Cyber-Attack on P2P Energy Transaction Between Connected Electric Vehicles: A False Data Injection Detection Based Machine Learning Model

Dhaou Said, Mayssa Elloumi, Lyes Khoukhi

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 6, 2022, accepted June 9, 2022, date of publication June 13, 2022, date of current version June 20, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3182689

Cyber-Attack on P2P Energy Transaction Between Connected Electric Vehicles: A False Data Injection Detection Based Machine Learning Model

DHAOU SAID[1], (Member, IEEE), MAYSSA ELLOUMI[2], (Student Member, IEEE), AND LYES KHOUKHI[3], (Senior Member, IEEE)

[1]Department of Electrical Engineering and Computer Science, University of Sherbrooke, Sherbrooke, QC J1K 2R1, Canada
[2]The National School of Computer Science Tunis, Manouba 2010, Tunisia
[3]GREYC Laboratory, ENSI CAEN, 14000 Caen, France

Corresponding author: Dhaou Said (dhaou.said@usherbrooke.ca)

ABSTRACT When cybersecurity is neglected, any network system loses its efficiency, reliability, and resilience. With the huge integration of the Information, Communication and Technology capabilities, the Connected Electric Vehicle (CEV) as a transportation form in cities is becoming more and more efficient and able to reply to citizen and environmental expectations which improve the quality of citizens' life. However, this CEV technological improvement increases the CEV vulnerabilities to cyber-attacks resulting to serious risks for citizens. Thus, they can intensify their negative impact on societies and cause unexpected physical damage and economic losses. This paper targets the cybersecurity issues for CEVs in parking lots where a peer-to-peer(P2P) energy transaction system based on blockchain, and smart contract scheme is launched. A False Data Injection Attack (FDIA) on the electricity price and power signal is proposed and a Machine Learning/SVM classification protocol is used to detect and extract the right values. Simulation results are conducted to prove the effectiveness of this proposed model.

INDEX TERMS Blockchain, connected electric vehicles, false data injection attack, machine learning, short vector machine, smart contract.

I. INTRODUCTION

Connected Electric Vehicles (CEVs) [1] are a new mobility concept that is growing rapidly over the last decades. CEVs are a mix of hardware and software pieces with communication capabilities making them expected to be the main part of the smart city deployment especially in terms of the energy ecosystem, clean mobility service and even for data collect and routing. Compared to traditional transportation system, CEVs are seen as a new form of mobility in cities able to help in the energy transition vision by replying to Net-Zero and COP26 commitments related to environmental issues, the pollution reduction, and the service efficiency for citizens. The success of the CEV concept is depending on its range capability and its battery energy management in terms of capacity, the charging and discharging rate, and the availability of the EV Supply Equipment (EVSE).

In one hand, automakers are already starting manufacturing thousands of new electric cars and trucks which can make pressure on the current power system especially for peak periods where an increased number of CEVs are plugged-in in the same period to charge their batteries. In the other hand, the CEV is co-locating electricity consumption and control based on its specific architecture and its capabilities on Information and Communication Technologies (ICTs) such as intelligent software systems with capabilities of network and Internet of Things (IoT). However, as show in Fig.1, all these ICT capabilities create potential cyber vulnerabilities and access points with a high risk of data privacy disclosure which can be maliciously exploited by cyber-attackers. This cybersecurity problem increases especially where decentralized models are considered in the interaction between CEVs for data and energy peer-to-peer (P2P) transaction.

The associate editor coordinating the review of this manuscript and approving it for publication was Rongbo Zhu.

One of the most common type of cyber-attacks that was originally introduced in the power systems (see Fig. 2) is the False Data Injection Attack (FDIA). This type of attack is able to compromise the most vital concern of the data integrity by infecting devices and surpassing firewalls. It can create untruthful values of the state estimation (SE) [2], use malware to infect servers of power suppliers, falsify the real quantity of energy truly provided, and maliciously forget the network states by invalidating nodes. Thus, the FDIA can provide a huge misleading of the energy distribution, resulting in devastating power shortage, extra energy transmission costs, blackouts, and overloads. Mainly, FDIA can target (1) the electricity price and (2) the power line load. For the first scenario, this attack manipulates the price data received from a utility or any other electricity service provider. As a result, each consumer will receive different electricity prices which make an uncontrollable demand side management mechanism by messing the metering data transmission. This false metering can cause for example a dysfunction of the load balancing procedure or scheduling protocol. The damage is in terms of instability of the grid network or in terms of decreased user satisfaction levels. The second case is based on the malfunction of a system operation caused by injecting false data into the measurement system. Thus, a hacker can manipulate the consumer and or the utility load which can result in significant and costly damage to the power grid. This damage can go to Smart Grid (SG) infrastructure and a potential SG failure by overloading the devices and power lines Which can cost billion of dollars for certain communities in addition to victims which are losing their life in certain situations.

To overcome this problem, the attack detection is the most essential step in minimizing the damages. Several approaches are proposed since 2010 to detect FDIAs [3]. Some of them were based on SE type such as the conventional bad data detection, the SE partitioning, and the detection based on dynamic SE. Other approaches are based on protection, among them there are the optimal Phasor Measurement Unit (PMU) placement [4], and the selection of optimal measurements.

