Article

A Novel Machine Learning-Based Framework for Optimal and Secure Operation of Static VAR Compensators in EAFs

Li Zeng ¹, Tian Xia ², Salah K. Elsayed ³ , Mahrous Ahmed ³ , Mostafa Rezaei ⁴ , Kittisak Jermsittiparsert ⁵ , Udaya Dampage ^{6,*} and Mohamed A. Mohamed ^{7,8,*}

¹ School of Electrical and Electronic Engineering, Hubei University of Technology, Wuhan 430068, China; zengli919679484@foxmail.com

² Hubei Collaborative Innovation Center for High-Efficiency Utilization of Solar Energy, Hubei University of Technology, Wuhan 430068, China; xiatianuhan@gmail.com

³ Department of Electrical Engineering, College of Engineering, Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia; salah_kamal1982@yahoo.com (S.K.E.); m.elsamman@tu.edu.sa (M.A.)

⁴ Queensland Micro- and Nanotechnology Centre, Griffith University, Brisbane 4111, Australia; mostafa.rezaei@griffithuni.edu.au

⁵ College of Innovative Business and Accountancy, Dhurakij Pundit University, Bangkok 10210, Thailand; kittisak.jer@dpu.ac.th

⁶ Faculty of Engineering, Kotelawala Defence University, Ratmalana 10390, Sri Lanka

⁷ Electrical Engineering Department, Faculty of Engineering, Minia University, Minia 61519, Egypt

⁸ Department of Electrical Engineering, Fuzhou University, Fuzhou 350116, China

* Correspondence: dampage@kdu.ac.lk (U.D.); dr.mohamed.abdelaziz@mu.edu.eg (M.A.M.)

Citation: Zeng, L.; Xia, T.; Elsayed, S.K.; Ahmed, M.; Rezaei, M.; Jermsittiparsert, K.; Dampage, U.; Mohamed, M.A. A Novel Machine Learning-Based Framework for Optimal and Secure Operation of Static VAR Compensators in EAFs. *Sustainability* **2021**, *13*, 5777. <https://doi.org/10.3390/su13115777>

Academic Editor: Nicu Bizon

Received: 6 April 2021

Accepted: 11 May 2021

Published: 21 May 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

Abstract: A static VAR compensator (SVC) is a critical component for reactive power compensation in electric arc furnaces (EAFs) that is used to relieve the flicker impacts and maintain the voltage level. A weak voltage profile can not only reduce the power-quality services, but can also result in system instability in severe cases. The cybersecurity of EAFs is becoming a significant concern due to their cyber-physical structure. The reliance of SVC controllers on reactive power measurement and network communications has resulted in a cyber-vulnerability point for unauthorized access to the EAF, which can affect its normal operation. This paper addresses concerns about cyber attacks on EAFs, which can cause network communication issues in measurement data for SVCs. Three significant and different types of cyber attacks that are launched on SVC controllers—a replay attack, delay attack, and false data injection attack (FDIA)—were simulated and investigated. In order to stop the activities of cyber attacks, a secured anomaly detection model (ADM) based on a prediction interval is proposed. The proposed model is dependent on a support vector regression and a new smooth cost function for constructing the optimal and symmetrical intervals. A modified algorithm based on teaching–learning-based optimization was developed to adapt the ADM's parameters during training. The simulation's outcomes on a genuine dataset showed the strong capability of the proposed model against cyber attacks in EAFs.

Keywords: static VAR compensator; reactive power; teaching–learning algorithm; electric arc furnace; secured model

1. Introduction

1.1. Necessity and Significance

An electric arc furnace (EAF) is a metallurgical furnace for melting and converting scrap steel into new steel by using a high current level. The electrodes installed on an EAF's top-head provide its energy, which is estimated as the energy required to power a city with a population of 100,000 [1]. A schematic diagram of an EAF is presented in Figure 1. The high reactive power demand in an EAF affects the neighboring loads' power quality by reducing the voltage level and injecting harmonics in the range of 0.5–0.25 Hz [2]. Such a high reactive power demand can cause severe challenges if it is not properly compensated [3].

The voltage flicker originating from the EAF can result in large voltage fluctuations in the coupling power grid, which, in turn, affect the normal operation of other interconnected loads. Several methods based on radial basis function neural networks [4] and dynamic modeling [5] have been proposed by researchers to model the flicker severity in EAFs and help the reactive power compensators to control the voltage fluctuations. To deal with this issue, some static VAR compensators (SVCs) are installed in EAFs to track the fast reactive power changes and continuously inject power.

Figure 1. Schematic diagram of an EAF.

1.2. Literature Review

A typical SVC includes a thyristor-controlled reactor (TCR), thyristor switched capacitor (TSC), and SVC controller [6]. Attributable to the highly variable disposition of the reactive power in the EAF, the reactive power compensation speed severely affects the power quality and voltage level. Therefore, several methods have been suggested by researchers to provide better reactive power modeling and compensation by SVCs. In [7], a time series-based approach was developed for the reactive measurement of power lines. In [8], a wavelet transform was used for reactive power and energy modeling considering power-quality disturbances. In [9], neural network models were used to measure the reactive power demand. An online genetic-based method and auto-regressive moving average were used in [10] to update the model coefficients in real-time. In [11], a hybrid gray model and Markov chain were used for reactive power modeling in an SVC. In [12], a support vector-based approach was devised to model the reactive power compensated by the SVC.

As can be deduced from these research works, reactive power tracking and compensation in EAFs are important issues for preserving the voltage level and power quality. In other words, appropriate SVC controller performance is vital for a proper reactive power compensation process. Due to the very large reactive power demand of an EAF, weak reactive power compensation can affect the system's voltage stability at the point of common coupling and, thus, the neighboring buses. A weak voltage profile can result in system instability and even a voltage collapse in severe cases [13]. Therefore, any action affecting the SVC's performance can be a source of voltage instability and power-quality issues in an EAF. In this regard, an SVC controller receives measured reactive power data through a wired or wireless sensor network. This is a vulnerable point in the EAF, making it a very attractive target for cyber attackers to penetrate the control system and compromise the reactive power measurements. In [14], a cyber attack is simulated on an SVC and it is shown that it can cause system angle and voltage instability, followed by physical failures. Discussions on some cyber attacks on FACTS devices in power systems can be found in [15]. This research shows that an SVC can be a potential cyber attack target for an adversary to penetrate the EAF system.

