A supervised energy monitoring-based machine learning approach for anomaly detection in a clean water supply system

1st Andres Robles-Durazno
School of Computing
Edinburgh Napier University
Edinburgh, UK
a.roblesdurazno@napier.ac.uk

2nd Naghmeh Moradpoor
School of Computing
Edinburgh Napier University
Edinburgh, UK
n.moradpoor@napier.ac.uk

3rd James McWhinnie
School of Engineering and Built Environment
Edinburgh Napier University
Edinburgh, UK
j.mcwhinnie@napier.ac.uk

4th Gordon Russell
School of Computing
Edinburgh Napier University
Edinburgh, UK
g.russell@napier.ac.uk

Abstract— ***Industrial Control Systems are part of our daily life in industries such as transportation, water, gas, oil, smart cities, and telecommunications. Technological development over time have improved their components including operating system platforms, hardware capabilities, and connectivity with networks inside and outside the organization. Consequently, the Industrial Control Systems components are exposed to sophisticated threats with weak security mechanism in place. This paper proposes a supervised energy monitoring-based machine learning approach for anomaly detection in a clean water supply system. A testbed of such a system is implemented using the Festo MPA Control Process Rig. The machine-learning algorithms, which include SVN, KNN, and Random Forest, perform classification tasks process in three different datasets obtained from the testbed. The algorithms are compared in terms of accuracy and F-measure. The results show that Random Forest achieves 5% better performance over KNN and SVM with small datasets and 4% regarding large datasets. For the time taken to build the model, KNN presents the best performance. However, its difference with Random Forest is smaller than with SVM.***

Keywords— Industrial Control System, Energy Monitoring, SCADA, KNN, Random Forest, SVM, Anomaly Detection.

I. INTRODUCTION

Industrial control systems (ICS) are widely used in critical and large industries like power plants, gas, water, oil, transportation, chemical, and pharmaceutical. ICS began to emerge decades ago and were not designed with security in mind, as they were not expected to be connected to office networks or the internet [2]. Currently, a considerable amount of ICS components can be found connected to the Internet, leading to the exposure of ICS to skilled hackers that might take advantage of their online availability with the intention to execute attacks with harmful consequences [12]. Fig 1 shows a possible integration between a corporate and industrial network. This includes three segments of: production network, SCADA, and corporate network where production network and SCADA are both part of ICS.

Attacks to ICS are not new. In 1982, an unverified report of a Trojan program inserted in a SCADA system software caused a natural gas explosion along the Trans-Siberian pipeline [11]. An attack on the Maroochy Shire sewage control system in Queensland- Australia in 2000 caused millions of litres of raw sewage to spill out into the City. The Stuxnet worm, which have been developed in 2005 but discovered in 2010, targeted the Iranian's nuclear facilities. Stuxnet is a sophisticated attack that exploited four zero-day Windows vulnerabilities to get into computers and the network. More recently, on December 2015, around 230,000 people from a small region of Ukraine suffered a power outage for few hours. This is caused by a variant of the malware which infected the power facilities and made some of the ICS's components unbootable [9]. These are just a few examples to understand the criticality of these systems for people and environment and to show that ICS face challenges with threats able to cause considerable impact.

The term ICS describes the integration of hardware and software in industrial environments [7]. Depending on the type of industry, each ICS is built to support different needs in an efficient manner. The components of an industrial process control the process by means of operating actuators, reading sensors, and Process Variables (PV) e.g. temperature, pressure, and flow [6]. One of the main components of this type of industrial network is the Programmable Logic Controller (PLC) which is an industrial solid-state computer generally composed of inputs, outputs, memory, CPU, communication modules, and a power supply [9]. The PLC was introduced in the late 60's and was designed to replace relay logic systems, however currently PLCs can also provide different capabilities such as web server, network integration and more. It monitors different types of automated process and makes logic-based decisions depending on the information provided by the components connected to it [5]. There are several types of ICS. Supervisory Control and Data

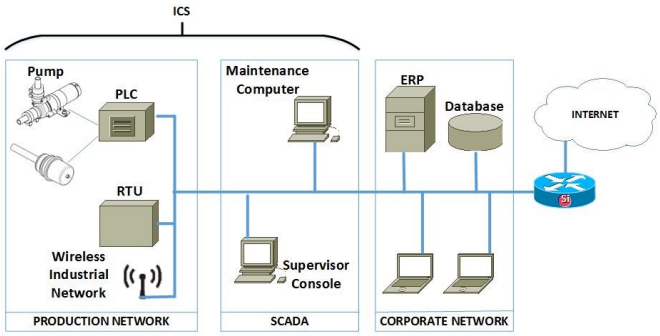

Fig. 1. Industrial Control System and Corporate Network.

Acquisition (SCADA) systems are mostly used for gathering data of the control process remotely. This data is presented through a Human Machine Interface (HMI). This type of architecture usually applies to large geographic areas such as power grid, water plants that might be located thousands of kilometers away [3]. Another type of ICS is Distributed Control Systems (DCS). These systems are process oriented and monitors local processes. DCS can be similar to SCADA systems regarding architecture and technology, however, DCS monitors complex industrial processes in a small area, for instance, an industrial plant with different time constraints [4] [10].