Another Method to detect FDIA Which is based on statistical modelling [5], argues that the Generalized Likelihood Ratio (GLR) test detector is not efficient when a large number of samples are compromised, and the Bayesian test detector also cannot detect FDIAs if the attacker replaces current meter readings with historical ones. Also, the quickest change detector, the statistical distance index, the sparse matrix recovery [6] and many other statistical approaches are used in cybersecurity literature. In this work, we focus on the detection of FDIA using Machine Learning (ML) approach (which is the most disruptive method of the Artificial Intelligence (AI)) for a P2P energy transaction between CEVs in parking lots.

Our contributions are as follows: 1) To date, this work is the first to focus on applying ML to tackle the cybersecurity challenge such as FDIA in parking lots where a P2P energy transaction between CEVs can be launched. 2) We present a detailed FDIA model. 3) We highlight the SVM as a powerful ML technique able to fight the FDIA. 4) The numerical simulations of FDIA on the price and power data are shown to prove the efficiency of our proposal.

The remainder of the paper is organized as follows. Section II discusses some challenges, issues and related work of cybersecurity in SG. In Section III, our model of the FDIA is presented. Section IV numerical simulations for the FDIA model and SVM detector for P2P energy transaction between CEVs is presented. Finally, concluding remarks and open issues are drawn in Section V.

II. RELATED WORKS

The topic of FDIA is attracting several industrials and cybersecurity researchers in different fields and especially in SG as a centralized architecture. To mitigate the FDIA, many approaches are proposed in literature. For the FDIA detection, research works can be classified into 4 essential sub-classes. The first one focuses on the SE type. The Second one targets the protection-based defense. The third one considers the statistical models and the last one is based on the using of the ML capabilities.

For the first category, in the reference [7], the statistical test of the Largest Normalized Residual (LNR) is presented to detect non-critical, single, and multiple, interacting issues but non-conforming bad data. It is shown that this model is not efficient for bad leverage points. For the second category, the authors of [4] propose a PMU placement technique to ensure that an L1 state estimator has the necessary amount of resilience against poor measurements. However, PMUs are expensive, and installing enough of them to ensure sensor readings is impractical. It is more expensive, particularly with the integration of new ubiquitous sensing technology into large-scale of network systems such as Smart Grids.

For the third category, many statistical models were proposed, for example the Bayesian test detector in reference [8] where authors developed a Bayesian test to identifying relay misbehavior (false data injection) at the packet level in loss one-way wireless relay networks, nevertheless, another study [9] shows that the Bayesian technique fails to detect an attack when malicious data has the same distribution pattern as historical data or when an adversary replaces current meter readings with prior readings with the same distribution. Although these approaches stated above are making improvement in detecting FDI assaults, but they are becoming increasingly limited as FDIAs get more complex and sophisticated schemes able to surpass the SG protection layers.

In the last category, based on examination of the current research works, it found out that many studies were conducted in the topic of FDIA using ML like [10], [11] where different ML models like the Recurrent Neural Network (RNN) and Artificial Neural Network (ANN) to detect FDIA in bad nodes or in power system state estimators and there are many other studies prove that ML is an efficient tool to detect FDIA in power system.