1.3. Contributions and Novelties

While the above research works have provided valuable results by showing the cyber vulnerability of the SVC, thus causing voltage instability, none of them has suggested any solution for stopping cyber attacks. Meanwhile, none of the above studies has addressed the cyber security issues in an EAF. This is a very significant issue and its negative effects have already been seen in the industry. In December 2014, a cyber attack was reported on an EAF in Germany [16]. The adversary penetrated a steel facility by sending a spear email and then gaining access to the corporate network. According to the report, the malicious actor could then access the plant network and make multiple components fail. Although the report does not provide further detailed information on the type of damage due to the security considerations, this clearly shows that an EAF can be a potential target for hackers in the near future. In this regard, an SVC, due to its cyber-physical structure, can be a vulnerable point for EAF hacking. Therefore, this paper assesses the cyber security of EAFs in the face of cyber attacks. To the best of the authors' knowledge, this is the first work to address EAF cyber security and provide a solution for stopping malicious attacks. To this end, three different types of cyber attacks, replay attack, time-delay attack and false data injection attack (FDIA), are assessed. These cyber attacks are launched on the measured data of SVCs installed in the EAF to cause problems in the data transmission process. It is stated in [17] that cyber attacks with such natures can be dangerous to SVCs. A successful cyber attack can add false data in the transmitted measured data either by fake/delay/replay and thus cause instability in the voltage profile correction. While being aware of the dangerous nature of the cyber attacks, an intelligent anomaly detection model (ADM) based on prediction intervals is proposed to secure the EAF. The proposed model is established to be dependent on the lower and upper estimation (LUBE) method and a new smooth fuzzy cost function to create the optimal prediction intervals. To make sure that there is no overfitting problem in the model, support vector regression (SVR) is used as the classification model. It is proved in support vector machine theory that any nonlinear relevance can be modeled by a linear model in a higher dimension [18]. Rather than the artificial neural network (ANN) models which focus on empirical risk minimization, the SVR model considers structure hazard minimization to keep the generalization error. Due to the dependence of the SVR model on its setting parameters, an optimization algorithm based on a teaching–learning algorithm (TLA) is employed here. TLA is a meta-heuristic optimization algorithm mimicking the knowledge transferred between a teacher and students and among the students themselves [19]. Furthermore, a novel two-stage modification strategy is proposed to help TLA to enhance its searching capability and avoid precocious convergence. Thusly, the unique contributions of this study can be summed up as follows:

- Assessing the security of EAFs notwithstanding different cyber attacks, including time-delay attack, replay attack and, FDIA on SVCs;
- Proposing an intelligent ADM based on SVR and prediction intervals for stopping cyber attacks in EAFs;
- Employing a new modification method based on TLA (MTLA) for adjusting the SVR model optimally.

The results of the cyber attacks on EAFs and the proposed ADM are assessed on a real EAF. The rest of this paper is organized as follows: Section 2 presents the EAF as a cyber-physical system and the cyber vulnerability. Section 3 describes the structure of the different cyber attack models. The proposed intelligent ADM is explained in Section 4. Sections 5 and 6 analyze the results and discuss the ideas for an EAF for cyber attacks and model performance, respectively. The main conclusions are presented in Section 7.

2. EAF as a Cyber-Physical System

An EAF, which is denoted as an alternative for bulk steel making, integrates control and communication techniques in its operating system to enable efficacy, accuracy and, cleanliness. Besides the physical layer, such as the furnace, electrodes, bus bars, nozzles,

burner systems, etc., an EAF has an integrated cyber layer dealing with the data measurements (active/reactive power), data communication and control systems. As a complex cyber-physical system, the control and operation of EAFs rely on measuring devices, computing systems, communication networks, etc. This makes an EAF an attractive object for cyber hackers to break through into its system and implement their malicious activities. In this regard, various factors, such as vulnerable metering devices, interaction with the main grid, sensitivity to time synchronization and communication delay, can cause the EAF insecurity in terms of the risk of a cyber attack. In an EAF, the SVC control system is the key component for hacking and affecting its whole operation. Technically, the SVC is an automated impedance device for reactive power management and is designed to bring the grid closer to the unity power factor. This would provide high power quality and avoid voltage flickers on the customer side. SVCs are used in two main cases:

- Connected to the power system, to regulate the transmission voltage, this is called “transmission SVC”;
- Connected close to large industrial loads, to enhance the power quality, this is called “industrial SVC”.