This paper focuses on SCADA systems and presents a supervised energy monitoring-based machine learning approach for anomaly detection in a clean water supply system. In order to develop this concept, we implement a SCADA testbed using the Festo MPA Process Control Rig. The testbed emulates a clean water supply system and allows monitoring of the energy consumption of two of its components, the pump and the pneumatic valve using the INA219 current sensor [28]. A raspberry pi collects and writes the values from the current sensors in an ARFF file format, which, is the file format used by WEKA version 3.8.2 [32]. This paper presents the results of three machine learning algorithms that perform classification tasks on the dataset collected. The next section presents the related research in the field.

II. RELATED WORK

In this section, existing work related to intrusion detection schemes for SCADA systems are discussed in the two main categories of supervised and unsupervised machine learning techniques with a particular focus on water treatment systems. The electronic literature search was conducted on Google Scholar using query phrases such as: “scada”, “intrusion detection system”, “anomaly-based detection”, “water”, “supervised machine learning” and “unsupervised machine learning” with 2010 to 2018 publication year filter applied.

A. Supervised Machinel Learning Papers

In [16], the authors proposed Support Vector Machine (SVM)-based technique to detect cyber-attacks on Industrial Control Systems (ICS) based on communication profile. They employed SVM with different optimization of the hyper-parameters to classify malicious and benign traffic on their own testbed. Their testbed contains two water tanks equipped with control devices and controlled automatically. Their datasets constructed from the period of four-stage penetration tests during which malicious and benign packets are labelled based on their source IP addresses. They used Metasploit Framework (Rapid7) for penetration tests and Wireshark to capture packets. Addressing their captured results, they achieved around 95% classification accuracy and 0.048% error rate which is the average of ten rounds with cross validation. However, their selected features are limited to two: packet intervals and packet length. Also, the type of their penetration tests (i.e. black box testing, white box testing or grey box testing) are not clear. This means it is unclear either they ran the penetration tests having the full knowledge of the system, without knowing the ins and outs of the system or having a partial knowledge of the system.

In [17], the authors proposed a one-class Network Introduction Detection System (NIDS) for SCADA using Software Defined Network (SDN). They employed One-Class Classification (OCC) based on SVM: One-Class Support vector Machine (OCSVM) and Support Vector Data Description (SVDD) to detect abnormal traffic behaviour on Smart Grids. They simulated an SDN-based SCADA system using a large-scale topology, with one main control centre, four intermediate control centres, eight distribution substations, and hundreds of field devices. They then used OpenFlow protocol to periodically extract statistics from the SCADA network. Their NIDS detects abnormal traffic behaviour from a training set containing only the signature of traffic generated under normal network operation. In addition to OpenFlow’s native features they enabled the use of other extracted features including packet inter-arrival time, packets per second and mean packet length. They also used Principal Component Analysis (PCA) and Genetic Algorithm (GA) to determine the optimal set of features for traffic classification. Addressing their captured results, they achieved more than 99% accuracy rate for OCSVM and less than 98% accuracy rate for SVDD. However, their attack scenario is limited to one simulated DoS attack. Additionally, given that they only considered the signature of normal traffic, it is not clear how they distinguish between an attack and a system misconfiguration.

In [18], the authors proposed a behaviour-based attack detection and classification scheme for a Secured Water Treatment (SWaT) system using machine learning algorithms. They used a SWaT testbed which is an operational scaled down water treatment plant producing five gallons of doubly filtered water per minute including six-stage filtering processes replicating those found in cities. Each process dependent on the previous one and having one dedicated separate PLC. They used nine supervised machine learning (ML) algorithms: Neural Networks (NNs), SVM, Logistic Regression (LR), Random Forest (RF), J48, Best-First Tree (BFTree), Bayesian Network (BayesNet), Naive Bayes (NB) and Instance-based Learning [16](IBK) with various parameter values to find the best parameters for each classifier. They employed 18 attacks from 10 different types to

build the model for their nine machine learning algorithms. Addressing their results, BFTree showed the best results in terms of precision and accuracy. However, their selected features e.g. sensor reading and actuator commands have not been clearly identified nor discussed. Additionally, their model may not be able to detect zero day attacks or the attacks that have not been considered in their selected categories.

In [21], the authors employed behaviour observation and big data analysis techniques for cyber threat detection in a simulated pressurised water nuclear reactor. In their simulation, each component has a corresponding observer to extract physical behavioural information that helps towards constructing the dataset for their experiments. They used two datasets to run their experiments. The first dataset includes smaller events with a reduced number of features while the second dataset includes larger events with a greater number of features. They have gathered features such as: overall water volumes, steam output, energy creation, water tank levels and speed of water flow. They then used supervised learning algorithms such as Uncorrelated Normal Density based Classifier (UDC), Quadratic Discriminant Classifier (QDC), Linear Discriminant Classifier (LDC), Decision Tree (TREEC), and Parzen Classifier (PARZENC) to detect attacks. Addressing their presented results, in the initial evaluation, the classifiers were able to produce 68.34% accuracy which is increased to 96.65% in the second evaluation where they increased the number of the events and number of the features captured for each event. However, while there are advantages in using simulation environments, they come with a set of disadvantages. For example, they are flexible, but they are not standardized. Additionally, building a simulation does not require data, but validation does.