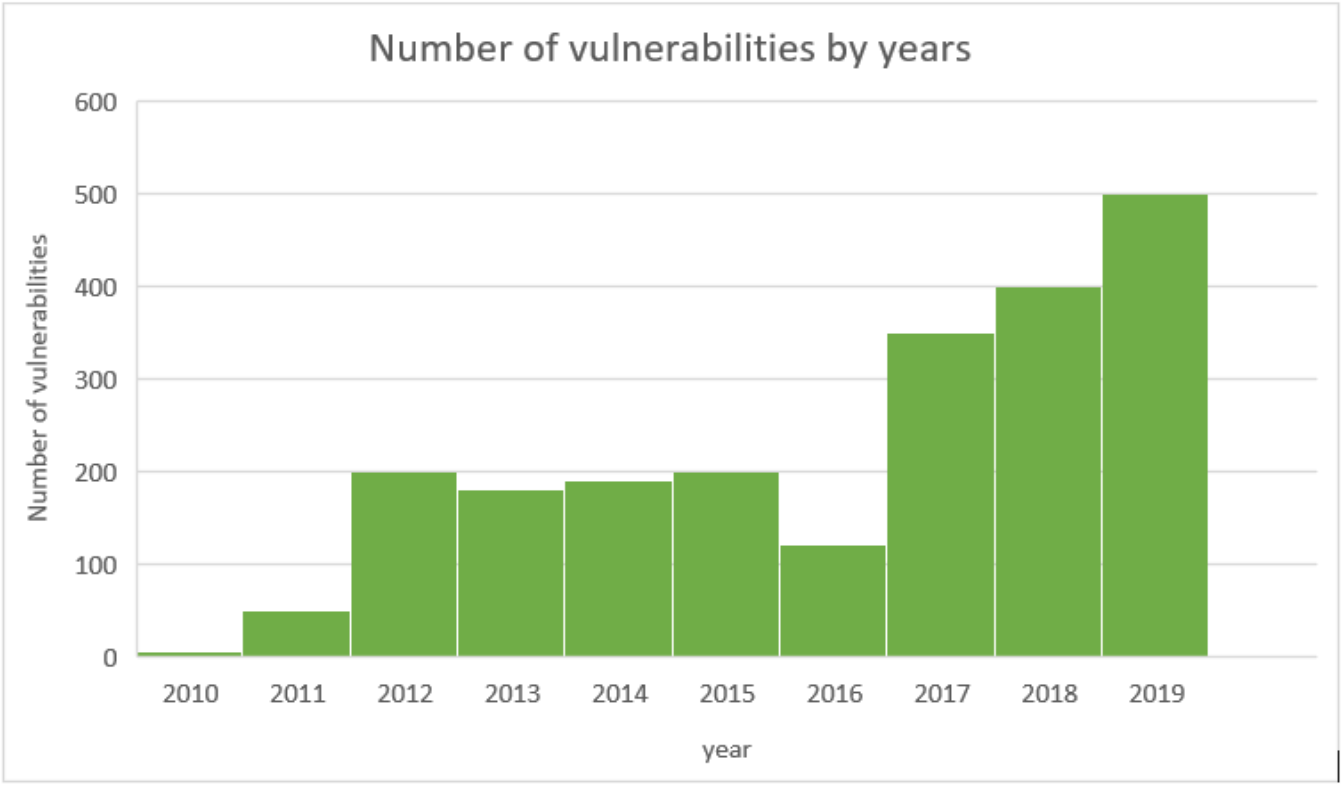

FIGURE 1. Cybersecurity vulnerabilities.

A recent method [12] is targeting the blind FDIA detection for large-scale power grid and high-level measurement noise. Also, the reference [13] presents a data-driven FDIA detection with improves reliability and resilience of the wind energy forecasting.

We mention that all these research efforts do not target the ML/SVM classification model in FDIA detection in a decentralized architecture between CEVs in P2P energy transaction.

III. PROPOSED MODEL

We consider a group of CEVs willing to launch an open electricity market in a parking lot when all supply plug-ins are occupied. The system is presented in Fig.3. We suppose that the parking lot is equipped by a blockchain server [1]. We use a consortium blockchain based Ethereum achitecture and any CEV buyer or seller can connect to our system.

We take into account a predictive bidding approach (PBA) [1] based on stochastic bids that will be run into the smart contract based on a trained model.

The smart contract is a digital contract that eases the process of agreement between CEVs by imposing predefined clauses such as bidding and payment functions. In our Blockchain based system, the data integrity, security, trustworthiness, and decentralization approach made it a trustful network. But that doesn't mean that it will be safe from any external attack, because the security is guaranteed only in case we are inside the Blockchain network.

This system environment is mainly based on ICT capabilities which increase its vulnerability to many kinds of cyber-attacks such as FDIA.

As presented in Fig.4, we suppose that an attacker injects a false data vector 'a' into our training data which will jeopardize the network and deliver a false results.

In this context, FDIA detection is treated as a supervised binary classification problem. Based on the research work done in [14] the SVM is more efficient than CNN and KNN in anomaly detection with 91.29 % of precision. Moreover, the SVM is a popular practice for training a decision boundary that divides data into several classes. as shown in Fig.5, the SVM is based on a hyperplane that maximizes the separation margin between two classes. The training points which are close to the limit defining this division margin are called support vectors. So, in this case we are seeking a hyper-plane that separates attacked $(+1)$ and secure data (-1) in a N dimensional feature space. We can illustrate the distribution of our data by the following system:

$$\begin{cases} W^T.S_i + b = +1, & \text{if } y_i = +1 \\ W^T.S_i + b = -1, & \text{if } y_i = -1 \end{cases} \tag{1}$$

considering that:

$$y = \begin{cases} +1, & \text{if } b \neq 0 \\ -1, & \text{if } b = 0 \end{cases} \tag{2}$$

A hyperplane is represented by a weight vector $W \in R^N$ and a bias variable $b \in R$, and a sample $S_i \in Dtrain$