It is clear that this paper deals with the second case, i.e., industrial SVC. In a report published by the German Federal Office for Information Security in December 2014 [16], a malicious attacker was shown to penetrate an EAF system and cause severe physical damage to the system components. The hacker had first issued an electronic message to gain entry to the EAF grid and go through the plant network. The report mentions that the hacker had shown knowledge in the field of the EAF control systems and thus could specifically affect several critical components. The email contained malicious code which, after opening, would have targeted a vulnerable point in the system. When the application was exploited, the code made a remote linking point, letting the hacker access the network and the control system. A similar cyber attack on control systems was reported with the Stuxnet worm in 2010 [20]. Therefore, the control system of EAFs can be a significant vulnerable point which, if accessed by hackers, can affect the performance of the whole EAF. Such a control system can be interpreted as a cyber layer that is prone to any cyber attack if not protected properly. In contrast to the conventional protection methods which only focus on the physical layers and abnormal signs, such as overvoltage, overcurrent, frequency collapse, etc., cyber protection requires advanced methods for protecting the cyber layer from malicious activities. This makes us consider an EAF as a cyber-physical system with an urgent need for cyber security reinforcement methods to avoid unexpected results. Figure 2 shows the schematic diagram of an EAF as a cyber-physical system. As can be seen from this figure, in the heart of the cyber layer, the control system is located, which relies on the measurements made by sensors/metering devices. On the right side of this figure, an SVC is shown, which is in charge of voltage profile correction and power-quality enhancement by compensating for the reactive power variations. From a technical point of view, if the SVC cannot do its job by appropriate tracking of the reactive power, the high EAF reactive power demand can severely affect the voltage profile (when injecting highly variable flickers into the system), which may trigger protection relays. The result can be physical damage, operation shutdown or economic losses in both the EAF and the neighboring buses. To better understand this concept, it should be noted that an SVC consists of three main parts: (1) TCR, (2) TSC and (3) control system. The SVC controller receives the reactive power data samples through either a wired or wireless sensor network. Depending on the control strategy, these data samples may come from a local or a remote location to the SVC controller. By penetrating the SVC control system performance, a hacker can launch compromised signals, disrupting the SVC reactive power compensation. In the next section, the structure of cyber attacks and their effects on the SVC are explained. The cyber hacking point would be the operation of the SVC which goes through the control system for voltage regulation. By affecting the voltage regulation, the reactive power compensation would be affected.

Figure 2. An EAF as a cyber-physical system.

3. Cyber Attack Model

As explained in the last section, the SVC controller uses the receiving measured data for making fast reactive power compensations. A cyber attacker can launch cyber attacks of different types to affect the normal behavior of the SVC and thus the entire EAF [21]. In our case study, the EAF is equipped with four SVCs, three TSCs and one TRC which are used for reactive power compensation to avoid voltage flickers. The control of this equipment is implemented in the software layer which is based on an internal internet network, isolated from the main internet network. Nevertheless, the operators in the EAF center can launch comments for control of the EAF performance through the internal network. Meanwhile, their computers can receive emails from outside which makes it possible for a hacker to penetrate at this point. Any malicious file can be opened by an electrical engineer operator and this would be the starting point for installing hacking software or launching comments in the background of the monitor. In this section, three different kinds of cyber attacks, comprising the time-delay attack, replay attack and FDIA, are explained.

3.1. Time-Delay Attack

As can be inferred from its name, the time-delay attack causes a network delay when transmitting reactive power data samples from metering devices to the SVC controller and on the other side after the controller towards the actuator. To better understand this type of attack, let us define $q(t)$ as the reactive power data message measured and transmitted by the metering device to the controller or from the controller to the actuator at time t . The transmitted data are maliciously delayed by τ time periods. Therefore, the reactive power data message $q(t)$ arrives at the destination, either the controller or the actuator, at time $(t + \tau)$. Therefore, the time-delay attack does not change the nature/value of the sample data but causes a delay in the transmission process. Having a discrete time window, the parameter τ is an integer value that can be either fixed or a random value. In this paper, both fixed time delay and exponentially distributed delay (random delay), as two commonly utilized delay models, are exploited [22]. A fixed delay attack is constructed by adding a fixed delay to the transmission data. The exponential distribution delay is constructed as follows:

$$f(\tau, \Delta) = \begin{cases} \frac{1}{\Delta} e^{-\frac{\tau}{\Delta}} & , x \geq 0 \\ 0 & , x < 0 \end{cases} \quad (1)$$

where Δ is the scale parameter which is the average value of the exponential distribution. By increasing the Δ value, longer random delays are generated. Figure 3 shows the conceptual illustration of a time-delay attack.

Figure 3. Time-delay attack to the control system.

3.2. Replay Attack

A replay attack is a kind of cyber attack which maliciously resends the recorded sample data to the controller. Therefore, in the first step, the attacker needs to monitor the transmitted data. In the second step, the hacker replaces the real data with the recorded data periodically. The dangerous feature of this cyber attack is that the attacker does not need any special skill or advanced knowledge for decryption of the message after recording. The replay attack occurs by resending the monitored signal to affect the control system. In addition, since the replay attack makes use of real data samples, it is possible that the corrupted signal is not recognized and passes the detection algorithm. Figure 4 shows how a replay attack is launched.

Figure 4. Replay attack on the control system.

3.3. False Data Injection Attack (FDIA)

An FDIA is launched by compromising the real data measurements from metering devices/sensors. In contrast to the last two types of cyber attacks, i.e., replay attack and time-delay attack, the FDIA affects the integrity of data recorded by injecting false sample values into the true sample data. In an EAF, the FDIA can replace the same normal reactive power data received by the SVC controller, thus jeopardizing the normal operation of the EAF by disrupting the compensation process.

4. Anomaly Detection Model-Based Prediction Intervals

This part presents the proposed ADM constructed depending on the LUBE and MTLA.

4.1. Prediction Interval-Based ADM

To detect cyber attacks in an EAF, this method exploits the concept of prediction intervals for constructing lower bounds and upper bounds around the reactive power sample data. This makes it possible to distinguish between the normal and abnormal reactive power samples. By

definition, a prediction interval comprises an upper bound and a lower bound encompassing the reactive power data samples. To construct the prediction interval, we utilize LUBE [23]. Unlike the other probabilistic interval methods, LUBE is a non-parametric approach that does not use any assumptions about the density of the sample forecast. Nevertheless, we need to make two changes in the LUBE to make it compatible with the case of reactive power sample modeling as an ADM: (1) developing a new smooth cost function for constructing optimal symmetric intervals, and (2) making use of the SVR model instead of an ANN (the original LUBE works based on an ANN) [24,25]. Each of these parts will be explained later. Figure 5 shows the concept of the proposed ADM.

Figure 5. Concept of LUBE-based support vectors as ADM.