B. Un-Supervised Machinel Learning Papers

Using a similar SWaT testbed, the authors in [19] employed unsupervised machine learning algorithms for anomaly detection in water treatment systems. For their implementations, they used logs from SWaT that contain both benign and malicious events including network traffic, sensor data and actuator data collected over eleven days of continuous operations. The benign logs, which are the events generated by SWaT under normal condition, have been used to train the model. The malicious logs, which include 36 different attack scenarios, have been used to evaluate the performance of their proposed unsupervised anomaly detection model. In their paper, they compared two unsupervised machine learning algorithms: a Deep Neural Network (DNN) with feed forward layers of multiple inputs and outputs and a one-class SVM. Additionally, they tuned some hyper parameters in both algorithms before training. Addressing their results, DNN performs slightly better than one-class SVM in general. However, some of the performance metrics they captured are poor and need to be improved e.g. recall for both DNN and SVM models.

Using a similar SWaT testbed, the authors in [20] employed unsupervised Recurrent Neural Networks (RNN) for anomaly detection in water treatment systems. Their dataset contains readings from sensors and actuators on the SWaT testbed during eleven days including seven days of normal continuous operation and four days of attack scenarios. The malicious scenarios include thirty six attacks some of which are consecutively within a ten minutes gap of each other, while some others are performed by leaving time for the system to stabilise. Their dataset has been normalised by removing the mean and scaling to unit variance during the data pre-processing stage and before feeding the data to unsupervised RNN. They then used Cumulative Sum method to identify anomalies in the SWaT testbed. Addressing their results, they were able to detect the majority of their designed attacks with low false positive rates. However, their model is restricted to identifying attacks on a single process (Process 1) and not the entire system.

In [22], the authors proposed an unsupervised clustering approach for Intrusion Detection Systems (IDS) in ICS/SCADA applications. They used datasets from a simulated power distribution system containing 15 sets with 37 power system events. Each event is either: a natural event, a no event, or an attack event. The attacks scenarios include: remote tripping command injection, relay setting change, and data injection. They applied PCA for the feature reduction, standardizing to improve clustering results, unity based normalization, and quantization to reduce the large variance in the dataset. After using PCA approach and to improve the computational efficiency, they employed only five features out of 128 to classify data in the dataset. They compared their proposed IDS, where clustering is combined with the Fuzzy Inference System (FIS), with K-MEANS and Fuzzy C-means (FCM) algorithms. Addressing their results, their proposed IDS shows the benefits of adding FIS claiming that adding such intelligent techniques can provide a mechanism that can be used to get more info out of the clustering algorithm results. However, as mentioned before, using simulated experiments comes with a set of disadvantages.

In [1], the authors proposed an unsupervised anomaly-based detection approach for integrity attacks on a water distribution system. Their proposal is based on k-nearest neighbour technique and includes two stages of: automatic identification and automatic extraction. They used a real dataset and two simulated datasets. Each simulated dataset consists of twenty-three nodes and 10,500 observations while the real dataset includes 38 data nodes and 527 observations. Addressing the results, their proposed unsupervised approach show better detection accuracy and efficiency results compared to three anomaly detection approaches, two of which are based on unsupervised learning, while the third is based on semi-supervised learning. However, given that their proposed approach is based on k-nearest neighbour technique, their scheme is rather computationally expensive particularly when it computes an inconsistency score for each observation.

In this paper, despite the fact both [21] and [22] employed simulation environments, we developed a SCADA testbed using The Festo MPA Process Control Ring which is an operational scaled down clean water supply system. Additionally, unlike [18], our selected features are comprehensively explained and discussed. Furthermore, unlike

[16], we have measured more features in our testbeds to achieve a better classification accuracy. Based on our best knowledge we could not find any research papers proposing a supervised machine learning approach based on energy consumption metrics on a Festo MPA Process Control Rig. Our implemented testbed allows energy consumption monitoring for anomaly detection using two components on a Festo MPA Process Control Rig by employing the INA219 sensor.

III. DESIGN AND IMPLEMENTATION

For testing purposes an uninterrupted clean water supply is physically modelled using the Festo MPA Process Control rig [23], Fig 2. It has four control loop integrated which can operate individually. For the testbed we use components such as: pump, pneumatic valve, ultrasonic level sensor and flow meter. The aim is to maintain the required tank water level set point using one control loop in the tank B102. An uninterrupted clean water supply is an essential utility in which the main water is usually gravity fed to a surrounding area from a water tank located at a height to sustain a suitable delivery pressure.