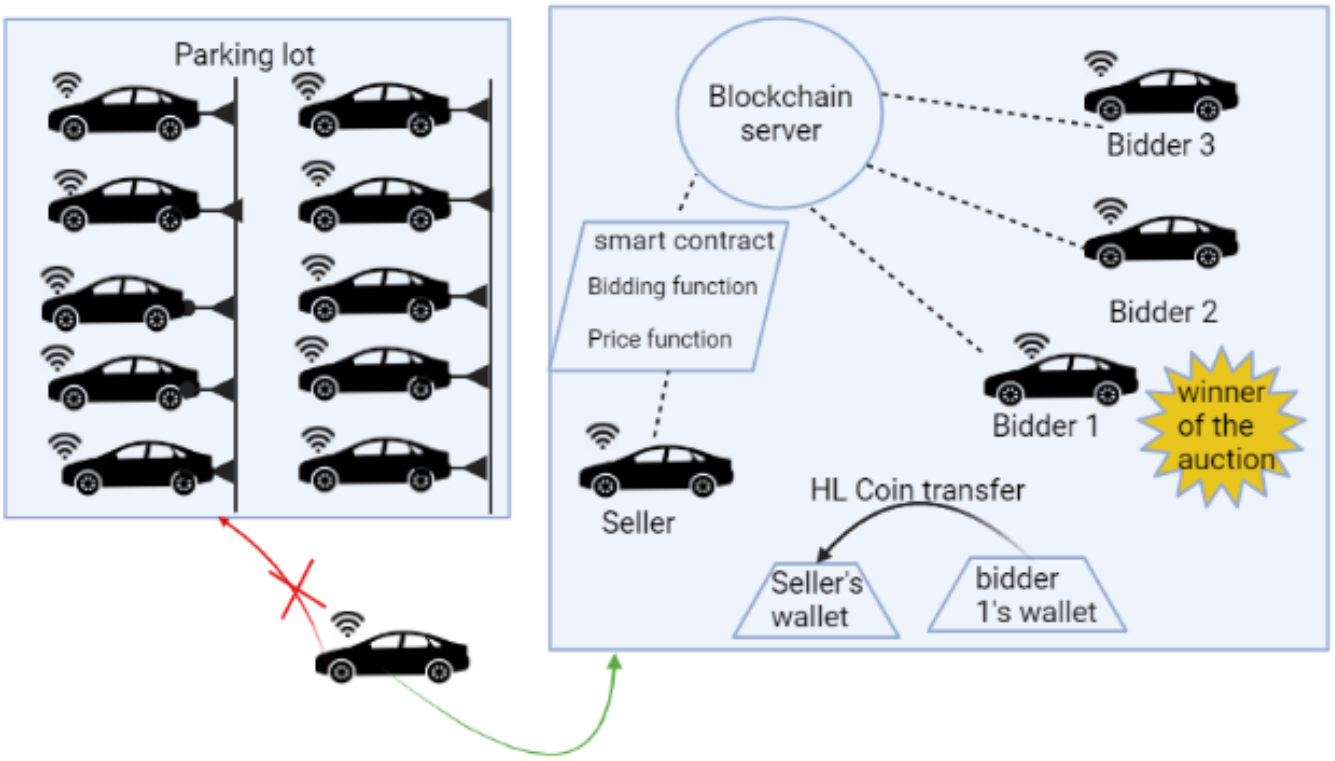

FIGURE 2. Conceptual architecture for our system model.

which results in:

$$W^T.S_i + b = 0 \tag{3}$$

where S_i is the feature vector of the given sample which located on the hyper plane. Fig.5 and Fig.6 illustrate the process of the attack detection using Machine Learning.

To determine the hyperplane this condition should be verified:

$$y_i.(W^T.S_i + b) \geq 1 \quad \forall i = 1, 2, 3 \ldots .T \tag{4}$$

where T is the number of the training data. As the margin between the two support vectors D is defined as:

$$\frac{D}{W^2} \tag{5}$$

the maximisation of margin hyper plane can be computed by the minimization of W^2.

Sometimes the training data is not linearly separable.

In other words, to ensure that the SVM classifier does not over-fit the noisy data (or to create a soft margin), we have to introduce a new variable, called slack variable $\xi_i \geq 0$, to allow some data points to lie within the margin, and in this case optimization problem will be descried as:

$$y_i(w^T + b) \geq 1 - \xi_i \tag{6}$$

In case $\xi_i > 0$ we can think of ξ_i as an error tern associated with variable S_i and the average error can be given as:

$$\frac{1}{n}.\sum_{i=1}^{n} \xi_i \tag{7}$$

and the determination of the hyper plane will be by solving this equation:

$$\min_{w,\xi_i} \frac{\|W\|^2}{2} + C\sum_{i=1}^{n} \xi_i \tag{8}$$

where C in a positive constant that calculates the trade-off between maximizing the margin and the number of training data points in the margin.

SVM Algorithm

Input: The training data Dtrain = [S,Y] where S is array of input with N features and Y is an array of class labels $\in \{-1, +1\}$

Output: $Y_i = sgn(W^T.S_i + b)$

1: Assign H(x)=$\sum_{i=1}^{N} W^T.S_i + b = 0$

2: Minimize the quadratic optimization problem: min $\theta(w, \xi_i) = \frac{\|W\|^2}{2} + C\sum_{i=1}^{N} \xi_i$

3: Calculate the Lagrangian multipliers: $minL_p(w, b, \alpha) = \frac{\|W\|^2}{2} - \sum_{i=1}^{N} \alpha_i.Y_i.(W^T.S_i + b) + \sum_{i=1}^{N} \alpha_i$ Where α is the Lagrange multiplier

4: Calculate $maxL_D(w, b, \alpha) = \sum_{i=1}^{N} \alpha_i - \frac{1}{2}.\sum_{i,j=1}^{N} \alpha_i\alpha_j Y_i Y_j S_i{}^T S_j$ subject to $\alpha_i \geq 0$ and $\sum_{i=1}^{N} Y_i.\alpha_i = 0$

IV. SIMULATION RESULTS

In this section, we present the simulation results and discussions of our proposed scheme performance. We consider a