To measure the quality of a prediction interval, three indices are used: (1) confidence level, (2) interval width and (3) interval balance. The prediction interval confidence level (*PICL*) evaluates the number of samples captured among the lower and upper bounds, which is calculated as follows:

$$PICL = \frac{1}{N} \sum_{t=1}^N \theta_t \quad (2)$$

where θ_t is a Boolean variable, calculated as:

$$\theta_t = \begin{cases} 1 & ; y_t \in [L_t, U_t] \\ 0 & ; y_t \notin [L_t, U_t] \end{cases} \quad (3)$$

In the anomaly detection case, it is observed that a minimum confidence level $(1 - \alpha)\%$ is needed for constructing informative prediction intervals. This means any other prediction interval with a probability lower than $(1 - \alpha)\%$ is ignored. As the second criterion, the prediction interval width (*PIW*) is calculated as follows:

$$PIW = \frac{1}{NR} \sum_{t=1}^N (U_t - L_t) \quad (4)$$

It is clear that a large *PIW* may result in a high confidence level but the prediction intervals do not contain much information. Therefore, a low *PIW* is preferred when fulfilling the required *PICL*. Finally, the prediction interval balance represents the balance in the diversity of the prediction bounds around the sample data, which is calculated as follows:

$$PIB = \frac{1}{N} \sum_{t=1}^N (\max\{|y_t - L_t|, |U_t - y_t|\}) \quad (5)$$

It is clear that a higher *PIB* reveals that better symmetric prediction intervals are attained. The above three indices determine the quality of the prediction interval in such a

way that it is preferred to have higher *PICL* with low *PIB* and *PIW*. This demonstrates a multi-objective problem, as follows :

Objectives :

$$\begin{aligned} \text{Max: } & \text{PICL}(W, b) \\ \text{Min : } & \text{PIW}(W, b) \\ \text{Min : } & \text{PIB}(W, b) \end{aligned} \quad (6)$$

Constraints :

$$\begin{aligned} (1 - \alpha) & \leq \text{PICL}(W, b) \leq 100\% \\ \text{PINAW}(W, b) & \succ 0 \end{aligned}$$

Owing to the conflicting progress tendency of these indices, a smooth fuzzy-based cost function is employed to optimize all three indices in the same framework, as follows:

$$F(X) = \min_{x \in \Omega} \left\{ \max_{k=1, \dots, n} |\mu_{ref,k} - \mu_{fk}(X)| \right\}, k = 1, \dots, 3 \quad (7)$$

In (7), μ_{fk} is a trapezoidal fuzzy membership function assigned to each criterion. Additionally, $\mu_{ref,k}$ is the fuzzy reference value that can take values in the range [0, 1] such that a higher value shows a higher weighting factor designated for the relevant criterion.

4.2. Support Vector Regression Based on MTLA

To determine the prediction intervals, SVR is a very appropriate tool owing to its special features like minimizing the structure risk to keep the generalization error. It also avoids the overfitting issues arising in ANNs. The core idea of SVR is that any nonlinear mapping in the original space can be converted into a linear relationship in a higher dimensional space. Having the training set of $\{(x_i, y_i)\}^N$, the nonlinear relationship $\varphi(\cdot) : \mathbb{R}^n \rightarrow \mathbb{R}^{n_h}$ can be modeled as follows:

$$f(x) = W^T \varphi(x) + b \quad (8)$$

To find W and b values, the following equation is formed [18]:

$$\text{Min } R_{SVR} = \frac{1}{N} \sum_{t=1}^N \Theta_{\varepsilon}(y_t, W^T \varphi(x_t) + b) \quad (9)$$

$$\Theta_{\varepsilon}(y, f(x)) = \begin{cases} |f(x) - y| - \varepsilon & ; |f(x) - y| \geq \varepsilon \\ 0 & ; \text{Otherwise} \end{cases} \quad (10)$$

The setting parameters are found by minimizing the training error and keeping a top hyperplane, simultaneously. Such a combinatorial idea is shown in the form of (11):

$$\text{Min}_{W, b, \xi^*, \xi} R_{\varepsilon}(W, \xi^*, \xi) = \frac{1}{2} W^T W + C \sum_{t=1}^N (\xi_t^* + \xi_t) \quad (11)$$

In the above, the first term addresses the model difficulty and the subsequent term optimizes the training error based on the ε -insensitive loss function. The ε -loss function penalizes any training error below $-\varepsilon$ by ξ_t and above $+\varepsilon$ by ξ_t^* . The above formulation is represented in a linear form below:

$$\begin{aligned} y_t - W^T \varphi(x_t) - b & \leq \varepsilon + \xi_t^* & ; & \quad t = 1, \dots, N \\ -y_t + W^T \varphi(x_t) + b & \leq \varepsilon + \xi_t & ; & \quad t = 1, \dots, N \\ \xi_t^* & \geq 0 & ; & \quad t = 1, \dots, N \\ \xi_t & \geq 0 & ; & \quad t = 1, \dots, N \end{aligned} \quad (12)$$

By solving (12), the weighting factor W is estimated as follows:

$$W = \sum_{t=1}^N (\beta_t^* - \beta_t) \varphi(x_t) \quad (13)$$

Based on that, the SVR function in (8) is reshaped as follows:

$$\begin{aligned} f(x) &= \sum_{i=1}^N (\beta_i^* - \beta_i) K(x_t, x) + b \\ K(x_t, x) &= \varphi(x_t) \circ \varphi(x) \end{aligned} \quad (14)$$

Here, $K(x_t, x)$ is a kernel task premeditated by the inner product of $\varphi(x_t)$ and $\varphi(x)$. As represented in (14), $K(x_t, x)$ is in charge of converting the nonlinear space into a linear space in a high dimensional space. Due to the simple concept and high mapping capability, this paper considers a radial basis function (RBF):

$$K(x_t, x_j) = \exp\left(\frac{-0.5\|x_t - x_j\|^2}{\sigma^2}\right) \quad (15)$$