In this exercise, we consider such a tank to be supplied from a downhole pump providing naturally filtered water from a water table located underground. The water is pumped via a variable speed drive so that the required tank water level can be maintained while the demand from the tank varies throughout the day. The water level of the tank is measured as Process Variable (PV) for closed-loop control of the delivery pump to maintain the required tank water level Set Point (SP). Minimising pump switching in this way reduces the pressure surges in the supply line and optimises tank storage capacity in event of high demand periods. A pneumatic valve, V102, simulates the demand from the tank. When the water is in demand, the downhole pump starts transferring water to the main tank until it reaches the set point.

A. *Testbed Components*

Fig 3 shows the diagram of the testbed built for this paper and Fig 4 shows the real implementation. It consists of the following components:

- Festo MPA Process Control Rig [23].
- Human Machine Interface (HMI).
- Switch.
- PLC Simatic S7-1500.
- Two INA219 current sensors.
- One Raspberry PI3.
- One desktop computer with TIA Portal V14.
- One laptop with Linux operating system.

B. *INA219 Sensor*

The INA219 sensor is a breakout board that measures voltage and current. It can measure up to 26v and ±3.2A. It is powered with 3v to 5V, and it has I2C pins.

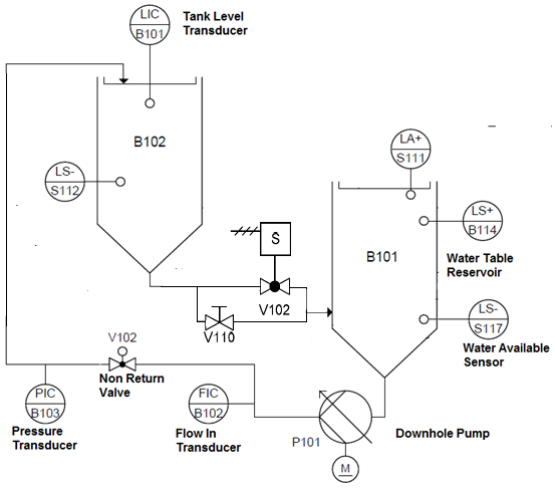

Fig. 2. Festo MPA Process Control Rig.

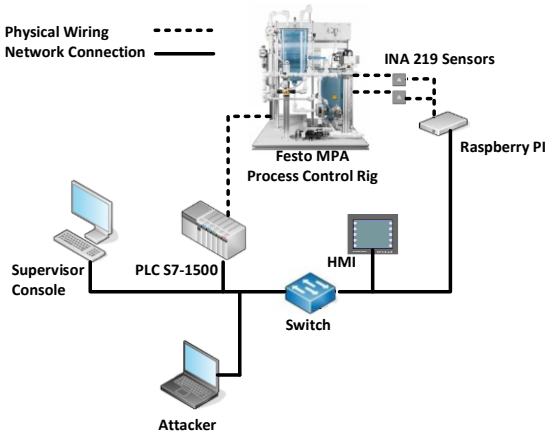

Fig. 3. Testebed implementation.

In this paper, we collected the power consumption of two devices: the pump and the pneumatic valve by means of the INA219 sensor. This sensor was used as a similar one was successfully applied in a previous industrial control research [14] [13]. Measuring the current of the pump and the pneumatic valve requires breaking its circuits and connecting the INA219 sensor as part of the electric circuit. The pump has an independent motor controller. Therefore, the INA219 sensor is wired to it in order to obtain the energy use of the pump. The pneumatic valve is connected to a digital output of the PLC. In order to monitor the operation from the pneumatic valve, the INA219 is wired to this output of the PLC. It is because unlike the pump the valve does not have an independent controller.

C. *Raspberry PI.*

The raspberry pi is a single-board computer that runs the Linux-based operating system [31]. It can run multiple tasks, unlike Arduino board. The raspberry pi3 collects the information obtained by the INA219 sensors through the

Fig. 4. Physical Testbed.

I2C bus. Each INA219 sensor is allocated its own I2C address to identify the sensor. The address jumpers of the INA219 sensor is set by a drop of soldering between them [28].

D. Normal and attack scenarios

This testbed simulates an uninterrupted clean water supply. In a normal operation, the tank B102 represents a reservoir of water to be maintained at a specified level. The tank B101 contains the water supply simulating the natural water table and feeds tank B102 through the variable speed pump P101. The valve V110 is slightly open representing a constant demand for water. During peak times, the pneumatic valve V102 represents a high demand for water. The pneumatic valve V102 opens for two minutes every three minutes. For the attack scenario, we assume that the attacker has access to the industrial network and is able to communicate with the PLC and execute attacks in the network such as man in the middle, with the aim to tamper with the information displayed in the HMI. Thus, the attacker will send commands to the PLC and modify its operation. Meanwhile, the operator will not be able to notice these modifications because the HMI shows the information modified by the attacker.

