly detection. The physical processes follow specific physical model that could be used to verify the ongoing process in the industrial control system components. As proposed in [19], physical modeling techniques will look at the received physical measurements to detect anomalies in physical processes. Here, we focus on the water tank level and the status of pumps and valves of the process. To perform a comprehensive evaluation of physical modeling we implemented the works [17–19] in our framework. There are residuals between estimated water tank level and received water tank level. As depicted in Figure 5a attacker choose the state C in her attack and intelligently reduce the water tank level with an angle lower than its normal angle to maintain the pump open for five more seconds. Then, the attacker stops her attack. This will cause a distortion in residual as depicted Figure 5c below the stateless detection thresholds. Then, she continues her attack when both pump and valves are open (state D). The goal is to keep the valve open for more 5 seconds. As Figure 5c shows, this will lead to higher residuals while the CUSUM of residuals remains below the stateless detection thresholds. Finally, the attacker chooses state B that has highest residuals.

Based on [19] the detector will detect these type of attacks after passing a specific threshold of CUSUM. However, the chosen threshold will not be reached during our implemented attack. This is while our detection mechanism will react to the attack from its start point and after passing the threshold, it will raise the alarm. The minimum proposed threshold of [19] is 300mm, and we chose 30mm as threshold due to the preciseness of proposed process-state aware anomaly detection system. We chose the threshold of proposed detection technique based on the behavior of CUSUM based detection technique in normal operation.

Figure 6a presents the number of false alarms generated during a one-day normal operation of SWaT when using different thresholds from 10 to 100. As this figure depicts, the best threshold that we could use is 30mm as its false alarms during the normal operation is close to zero. The comparison between our proposed method and the work [19] shows that our proposed method provides less false alarms compared to existing state-of-the-art stateful detection mechanisms. Figure 6b demonstrates the time-to-detect of a launched attack to increase the tank level by keeping the valve open. As this figure shows, our method achieves a lower detection time comparing with [19]. We could conclude from Figures 6b and 6a that proposed method achieves lower attack detection time in SWaT while generating less false alarms.



6(a) Comparison between number of false alarms generated with different thresholds.



6(b) Comparison between time-to-detect of the attack with different thresholds.

Figure 6: False alarm and time-to-detect

6 RELATED WORK

Stateful Detection. Traditional non state-aware stateful detectors were proposed in combination with data analytics techniques in [4, 8].

Such detection mechanism was used to evaluate different scenarios such as detect coordinated injection attacks [5], prevent collisions in a vehicular platoon [14], and monitor the state of a security camera [20]. A window of stateful detection techniques were discussed in [9, 12, 15].

Alternative CUSUM-based detectors were also proposed, e. g., Variable Threshold Window Limited CUmulative SUM (VTWL CUSUM) [21]. State-aware detection mechanisms based on sensor values clustering are discussed in [7, 8]. An evaluation of a state-aware detector against stealthy attack is presented in [4]. The authors of [17] discussed the impact of the attacking Fieldbus communication. In [19] the authors proposed stateful CUSUM to limit the impact of Fieldbus attacks. In this paper, we used the *intelligent attack against tank level* that the attacker tries to change the sensor reading of the tank level with a constant value to remain undetected by changing the sensor measurement slowly. Our proposed method significantly improves the existing work in terms of detection rate and detection time compared to other proposed solutions like [17], [19], and [18]. We implemented these solutions in our framework and we compared them in experimental evaluation part.

7 CONCLUSIONS

In this paper, we proposed a framework for state aware anomaly detection in industrial control systems. We implemented the framework by extending the HAMIDS framework with added support for log recording, processing, analysis, and anomaly detection. Besides,

we propose a state-aware anomaly detection based on CUSUM computation. Our experimental results demonstrate that the proposed method improves existing works by providing lower exposure time while offering better detection. In particular, the proposed method decreases up to 30.66% time to detect and close false alarm rate by choosing the threshold of 100 mm. Also, the proposed method offers up to 99.21% fewer false alarm with the threshold of 30 mm and 14.50% less time to detect.

ACKNOWLEDGMENTS

We would like to thank the anonymous reviewers for their productive feedbacks and suggestions, and professor Saeed Moghimi at the Coast Survey Development Lab of National Ocean Service, Silver Spring, Maryland, for his insightful comments.

REFERENCES

[1] D. Antonioli, H. R. Ghaeini, S. Adepu, M. Ochoa, and N. O. Tippenhauer. Gamifying ICS security training and research: Design, implementation, and results of S3. In *Proceedings of the Workshop on Cyber-Physical Systems Security and PrivaCy (CPS-SPC)*, pages 93–102, New York, NY, USA, 2017. ACM.