In the SVR model, three parameters that need to be optimized carefully since they can affect the prediction interval quality. These parameters are kernel function (σ) and hyperplane parameters (C and ε). The parameter C maintains a tradeoff between the hyperplane flatness and model training error. The parameter ε regulates the ε -insensitive loss range so that a large ε results in a smaller number of support vectors during the regression. Finally, the parameter σ affects the standard deviation of the kernel function affecting the prediction quality. This paper proposes a modified TLA (MTLA) for optimal adjustment of the above three parameters. TLA is a heuristic optimization algorithm that is inspired by the teaching process and how a teacher attempts to help students grow. The main features of TLA are local and global search operators, few adjusting parameters and a simple concept. Initially, TLA generates a random population in which each member (student) shows a possible solution, here $X = [\sigma, C, \varepsilon]$. After saving the fittest member as a teacher X_T , the whole population needs to be improved. TLA has two main steps as the improvisation phase:

Teacher Learning: Simulates the teacher's attempt to increase the students' knowledge. Therefore, the teacher, as the best member in a class X_T , moves the mean of the students to a better position, as follows:

$$X^{Iter+1} = X^{Iter} + \gamma_1 (X_T - T_F M_S) \quad (16)$$

In (16), the mean of the population is moved toward the X_T position.

Student Learning: Students can discuss a problem with each other and share knowledge to improve their positions. Such a relationship between students X_i and X_j is simulated as follows:

$$\begin{aligned} &\text{for } i = 1 : N_p \\ &\quad \text{If } F(X_i^{Iter}) < F(X_j^{Iter}) \\ &\quad \quad X_i^{Iter+1} = X_i^{Iter} + \gamma_2 (X_i^{Iter} - X_j^{Iter}) \\ &\quad \quad \text{If } F(X_i^{Iter}) < F(X_j^{Iter}) \\ &\quad \quad \quad X_i^{Iter+1} = X_i^{Iter} + \gamma_3 (X_j^{Iter} - X_i^{Iter}) \\ &\quad \text{End if} \\ &\text{End for} \end{aligned} \quad (17)$$

As can be seen in the above formulations, TLA's main advantage is that it does not require any special setting parameter. In addition, the teaching-learning step is a powerful local search that improves the convergence rate when keeping the high robustness of the algorithm. Yet, this article offers a two-stage modification approach to increase the TLA's searchability. Figure 6 shows the flowchart of the proposed MTLA algorithm.

Figure 6. Flowchart of the proposed MTLA algorithm.

Modification Method One: This modification is borrowed from the genetic algorithm (GA). It raises the diversity of the populace to avoid the occurrence of premature convergence. Therefore, for each scholar X_i , three random solutions X_{s1} , X_{s2} and X_{s3} are chosen randomly so that $s_1 \neq s_2 \neq s_3 \neq i$. A mutated individual is then generated as follows:

$$X^{mut} = X_{s1} + \gamma_4 \times (X_{s2} - X_{s3}) \quad (18)$$

Three test students are made, deploying the crossover operator:

$$\begin{aligned} x_j^{test1} &= \begin{cases} x_{mut,j} & \text{if } \gamma_5 \leq \gamma_6 \\ x_{T,j} & \text{if } \gamma_5 > \gamma_6 \end{cases} \\ x_j^{test2} &= \begin{cases} x_{mut,j} & \text{if } \gamma_6 \leq \gamma_7 \\ x_{i,j} & \text{if } \gamma_6 > \gamma_7 \end{cases} \\ X^{test3} &= \phi \times X_T + \lambda_8 \times (X_T - X_{mut}) \end{aligned} \quad (19)$$

The most optimal solution amongst X^{test1} , X^{test2} , X^{test3} and X_i is stored in the population.

Modification Method Two: This modification method simulates a local search around each solution to fix its position at the best position in the neighboring area:

$$X_j^{Iter+1} = X_j^{Iter} + \Gamma \times A_j^{Iter} \quad (20)$$

5. Simulation Results

In this part, the enactment of the proposed ADM on the cyber security of an EAF is assessed. There are four SVCs located in the EAF on the 12.66 kV side of the transformer. The reactive power data are recorded for every half-cycle period at a frequency of 60. To secure the reactive power compensation carried out by the SVC in the face of cyber attacks, a confidence level of 90% is considered, making sure that any prediction interval with a lower PICL is omitted from the set. The total reactive power data samples are divided into three sets: training 40%, validation 40% and test 20%. After constructing the proposed ADM with 80% of the dataset, the other 20% is used for launching a cyber attack and assessing the model response quality. For the TLA, the initial population size is set at 20 and the termination criterion is 100. The reason for this is that it was seen that there is no further progress after 100 iterations. The ADM is located in the SVC control module to check the health of the incoming reactive power samples. Three different cyber attacks, replay attack, delay attack and FDIA, are launched on the reactive power data during the normal operation of the EAF at the refining stage at different times. Figure 7 provides the single-line diagram of the proposed test system.

Figure 7. Single-line diagram of the test system.

Since the proposed ADM works based on the prediction interval concept, at the first step, the quality of the prediction intervals made around the reactive power data of an SVC is assessed. Table 1 shows the values of the prediction criteria. To assess the tuning capability of the MTLA, the outcomes of the original TLA, genetic algorithm (GA) [26] and particle swarm optimization (PSO) [27] are compared, simultaneously. This means that the above algorithms are used for training the LUBE using the proposed smooth fuzzy cost function. These results show that the proposed LUBE-MTLA could obtain a higher PLCL value when providing a very low value of PIW. Additionally, the low value of PIB

shows that the constructed prediction intervals are more symmetric around the real reactive power samples, making it more capable of playing its role as an active ADM. Keeping in mind that these optimal criterion values are achieved by optimizing the proposed smooth fuzzy cost function, the appropriate quality of the cost function is proved.

Table 1. Constructing optimal prediction intervals based on the proposed smooth fuzzy cost function.