The aim of the attacker is to disrupt the water supply in a small town by reducing the amount of water in the reservoir tank. To achieve this goal the attacker modifies the PLC memory that holds the value of the tank water level set point. The attack is performed against the PLC over the network. In this scenario, the attacker modifies the space of memory of the PLC that contains the set point of the reservoir tank.

E. Dataset

The dataset contains the information collected by the sensors INA219 wired in the Festo MPA Process Control Rig. Each sensor provides four features:

- Voltage. The voltage at the pump and the valve.
- Current. The current flowing in the pump and the valve solenoid.
- Energy Consumption. The amount of energy or power used by the pump and the valve.
- Voltage in shunt resistor. It calculates the current by measuring the voltage dropped across the known shunt resistor.

We have considered three different datasets. Table 1 shows the characteristics of the datasets in each case. For the first case, only one sensor is wired to the testbed. The sensor monitors the energy consumption from the pump. It should be noted that the attacker only modifies the reservoir tank set point, which is related to the energy consumption in the pump. The remaining datasets provide information about both INA219 sensors.

F. Data preprocessing

Machine learning algorithms learn from data. Data preprocessing is an important step although it is less known than other steps such as data mining [26]. Usually, the raw data comes with imperfections like missing values, inconsistencies, and noise. The removal of these imperfections could be one of the most difficult issues for machine-learning. The performance of the machine learning algorithms depends on the quality of the pre-processed data [24]. The data pre-processing step can be summarized in the following steps:

1) Selecting the data: Sometimes all the collected data is not useful. Additionally, selecting the right features usually has an impact on the results expected by the machine learning algorithm [25]. The current sensor INA219 provides four features. We removed the voltage feauture from the pump because the value is constant either under attack or normal operation. At the end, we add class feature in each dataset which identifies each instance either as malicious or benign. It is considered malicious if the timeframe that the reservoir tank setpoint is modified.

TABLE I. DATASETS SUMMARY.

Case	Dataset Characteristics				
	Instances	**Attributes**	**INA219 sensors**	**Training Data**	**Testing Data**
Case I	3547	4	1	2341	1206
Case II	6907	8	2	4558	2349
Case III	13252	8	2	8746	4506

2) Preprocessing the data: The raspberry pi collects and writes the values from the current sensors in an ARFF file format, which, is the file format used by WEKA. Another point to consider at this stage is that our data does not have any missing values that might affect the performance of the algorithm.

3) Transforming the data: Processing raw data through machine learning algorithms usually is not a good practice. Each machine learning algorithm has its own requirements regarding preprocessing data. For instance, the KNN algorithm shows a better performance when the input data is normalized [26]. We applied normalization and standardization techniques to the three datasets obtained in our testbed. In addition, the datasets captured from the testbed show unbalanced classes, as a consequence, it might bring inaccurate results when the model is trained.

G. Supervised Approach

In this paper, we applied three supervised machine learning algorithms performing classification tasks for the dataset obtained from the Festo MPA Process Control Rig. The algorithms are KNN, SVM and Random Forest.

- KNN. The KNN (K-Nearest Neighbour) algorithm stores entire dataset in memory, consequently, there is no learning involved. The training data has to be consistent and pre-processed properly. KNN classifies a case by a majority vote of its neighbours. One case is assigned to the class most common among its K-nearest neighbours measured by a distance function. In addition, KNN performs better when the dataset is normalized [26]. The majority of the features obtained in the control process implemented in this research are continuous; consequently applying the normalization techniques might speed up the classification process.
- SVM. The SVM algorithm (Support Vector Machine) has shown efficiency classifying text features. SVM seeks for a hyperplane in a multidimensional space and separates different cases with a given margin. SVM uses different kernels for classifying the data [24]. In this case, we run SVM in the datasets with different parameters with the aim of finding the highest accuracy.
- Random Forest. This is considered one of the most versatile algorithms as it is capable of performing either regression or classification. Random Forest grows multiple trees and classifies new cases depending on attributes. One of the benefits of this algorithm is the capability of handling large amounts of data [27]. We expect to gather variations in energy consumption of the endpoints in the control system implemented. To do so, we monitor the energy consumption of the endpoints on-line.

We chose the algorithms above because they have been applied in similar researches as it can be seen in section II. Each algorithm has different parameters that can be tuned in order to improve its performance [30]. We tuned each algorithm with the optimal parameters based on the highest accuracy and F-measure. We avoid overfitting by using a resample technique (K-fold cross validation) in order to estimate the model accuracy. The next section provides the classified results under optimal parameters with the intention of comparing them fairly. The next section presents the results of the three algorithms run on our three.

IV. RESULTS

We use WEKA machine learning and data mining software because it is widely used and it provides an extensive number of algorithms for testing purposes. The algorithms chosen for this test were KNN, SVM and Random. Fig 5 shows the energy consumption from the pump and the valve under normal and attack conditions. The parallel red lines in Fig 5 show the execution of an attack. When the control system is operating under normal conditions the pattern of energy is stable, however, when the set point from the reservoir tank is modified by the attacker the energy consumption in the pump changes as it can be seen in Fig 5. The attacker does not manipulate the pneumatic valve in this scenario. It should be considered that this attack will affect the distribution of water in a real scenario because the operator does not notice the change in the reservoir tank set point in the monitoring system.