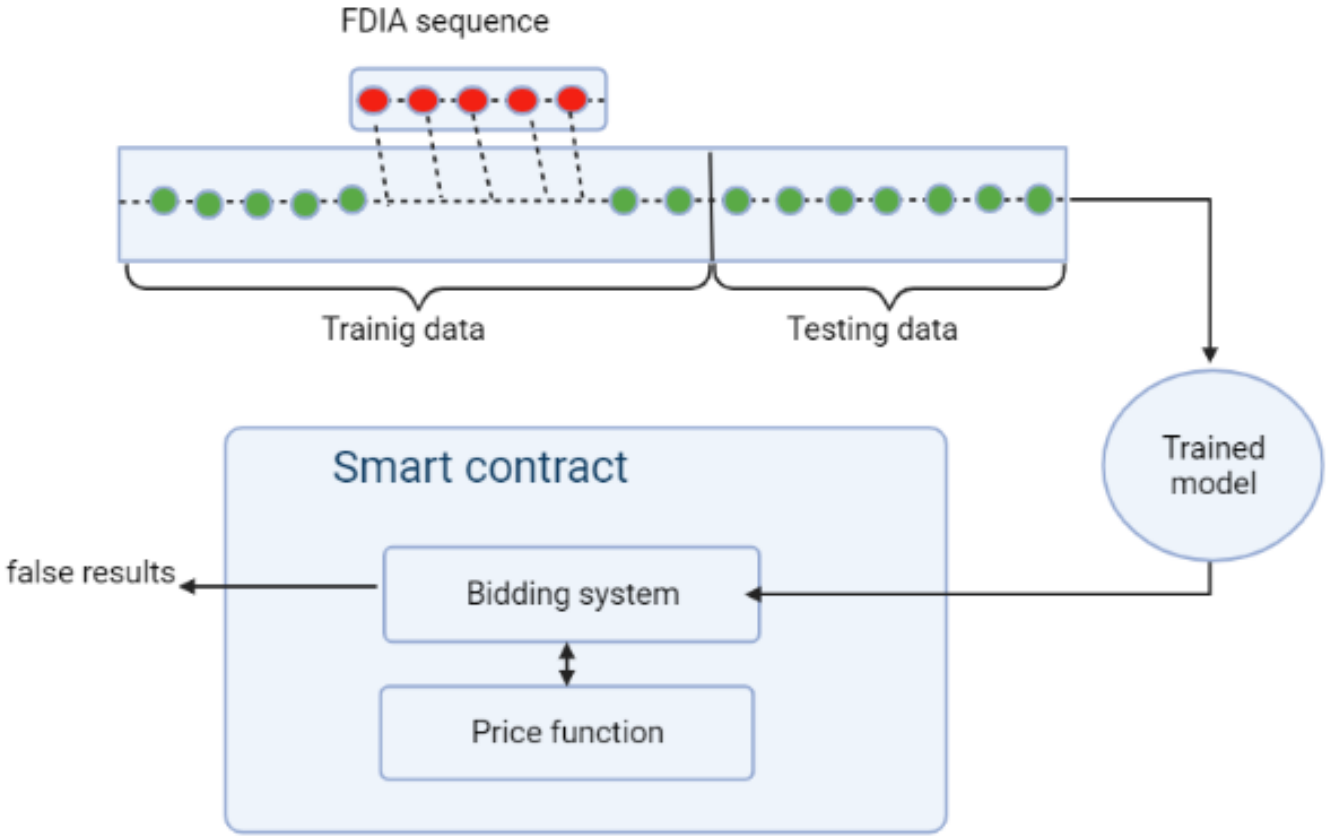

FIGURE 3. A false data injection attack on our machine learning model.

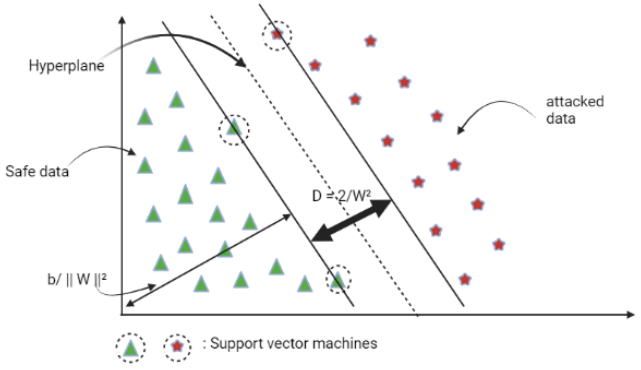

FIGURE 4. Attack detection using support vector machine.

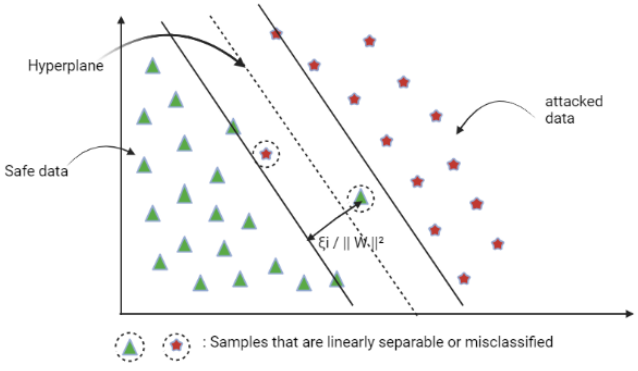

FIGURE 5. Attack detection using the linearly non-separable dataset.

scenario in a real urban area of Ottawa where 20 parking lots are sharing a 4 × 4 km 2.

The simulation parameters of this study are summarized in TABLE 1.