Algorithm	PICL	PIW	PIB	Fuzzy Function
LUBE-GA	89.8729	27.5210	12.5624	0.22166
LUBE-PSO	90.4106	24.4186	9.5277	0.10532
LUBE-TLA	92.1732	25.3168	7.4624	0.11167
LUBE-MTLA	94.8264	21.5539	6.2764	0.04234

At this point, the appropriate performances of the proposed LUBE-MTLA as well as the smooth fuzzy cost function are revealed. Now, it is time to assess the performance of the model against cyber attacks. As was mentioned before, three different types of cyber attacks are launched to compromise the reactive power samples received by the SVC controller. Based on the sample data received, the proposed anomaly detection response will result in four different decisions: (1) true positive, (2) true negative, (3) false positive and (4) false negative. A decision is positive when the model recognizes it as malicious activity. A decision is negative when it is recognized as normal behavior. True and false decisions are made when the model makes a correct decision and a wrong decision, respectively. This makes us conclude that an ADM with high true rates and low false rates is preferred. Based on these four decisions, four indices are defined to assess our model performance, including hit rate (*HR*), false alarm rate (*FR*), miss rate (*MR*), and correct reject rate (*CR*). Figure 8 shows the confusion matrix representing these four indices.

		Actual Value From Experiment	
		positives (C_A)	negatives (C_N)
Anomaly Detection Model Response	positives (C_O)	<u>Hit Rate</u> True Positive (TP)	<u>False Alarm Rate</u> False Positive (FP)
	negatives (C_I)	<u>Miss Rate</u> False Negative (FN)	<u>Correct Rejection Rate</u> True Negative (TN)

Figure 8. Confusion matrix for the proposed ADM.

In order to formulate the above indices, C_A and C_N are defined as the compromised data and normal data, respectively. Then, *HR*, *FA*, *MR* and *CR* can be calculated:

$$HR = \frac{|H_i|}{|C_A|} ; H_i = \{X \in D | X \in C_A \& X \in C_O\} \quad (21)$$

$$FR = \frac{|F_A|}{|C_N|} ; F_A = \{X \in D | X \in C_N \& X \in C_O\} \quad (22)$$

$$MR = \frac{|M_i|}{|C_A|} ; M_i = \{X \in D | X \in C_A \& X \in C_I\} \quad (23)$$

$$DR = \frac{|C_R|}{|C_N|} ; C_R = \{X \in D | X \in C_N \& X \in C_I\} \quad (24)$$

where D shows the set of all data received by the SVC controller, C_I shows the inlier set and C_O shows the outlier set. Table 2 shows the performance quality of the proposed ADM in the face of cyber attacks of different types. For the replay attack, 20 samples of the reactive power are recorded and resent by the attacker. For the delay cyber attack, a time delay of 83 (ms) is launched by the hacker (simulating a 10-sample delay) to affect the SVC performance. In the case of an FDIA, 28 fake samples are injected into the system. All cyber attacks are repeated at different time intervals to assess the model performance at different times of the EAF operation. According to the results in Table 2, the proposed ADM has shown great performance by providing high HR% and CR% rates. In other words, the prediction intervals constructed by the model could distinguish between the false data and true data with a high percentage. It is also seen that making correct reject decisions in the face of an FDIA is a harder task in comparison with the replay attack and delay attack. The low values of FR% for a replay attack and time-delay attack demonstrate this concept. Overall, it is seen that the ADM is resistant to cyber attacks of different types. It should be noted that the low values of the false positive decisions made by the proposed model are not dangerous to the EAF since they happen in the limited lower and upper bounds. Such a very low false positive value shows the very high reliability and accuracy of the proposed ADM, which cannot cause any problem for the EAF. This means that the false-positive decisions of the model have happened for those compromised reactive power samples with values close to the real samples. Although such small values may cause flickers in the neighboring load, they cannot cause severe issues which need big estimation errors in the reactive power estimation.

Table 2. Confusion matrix values for different ADMs.

Cyber Attack	HR (%)	MR (%)	FR (%)	CR (%)
FDIA	95.23%	4.76%	9.52%	90.47%
Replay Attack	94.11%	5.88%	2.59%	97.41%
Time-Delay Attack	93.28%	6.71%	1.87%	98.13%

In order to better perceive this idea, a part of the compromised reactive power signal is shown in Figure 9. In this figure, the prediction intervals constructed by the proposed model along with the real reactive power samples are plotted in the same frame. The small black circles show the fake data being injected by either a replay attack, FDIA, or time-delay attack. The red line and the blue solid line show the upper and the lower bounds of the prediction intervals constructed by the model. The small green points show the real reactive power data. The black circles show fake data and red circles show real data being compromised. According to this figure, the real data samples of the reactive power data in the EAF are surrounded by the lower and upper bounds made by the prediction intervals. The model shows how a prediction interval model can distinguish compromised data from real data in the face of different cyber attacks at different times.

Table 3 compares the anomaly detection capability of the proposed model with the conventional LUBE-based ANN and the conventional LUBE-based SVR. The simulation outcomes show that the proposed model has higher HR% and CR% rates than the other algorithms. This may be partly due to the proposed smooth fuzzy cost function and partly due to the MTLA. The former helps to construct symmetric intervals around the reactive power data, which is significant in anomaly detection processes, and the latter improves the training process of the support vectors by optimal adjustment of the setting parameters. By comparing the results of the conventional LUBE method in the first row with other models, it is deduced that the high complexity of the reactive power demand in the EAF has caused overfitting issues by the model, thus reducing its modeling capabilities. Such high HR% and CR% rates show the high classifying capability of the proposed model as an ADM.

Figure 9. Detecting cyber attacks launched in an EAF using the proposed ADM.

Table 3. Indices values of confusion matrix against different cyber attacks.