Fig 6 to 8 show the results of the three algorithms performing classification tasks on our three pre-processed datasets. The test for the algorithm KNN was performed using the following distances: Euclidean, Manhattan, Minkowski and K distances from zero to ten. The chosen distance parameter did not affect the results of precision, accuracy and recall; instead, it increased and decreased the time to build the model. When the k-neighbour parameter changes the results also change although it does not vary much. The SVM algorithm shows different results depending on the kernel selected. We tested SVM algorithm with the following kernels: Polynomial, normalized polynomial, Pearson VII and radial basis function. Fig 6 shows the result of Pearson VII kernel function (PUK) and Fig 7 shows that Random Forest algorithm presents a better result compared with the other two algorithms. For this algorithm, the parameter depth was modified ten times however the default depth presents the best result.

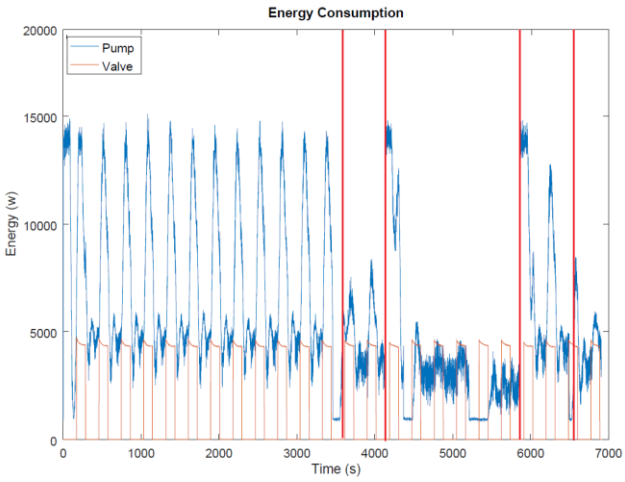

Fig. 5. Energy consumption in the valve and the pump

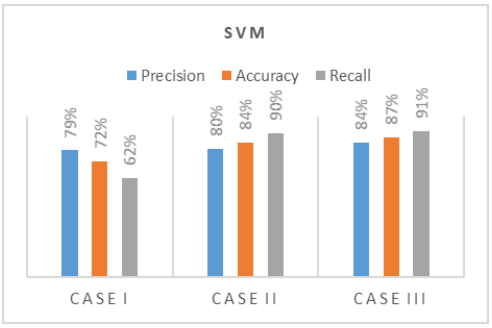

Fig. 6. SVM Performance.

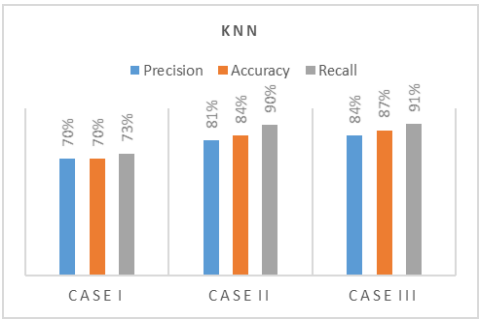

Fig. 7. KNN Performance.

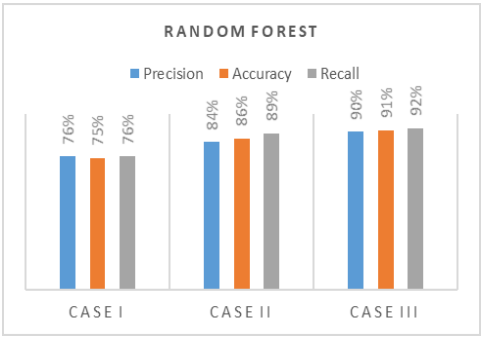

Fig. 8. Random Forest performance.

Table II presents a summary of the time taken to build the model for each case (case I to case III). It can be seen that SVM takes much longer time than the rest of the algorithms. This is because the number of kernel evaluations that perform this algorithm increases with the amount of data in the dataset. For instance, the difference between the first and the third case regarding the number of kernel evaluations is about one thousand million, which results in 131.93 seconds of difference between them. KNN is one of the most simplistic algorithms and the fastest compared with SVM and Random forest. It only computes the distance with the K-nearest neighbor and does not show considerable variation among the datasets.

Accuracy provides an intuitive performance measure and it is the number of correct predictions over the total observations, however, accuracy alone is not the only metric to consider during the performance evaluation [24].

TABLE II. SUMMARY OF TIME.

Algorithm	Time taken to build the model		
	Case I	Case II	Case III
SVM	5.57s	31.15s	137.43s
KNN	0s	0s	0.1s
Random Forest	0.73s	0.1s	3.63s

TABLE III. DATASETS F-MEASURE.