To illustrate our problem, we assume that CEVs can interact wirelessly with one another and each CEV decides the amount of power to be sold or purchased during a certain period. We suppose that all parking lots have a blockchain server that is active, and that the blockchain server can receive all information about CEV buyers and sellers. Also, we assume that a bidding auction is launched between CEVs buyers and sellers of electricity.

To show the effectiveness of our proposed scheme, we consider a cyber attack: (1) on the CEV buying and selling price data and (2) on the CEV seller power data using for both our proposed method to compare simulations with and without FDIA.

A. FDIA ON THE ELECTRICITY PRICE

Fig. 6. highlights the performance of our SVM Algorithm in detecting FDIA in buying and selling price (represented by

TABLE 1. Simulation parameters.

Parameter	value
Electricity Price (based electricity requested level)	15 c/kWh [15]
Minimum Electricity Selling Price(Bidding based on game theory)	8c/k Wh
Maximum Electricity Selling Price(Bidding based on game theory)	18c/k Wh
Number of CEV buyers N_b	10,30,60 [16]
Number of CEV sellers N_s	10,30,60
Energy requested by CEV buyers	Uniform distributed between 20-75%
Energy to sell by CEV sellers	Uniform distributed between 20-75%
Dch, DDisch	60 kW DC [17,18,19]
Charging time Max	20 min [20]
CEV SoC	Uniform distribution between 20-100 %
CEV Battery capacity	24 kWh [21]
Electricity price	ToU (Ontario) [22]
SoC-BDT	The battery depletion threshold (BDT) [23]

FIGURE 6. The SVM performance in extracting the right price value (buying and selling) after FDIA.

TABLE 2. Comparison between the buying and selling price with and without FDIA.

	Average value	Deviation %
Buying price classified with SVM	0.16	
Buying price attacked by FDIA	0.234	31
Selling price classified with SVM	0.14	
Seling price attacked by FDIA	0.244	42

black and Burgundy color) which reveals a large deviation margin that disturbs the whole bidding system.

From Fig.6, we can see that our SVM Algorithm performs well in anomaly detection in the data exchange between CEVs. Thus, our SVM Algorithm is able to locate and remove the corrupted data from the price signal to show as our selling price (blue one) and our buying price (red color).

The Table 2 demystifies the role of the SVM Algorithm in detecting the FDIA in our system. In fact, the average values of the buying price with and without FDIA are respectively

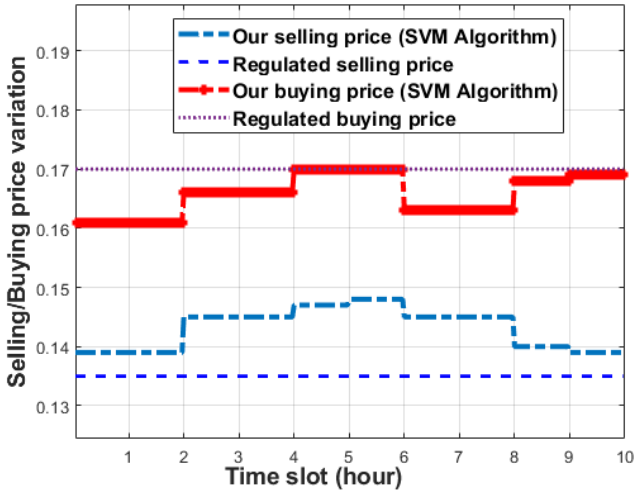

FIGURE 7. The system performance: the selling/buying electricity price in our open market between CEVs compared to the regulated ones.

0.23 and 0.16 which means a deviation of 31 percent. This misinformation will make the system failure by harming the peer's wallets when they pay more than the real amount of the price.

The same rationale is used when studying the attacked selling price and the average values of the selling price with and without FDIA are respectively 0.24 and 0.14 which means a deviation of 42 percent.

Thus, the FDIA provides a huge increase in the selling/buying price will not incentives CEVs to connect to the system of the electricity liberalized market in parking lots.

Fig.7 shows the selling/buying electricity price in our open market between CEVs compared to the regulated ones. It is clear that without cyber-attacks, the price system adapted is outperforming the regulated one.

B. FDIA ON THE AMOUNT OF ELECTRICITY ANNOUNCED BY CEV SELLER

In this case we suppose that the electricity profile of the CEV seller is falsified by an FDIA. We study throw simulations the capability of our SVM Algorithm to detect and extract the right electricity profile data. Fig. 8 compares three signals during a week (only day time is considered): the real measured data (blue color), the attacked data (black color) and the extracted data (red color) using our SVM Algorithm. From Fig.8, it is clear that our SVM Algorithm is able the detect and extract the right CVE seller' power profile. To conclude, the FDIA detection remains essential in our system (between CEVs) in order to maintain our liberalized market more and more attractive for CEV owners to exchange energy. Table 3 presents the observation results obtained from Fig. 9, which illustrates the performance of our SVM Algorithm from 9 AM to 6 PM in term of FDIA detection and extraction when the CEV seller power is attacked. As shown in Table 3, it is clear that the deviation between the true CEV seller power values and the attacked ones is around 32 percent.