Outlier Algorithm	HR (%)	MR (%)	FR (%)	CR (%)
Conservative LUBE	86.21%	13.79%	11.40%	89.60%
Support Vector	91.93%	8.07%	8.52%	91.48%
Machine-Based LUBE	94.22%	5.78%	4.66%	95.34%
Proposed Model	94.22%	5.78%	4.66%	95.34%

6. Discussion

This article proposes a novel anomaly detection method based on LUBE and MTLA for securing the reactive power compensation in the SVC in EAFs. In this regard, three different cyber attacks, the time-delay attack, replay attack and FDIA, are explained. The proposed method shows special features which are of significant importance for the cyber security of EAFs:

- **EAF as a cyber-physical system:** The performance of the EAF for reactive power compensation depends on the SVC. Fundamentally, the SVC structure comprises a control system (as the cyber layer) and power electronic devices (as the physical layer) which makes it vulnerable to cyber attacks. This article proves the necessity of assessing the cyber security of EAFs from a new perspective.
- **Precise ADM:** Compared to the other anomaly detection methods, the proposed ADM shows superior performance considering the prediction interval-based structure. Making use of the LUBE method, the proposed model is equipped with a lower and an upper bound based on specific probabilities which can estimate the reliability and health probability of the incoming reactive power data. According to the confusion matrix, the proposed ADM method could reach 94.22%, 5.78%, 4.66%, and 95.34% for HR, MR, FR and CR, respectively. The superiority of the model over the conservative and support vector machine is proved.
- **Evolving nature:** The proposed MTLA approach could provide a more optimal training process for LUBE to reach the highest PICL and lowest PIW. Such an evolving concept would enhance the quality of LUBE by creating more fitting prediction intervals. The proposed MTLA is equipped with three modification methods for avoiding premature convergence and more optimal search abilities.

7. Conclusions

It is shown in this research that an EAF is a significant cyber-physical system that requires a powerful ADM for detecting and stopping any cyber hacking. In this way, this paper proposed a secure and reliable ADM based on prediction intervals to construct

estimation bounds around the reactive power demands of the EAF. The model structure benefited from a new smooth fuzzy cost function developed to provide symmetrical intervals based on SVR. The simulation outcomes on the EAF real data show that, despite the highly variable nature of the reactive power signal, the proposed model could follow it very appropriately. The cyber indices calculated by the confusion matrix reveal the high CR% and CR% rates against different cyber attack types, including replay attack, FDIA, and delay-attack. From an optimization point of view, the proposed MTLA could help with better training of SVR models for optimal parameter adjustment and thus optimizing the fuzzy cost function. The simulation results show the high following capability of the proposed model for the reactive power data. The high accuracy of over 94% shows the highly reliable and secure performance of the proposed ADM method over the conventional SVR and LUBE method.

Author Contributions: Conceptualization, M.R., L.Z. and M.A.M.; methodology, T.X.; software, L.Z. and M.A.M.; validation, S.K.E., M.A., K.J., U.D. and M.A.M.; formal analysis, M.R., T.X., M.A.; investigation, M.R., S.K.E., U.D. and M.A.M.; resources, U.D.; data curation, M.A.M.; writing—original draft preparation, M.R., L.Z. and M.A.M.; writing—review and editing, S.K.E. and M.A.M.; visualization, K.J.; supervision, M.A.M.; project administration, M.A.; funding acquisition, U.D. All authors have read and agreed to the published version of the manuscript.

Funding: The authors would like to acknowledge the financial support received from Taif University Re-searchers Support, Project Number (TURSP-2020/146), Taif University, Taif, Saudi Arabia.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available on request from the corresponding author: dr.mohamed.abdelaziz@mu.edu.eg (M.A.M.).

Acknowledgments: The authors would like to acknowledge the financial support received from Taif University Researchers Support, Project Number (TURSP-2020/146), Taif University, Taif, Saudi Arabia.

Conflicts of Interest: The authors declare no conflict of interest.

Nomenclature

w/b	Weight/bias factors in support vector model ($b \in \mathbb{R}$).
C	Tradeoff constant between two terms.
$K(x_t, x)$	Kernel function.
M_s	Mean of the class population in TLA.
$Iter$	Iteration counter.
N/N_p	Amount of TLA population/forecast data.
$C_I/C_O/C_A/C_N$	Set of inlier/outliers/positive data/negative data.
A_i	Distance between i^{th} solution and X_T .
R	Underlying target range used for normalizing prediction intervals.
T_F	Random value equivalent to 1 or 2 in TLA.
U_t/L_t	Higher and lower bounds of the PIs.
X_i^{Iter}	Position of i^{th} solution (student) in iteration number $Iter$.
x, y	Input/output sample points.
X_T	Position of the best solution (teacher) in TLA.
α	Confidence level complement.
ε	Small constant value.
Θ_ε	Loss function in SVR.
σ	Kernel function standard deviation.
Γ	Small constant value for neighboring local search.
ζ	Preparation error.
$\beta^* \text{ \& } \beta$	Lagrangian multipliers.

$\mu_{f,k}$	Fuzzy membership function value for the k^{th} index.
$\gamma_1, \dots, \gamma_8$	Random values in the range [0, 1].
$\mu_{ref,k}$	Fuzzy reference value for k^{th} index.
Δ	Scale parameter in the exponential model.
τ	Delay parameter in the delay attack.