Algorithm	F-Measure		
	Case I	Case II	Case III
SVM	69%	85%	87%
KNN	71%	85%	87%
Random Forest	76%	86%	91%

The F-measure is the weighted average of precision and recall. F-measure is more useful than accuracy, although, it happens in unbalanced class distributions only [29]. The results show that Random Forest achieves 75% of accuracy with the smallest dataset and 91% when the data and attributes increased. In general, the three algorithms increase the accuracy along with the data, which can be compared with how the humans learn. This means better knowledge with more data. We use statistically significance, in order to choose the best algorithm for each dataset. The null hypothesis for this paper states that the three algorithms perform the same. The level of statistical significance is 0.03. It can be said that the statistical significance depends on the criticality of the data. Thereby, we choose 0.03 because the testbed represents a clean water supply system. Bearing that in mind, in case I, Random Forest outperforms with 5% to KNN and 3% to SVM. In case II, the three algorithms perform the same but in Case III, Random Forest presents the best performance again with 4% over KNN and SVM.

Table III shows the results of the F-measure for each of the cases. It can be seen that the results are similar to the accuracy presented in Fig 6 to Fig 8. This is the result of having balanced datasets.

V. CONCLUSIONS AND FUTURE WORK

This paper describes a new approach based on the power monitoring of the endpoints from a control system in order to detect anomalies. The information is obtained by wiring two sensors INA219 in the control system. Afterwards, the reading from the sensors is collected with a raspberry pi3. The information obtained from the sensors is tagged as benign or malicious then classified using three different machine learning algorithms. Each algorithm was tuned with different parameters. The Random Forest algorithm provides the best results during the classification phase. The data is obtained from a real testbed designed and implemented at Edinburgh Napier University. The attacks were conducted to the control system implemented in Festo MPA Process Control rig. This system emulates a clean water supply. It can be seen that an attack on the reservoir tank set point results in a water outage for the user. In addition, it can be seen that applying supervised machine learning to the energy consumption of the pump and

pneumatic valve of a downscaled clean water supply system permits to detect anomalous behaviour.

For future work, we plan to extend our work by improving our testbed in order to simulate the demand of customers in a more realistic manner. We have also planned to conduct different type of attacks and use machine learning for two attack classifications.

ACKNOWLEDGMENT

This research is supported by the School of Computing and the School of Engineering and the Built Environment of Edinburgh Napier University.

REFERENCES

[1] A. Almalawi, X. Yu, Z. Tari, A. Fahad and I. Khalil, "An unsupervised anomaly-based detection approach for integrity attacks on SCADA systems," Computers & Security, pp. 94 - 110, 2014.

[2] Q. Chen and S. Abdelwahed, "A Model-based Approach to Self-Protection in SCADA Systems," in 9th International Workshop on Feedback Computing (Feedback Computing 14), Philadelphia, 2014.

[3] D. Hadziosmanovic, R. Sommer, E. Zambon and P. H. Hartel, "Through the Eye of the PLC: Semantic Security Monitoring for Industrial Processes," in Proceedings of the 30th Annual Computer Security Applications Conference, New Orleans, Louisiana, USA, 2014.

[4] W. Li, . L. Xie, Z. Deng and Z. Wang, "False sequential logic attack on SCADA system and its physical impact analysis," Computers & Security, pp. 149 - 159, 2016.

[5] S. S and P. Winston, "An enhanced optimization based algorithm for intrusion detection in SCADA network," Computers & Security, pp. 16 - 26, 2017.

[6] Y. Wang, Z. Xu, J. Zhang, L. Xu, H. Wang and G. Gu, "SRID: State Relation Based Intrusion Detection for False Data Injection Attacks in SCADA," in Computer Security - ESORICS 2014: 19th European Symposium on Research in Computer Security, Poland, 2014.

[7] Y. Yang, H.-Q. Xu, L. Gao, Y.-B. Yuan, K. McLaughlin and S. Sezer, "Multidimensional Intrusion Detection System for IEC 61850-Based SCADA Networks," IEEE Transactions on Power Delivery, pp. 1068-1078, 2017.

[8] A. Cardenas, S. Amin, Z.-S. Lin, Y. Huang, C.-Y. Huang and S. Sastry, "Attacks against process control systems: Risk assessment, detection,," Proceedings of the 6th International Symposium on Information, , pp. 355-366, 2011.

[9] IBM, "Security attacks on industrial control systems," 12 06 2017. [Online]. Available: https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03046USEN.

[10] Ö. Yüksel, J. den Hartog and S. Etalle, "Reading between the fields: practical, effective intrusion detection for industrial control systems," pp. 2063-2070, 2016.

[11] A. Ali Abbasi and H. Majid , "Ghost in the PLC: Designing an Undetectable Programmable Logic," Black Hat Europe, 2016.

[12] KASPERSKY, INDUSTRIAL CONTROL SYSTEMS VULNERABILITIES STATISTICS, 2016.