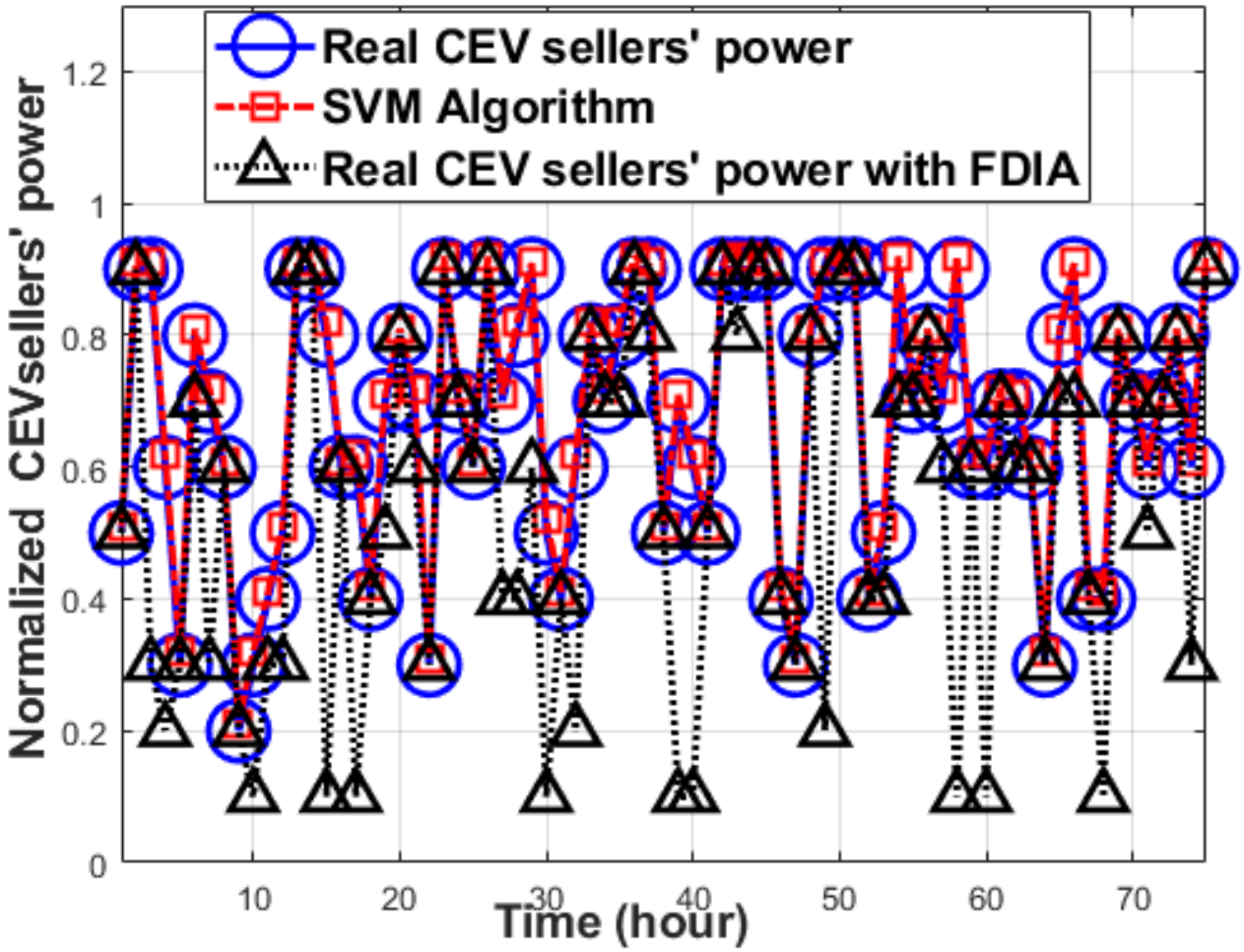

FIGURE 8. Cybersecurity vulnerabilities.

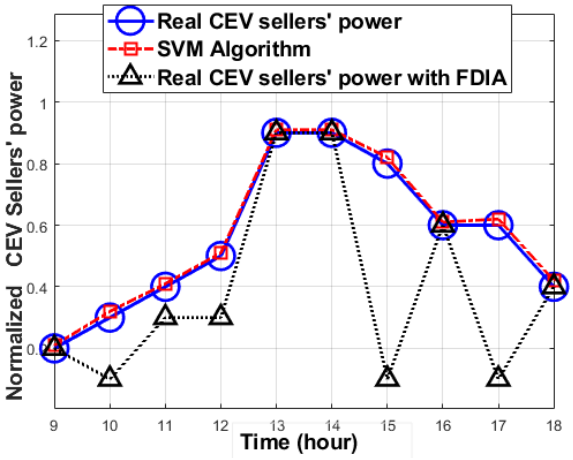

FIGURE 9. The normalized power exchanged between CEVs after FDIA during day time (from 9 AM to 6 PM).

We can conclude that our SVM Algorithm can improve the decentralized trading of the electricity provided by CEV sellers and buyers in parking lots by tackling cybersecurity issues when detecting FDIA and extracting the real values for the electricity price for selling or buying as well as the CEV electricity profile.

TABLE 3. Comparison between the buying and selling price with and without FDIA.

	Average value	Deviation %
Average real power with FDIA	0.39	
SVM ALgorithm	0.58	32

V. CONCLUSION

False data injection attacks are considered to be one of the most dangerous threats against ML and data driven technologies. Attackers can damage the whole system and degrade its performance by injecting malicious data in a training sequence set of the ML. This paper presents a cybersecurity scheme able to identify attacked sequence using our SVM Algorithm. Numerical results and simulations demonstrate the strength of the proposed algorithm to detect FDIA and extract the right values.