[2] G. Bishop and G. Welch. An introduction to the kalman filter. *Proc of SIGGRAPH, Course*, 8(27599-23175):41, 2001.

[3] B. Brumback and M. Srinath. A chi-square test for fault-detection in kalman filters. *IEEE Transactions on Automatic Control*, 32(6):552–554, 1987.

[4] A. A. Cárdenas, S. Amin, Z.-S. Lin, Y.-L. Huang, C.-Y. Huang, and S. Sastry. Attacks against process control systems: risk assessment, detection, and response. In *Proceedings of the symposium on information, computer and communications security (ASIACCS)*, pages 355–366. ACM, 2011.

[5] S. Cui, Z. Han, S. Kar, T. T. Kim, H. V. Poor, and A. Tajer. Coordinated data-injection attack and detection in the smart grid: A detailed look at enriching detection solutions. *IEEE Signal Processing Magazine*, 29(5):106–115, 2012.

[6] H. R. Ghaeini and N. O. Tippenhauer. Hamids: Hierarchical monitoring intrusion detection system for industrial control systems. In *Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy (CPS-SPC)*, pages 103–111. ACM, 2016.

[7] I. Kiss, B. Genge, and P. Haller. A clustering-based approach to detect cyber attacks in process control systems. In *IEEE International Conference on Industrial Informatics (INDIN)*, pages 142–148. IEEE, 2015.

[8] M. Krotofil, J. Larsen, and D. Gollmann. The process matters: Ensuring data veracity in cyber-physical systems. In *Proceedings of the Symposium on Information, Computer and Communications Security (ASIACCS)*, pages 133–144. ACM, 2015.

[9] J. Liang, O. Kosut, and L. Sankar. Cyber attacks on ac state estimation: Unobservability and physical consequences. In *Proceedings PES General Meeting Conference & Exposition*, pages 1–5. IEEE, 2014.

[10] A. Mathur and N. O. Tippenhauer. A water treatment testbed for research and training on ICS security. In *Proceedings of Workshop on Cyber-Physical Systems for Smart Water Networks (CySWater)*, 2016.

[11] S. McLaughlin, C. Konstantinou, X. Wang, L. Davi, A.-R. Sadeghi, M. Maniatakos, and R. Karri. The cybersecurity landscape in industrial control systems. *Proceedings of the IEEE*, 104(5):1039–1057, 2016.

[12] Y. Mo, R. Chabukswar, and B. Sinopoli. Detecting integrity attacks on scada systems. *IEEE Transactions on Control Systems Technology*, 22(4):1396–1407, 2014.

[13] A.-R. Sadeghi, C. Wachsmann, and M. Waidner. Security and privacy challenges in industrial internet of things. In *Proceedings of the Annual Design Automation Conference (DAC)*, pages 54:1–54:6, New York, NY, USA, 2015. ACM.

[14] I. Sajjad, D. D. Dunn, R. Sharma, and R. Gerdes. Attack mitigation in adversarial platooning using detection-based sliding mode control. In *Proceedings of the ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy (CPS-SPC)*, pages 43–53. ACM, 2015.

[15] Y. Shoukry, P. Martin, Y. Yona, S. Diggavi, and M. Srivastava. Pycra: Physical challenge-response authentication for active sensors under spoofing attacks. In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS)*, pages 1004–1015. ACM, 2015.

[16] E. D. Sontag. *Mathematical control theory: deterministic finite dimensional systems*, volume 6. Springer Science & Business Media, 2013.

[17] D. Urbina, J. Giraldo, N. O. Tippenhauer, and A. Cárdenas. Attacking fieldbus communications in ICS: Applications to the SWaT testbed. In *Proceedings of Singapore Cyber Security Conference (SG-CRC)*, Jan. 2016.

[18] D. I. Urbina, J. Giraldo, A. A. Cardenas, J. Valente, M. Faisal, N. O. Tippenhauer, J. Ruths, R. Candell, and H. Sandberg. Survey and new directions for physics-based attack detection in control systems. *US Department of Commerce, National Institute of Standards and Technology*, 2016.

[19] D. I. Urbina, J. A. Giraldo, A. A. Cardenas, N. O. Tippenhauer, J. Valente, M. Faisal, J. Ruths, R. Candell, and H. Sandberg. Limiting the impact of stealthy attacks on industrial control systems. In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS)*, pages 1092–1105. ACM, 2016.

[20] J. Valente and A. A. Cárdenas. Using visual challenges to verify the integrity of security cameras. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, pages 141–150. ACM, 2015.

[21] L. F. Van Long Do and I. Nikiforov. A statistical method for detecting cyber/physical attacks on scada systems. In *IEEE Conference on Control Applications (CCA)*, pages 364–369.