References

- Roslan, N.H.; Ismail, M.; Khalid, N.H.A.; Muhammad, B. Properties of concrete containing electric arc furnace steel slag and steel sludge. *J. Build. Eng.* **2020**, *28*, 101060. [\[CrossRef\]](#)
- Esfahani, M.T.; Vahidi, B. A predictive reactive power measuring based on time series and DLSL algorithm for compensating applications. *IEEE Trans. Instrum. Meas.* **2015**, *64*, 2646–2656. [\[CrossRef\]](#)
- Naji Alhasnawi, B.; Jasim, B.H.; Anvari-Moghaddam, A.; Blaabjerg, F. A New Robust Control Strategy for Parallel Operated Inverters in Green Energy Applications. *Energies* **2020**, *13*, 3480. [\[CrossRef\]](#)
- Hsu, Y.J.; Chen, K.H.; Huang, P.Y.; Lu, C.N. Electric arc furnace voltage flicker analysis and prediction. *IEEE Trans. Instrum. Meas.* **2011**, *60*, 3360–3368. [\[CrossRef\]](#)
- Nami, H.; Anvari-Moghaddam, A.; Arabkoohsar, A. Thermodynamic, economic, and environmental analyses of a waste-fired trigeneration plant. *Energies* **2020**, *13*, 2476. [\[CrossRef\]](#)
- Júnior, H.G.; Liberado, E.V.; Pomilio, J.A.; Marafão, F.P. General-compensation-purpose Static var Compensator prototype. *HardwareX* **2019**, *5*, e00049.
- Spasojevic, B. The time domain method for power line reactive energy measurement. *IEEE Trans. Instrum. Meas.* **2007**, *56*, 2033–2042. [\[CrossRef\]](#)
- Morsi, W.G.; Diduch, C.P.; Chang, L.; El-Hawary, M.E. Wavelet-based reactive power and energy measurement in the presence of power quality disturbances. *IEEE Trans. Power Syst.* **2010**, *26*, 1263–1271. [\[CrossRef\]](#)
- Chow, T.W.S.; Yam, Y.F. Measurement and evaluation of instantaneous reactive power using neural networks. *IEEE Trans. Power Deliv.* **1994**, *9*, 1253–1260. [\[CrossRef\]](#)
- Golshan, M.H.; Samet, H. Updating stochastic models of arc furnace reactive power by genetic algorithm. In Proceedings of the 14th International Conference on Harmonics and Quality of Power-ICHQP 2010, Bergamo, Italy, 26–29 September 2010; pp. 1–9.
- Samet, H.; Mojallal, A. Enhancement of electric arc furnace reactive power compensation using Grey–Markov prediction method. *IET Gener. Transm. Distrib.* **2014**, *8*, 1626–1636. [\[CrossRef\]](#)
- Zhang, D.J.; Zhang, G.L.; Zhang, N.N. The operating conditions prediction of electric arc furnace based on least squares support vector machines. In Proceedings of the 2010 International Conference on Computer, Mechatronics, Control and Electronic Engineering, Changchun, China, 24–26 August 2010; Volume 3, pp. 263–266.
- Govindarasu, M.; Hann, A.; Sauer, P. Cyber-physical systems security for smart grid. *Power Syst. Eng. Res. Cent.* **2012**. Available online: https://pserc.wisc.edu/documents/research_documents/futuregrid/info_architecture/Govindarasu_BA_Info_PSERC_DOE_Poster_2011.pdf (accessed on 14 May 2021).
- Chen, B.; Butler-Purpy, K.L.; Nuthalapati, S.; Kundur, D. Network delay caused by cyber-attacks on SVC and its impact on transient stability of smart grids. In Proceedings of the 2014 IEEE PES General Meeting, Conference and Exposition, National Harbor, MD, USA, 27–31 July 2014; pp. 1–5.
- Ten, C.W.; Yamashita, K.; Yang, Z.; Vasilakos, A.V.; Ginter, A. Impact assessment of hypothesized cyberattacks on interconnected bulk power systems. *IEEE Trans. Smart Grid* **2017**, *9*, 4405–4425. [\[CrossRef\]](#)
- Lee, R.M.; Assante, M.J.; Conway, T. German steel mill cyber-attack. *Ind. Control Syst.* **2014**, *30*, 62.
- Chen, B.; Mashayekh, S.; Butler-Purpy, K.L.; Kundur, D. Impact of cyber attacks on transient stability of smart grids with voltage support devices. *IEEE Power Energy Soc. Gen. Meet.* **2013**. [\[CrossRef\]](#)
- Kavousi-Fard, A. Modeling uncertainty in tidal current forecast using prediction interval-based SVR. *IEEE Trans. Sustain. Energy* **2016**, *8*, 708–715. [\[CrossRef\]](#)
- Yu, K.; While, L.; Reynolds, M.; Wang, X.; Liang, J.J.; Zhao, L.; Wang, Z. Multiobjective optimization of ethylene cracking furnace system using self-adaptive multiobjective teaching-learning-based optimization. *Energy* **2018**, *148*, 469–481. [\[CrossRef\]](#)
- Langner, R. Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Secur. Priv.* **2011**, *9*, 49–51. [\[CrossRef\]](#)
- Chen, B.; Butler-Purpy, K.L.; Kundur, D. Impact analysis of transient stability due to cyber-attack on FACTS devices. In Proceedings of the 2013 North American Power Symposium (NAPS), Manhattan, KS, USA, 22–24 September 2013; pp. 1–6.
- Davis, C.M.; Tate, J.E.; Okhravi, H.; Grier, C.; Overbye, T.J.; Nicol, D. SCADA cyber security testbed development. In Proceedings of the 2006 38th North American Power Symposium, Carbondale, IL, USA, 17–19 September 2006; pp. 483–488.
- Khosravi, A.; Nahavandi, S.; Creighton, D.; Atiya, A.F. Lower upper bound estimation method for construction of neural network-based prediction intervals. *IEEE Trans. Neural Netw.* **2010**, *22*, 337–346. [\[CrossRef\]](#)
- Lan, T.; Jermisittiparsert, K.; Alrashood, S.T.; Rezaei, M.; Mohamed, M.A. An advanced machine learning based energy management of renewable microgrids considering hybrid electric vehicles' charging demand. *Energies* **2021**, *14*, 569. [\[CrossRef\]](#)
- Wang, Q.; Jin, T.; Mohamed, M.A. A Fast and Robust Fault Section Location Method for Power Distribution Systems Considering Multisource Information. *IEEE Syst. J.* **2021**. [\[CrossRef\]](#)

-
26. Mohamed, M.A.; Eltamaly, A.M.; Alolah, A.I. Sizing and techno-economic analysis of stand-alone hybrid photovoltaic/wind/diesel/battery power generation systems. *J. Renew. Sustain. Energy* **2015**, *7*, 063128. [[CrossRef](#)]
 27. Mohamed, M.A.; Eltamaly, A.M.; Alolah, A.I. PSO-based smart grid application for sizing and optimization of hybrid renewable energy systems. *PLoS ONE* **2016**, *11*, e0159702. [[CrossRef](#)] [[PubMed](#)]