[13] J. Hoffmann, S. Neumann, T. Holz, S. Stolfo, A. Stavrou and C. Wright, "Mobile Malware Detection Based on Energy Fingerprints --- A Dead End?," in Research in Attacks, Intrusions, and Defenses: 16th International Symposium, RAID 2013, Rodney Bay, St. Lucia, Berlin, Heidelberg, 2013.

[14] J. M. Hernandez, Q. Chen, C. Calhoun, S. Sykes and J. A. Nichols, "Towards a Cyber Defense Framework for SCADA Systems Based on Power Consumption Monitoring," in Proceedings of the 50th Hawaii International Conference on System Sciences, 2017.

[15] C. A. Gonzalez and A. Hinton, "Detecting Malicious Software Execution in Programmable Logic Controllers Using Power Fingerprinting," in 8th International Conference on Critical Infrastructure Protection (ICCIP), Arlington, United States, 2014.

[16] A. Terai, S. Abe, S. Kojima, Y. Takano and I. Koshijima, "Cyber-Attack Detection for Industrial Control System Monitoring with Support Vector Machine based on Communication Profile," 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), pp. 132-138, 2017.

[17] E. Germano da Silva, A. Santos da Silva, J. A. Wickboldt, P. Smith, L. Z. Granville and A. Schaeffer-Filho, "A One-Class NIDS for SDN-Based SCADA Systems," 2016 IEEE 40th Annual Computer Software and Applications Conference, pp. 303 - 312, 2016.

[18] K. Nazir Junejo and J. Goh, "Behaviour-Based Attack Detection and Classification in Cyber Physical Systems Using Machine Learning," Proceedings of the 2nd ACM International Workshop on Cyber-Physical System Security, pp. 34-43 , 2016.

[19] J. Inoue, Y. Yamagata, Y. Chen, C. M. Poskitt and J. Sun, "Anomaly Detection for a Water Treatment System Using Unsupervised Machine Learning," IEEE International Conference on Data Mining Workshops, pp. 1058-1065, 2017.

[20] J. Goh, S. Adepu, M. Tan and Z. Shan Lee, "Anomaly Detection in Cyber Physical Systems Using Recurrent Neural Networks," Data Mining Workshops (ICDMW) 2017 IEEE International Conference on, pp. 1058-1065, 2017.

[21] W. Hurst, M. Merabti and P. Fergus , "Big Data Analysis Techniques for Cyber-Threat Detection in Critical Infrastructures," 28th International Conference on Advanced Information Networking and Applications Workshops, pp. 916-921, 2014.

[22] L. Tomlin and M. R. Farnam, "A Clustering Approach to Industrial Network Intrusion Detection," Proceedings of the 2016 Information Security Research and Education (INSuRE) Conference (INSuRECon-16), 2016.

[23] FESTO, "MPS® PA Compact Workstation with level, flow rate, pressure and temperature controlled systems," [Online]. Available: http://www.festo-didactic.com/int-en/learning-systems/process-automation/compact-workstation/mps-pa-compact-workstation-with-level,flow-rate,pressure-and-temperature-controlled-systems.htm?fbid=aW50LmVuLjU1Ny4xNy4xOC44ODIuNDM3Ng.

[24] R. Astuti Nugrahaeni and K. Mutijarsa, "Comparative Analysis of Machine Learning KNN, SVM, and Random Forests Algorithm for Facial Expression Classification," International Seminar on Application for Technology of Information and Communication, pp. 163-168, 2016.

[25] Z. Zhou, C. Wen and C. Yang, "Fault Isolation Based on k -Nearest Neighbor Rule for Industrial Processes," IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, vol. 63, no. 4, pp. 2578-2586, 2016.

[26] A. A. Aburomman and M. B. Ibne Reaz, "A novel SVM-kNN-PSO ensemble method for intrusiondetection system," Applied Soft Computing, vol. 38, p. 360–372, 2016.

[27] J. Zhang, M. Zulkernine and A. Haque, "Random-Forests-Based Network Intrusion Detection Systems," IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS—PART C: APPLICATIONS AND REVIEWS, vol. 38, no. 5, pp. 649 - 659, 2008.

[28] Adafruit, "Adafruit INA219 Current Sensor Breakout," [Online]. Available: https://cdn-learn.adafruit.com/downloads/pdf/adafruit-ina219-current-sensor-breakout.pdf.

[29] K. Yau, K. Chow, S. Yiu and C. Chan , "Detecting Anomalous Behavior of PLC using Semisupervised Machine Learning," IEEE Conference on Communications and Network Security (CNS): The Network Forensics Workshop, pp. 580-585, 2016.

[30] Y. Cui, M. Cai and E. Stanley, "Comparative Analysis and Classification of Cassette Exons and Constitutive Exons," BioMed Research International, pp. 96 - 103, 20.

[31] RASPBERRY PI FOUNDATION, "Raspberry Pi - Teach, Learn, and Make with Raspberry Pi," [Online]. Available: https://www.raspberrypi.org.

[32] University of Waikato, "Machine Learning Group at the University of Waikato," [Online]. Available: https://www.cs.waikato.ac.nz/ml/weka/.