As a future works, this article can be extended for a large scale with realistic testbed considering the Denial of the Service (DoS) and ransomware/crypto-ransomware attacks.

REFERENCES

[1] D. Said, "A decentralized electricity trading framework (DETF) for connected EVs: A blockchain and machine learning for profit margin optimization," *IEEE Trans. Ind. Informat.*, vol. 17, no. 10, pp. 6594–6602, Oct. 2021, doi: 10.1109/TII.2020.3045011.

[2] L. Liu, M. Esmalifalak, Q. Ding, V. A. Emesih, and Z. Han, "Detecting false data injection attacks on power grid by sparse optimization," *IEEE Trans. Smart Grid*, vol. 5, no. 2, pp. 612–621, Mar. 2014, doi: 10.1109/TSG.2013.2284438.

[3] S. Zheng, T. Jiang, and J. S. Baras, "Robust state estimation under false data injection in distributed sensor networks," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, Dec. 2010, pp. 1–5, doi: 10.1109/GLOCOM.2010.5685223.

[4] C. Pei, Y. Xiao, W. Liang, and X. Han, "PMU placement protection against coordinated false data injection attacks in smart grid," *IEEE Trans. Ind. Appl.*, vol. 56, no. 4, pp. 4381–4393, Aug. 2020, doi: 10.1109/TIA.2020.2979793.

[5] B. Tang, J. Yan, S. Kay, and H. He, "Detection of false data injection attacks in smart grid under colored Gaussian noise," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Oct. 2016, pp. 172–179, doi: 10.1109/CNS.2016.7860483.

[6] K. Huang, Z. Xiang, W. Deng, C. Yang, and Z. Wang, "False data injection attacks detection in smart grid: A structural sparse matrix separation method," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 3, pp. 2545–2558, Jul. 2021, doi: 10.1109/TNSE.2021.3098738.

[7] J. Zhao and L. Mili, "Vulnerability of the largest normalized residual statistical test to leverage points," *IEEE Trans. Power Syst.*, vol. 33, no. 4, pp. 4643–4646, Jul. 2018.

[8] X. Liu, Y. Guan, and S. W. Kim, "Bayesian test for detecting false data injection in wireless relay networks," *IEEE Commun. Lett.*, vol. 22, no. 2, pp. 380–383, Feb. 2018.

[9] S. K. Singh, K. Khanna, R. Bose, B. K. Panigrahi, and A. Joshi, "Joint-transformation-based detection of false data injection attacks in smart grid," *IEEE Trans. Ind. Informat.*, vol. 14, no. 1, pp. 89–97, Jan. 2018, doi: 10.1109/TII.2017.2720726.

[10] D. Xue, X. Jing, and H. Liu, "Detection of false data injection attacks in smart grid utilizing ELM-based OCON framework," *IEEE Access*, vol. 7, pp. 31762–31773, 2019, doi: 10.1109/ACCESS.2019.2902910.

[11] A. Ayad, H. E. Z. Farag, A. Youssef, and E. F. El-Saadany, "Detection of false data injection attacks in smart grids using recurrent neural networks," in *Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. (ISGT)*, Feb. 2018, pp. 1–5, doi: 10.1109/ISGT.2018.8403355.

[12] H. Yang, X. He, Z. Wang, R. C. Qiu, and Q. Ai, "Blind false data injection attacks against state estimation based on matrix reconstruction," *IEEE Trans. Smart Grid*, early access, Apr. 5, 2022, doi: 10.1109/TSG.2022.3164874.

[13] A. Ahmadi, M. Nabipour, S. Taheri, B. Mohammadi-Ivatloo, and V. Vahidinasab, "A new false data injection attack detection model for cyberattack resilient energy forecasting," *IEEE Trans. Ind. Informat.*, early access, Feb. 15, 2022, doi: 10.1109/TII.2022.3151748.

[14] Z. Wang, G. Yuan, H. Pei, Y. Zhang, and X. Liu, "Unsupervised learning trajectory anomaly detection algorithm based on deep representation," *Int. J. Distrib. Sensor Netw.*, vol. 16, no. 12, Dec. 2020, Art. no. 155014772097150, doi: 10.1177/1550147720971504.

[15] D. Said, S. Cherkaoui, and L. Khoukhi, "Queuing model for EVs charging at public supply stations," in *Proc. 9th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jul. 2013, pp. 65–70, doi: 10.1109/IWCMC.2013.6583536.

[16] D. Said and H. T. Mouftah, "Novel communication protocol for the EV charging/discharging service based on VANETs," *IEEE Trans. Intell. Vehicles*, vol. 2, no. 1, pp. 25–37, Mar. 2017, doi: 10.1109/TIV.2017.2708604.

[17] S. Chaurasiya and B. Singh, "A 20 kW three phase off-board charging system with multiple outputs for wide variety of EVs," in *Proc. IEEE Int. Power Renew. Energy Conf. (IPRECON)*, Sep. 2021, pp. 1–6, doi: 10.1109/IPRECON52453.2021.9641049.

[18] V. M. Iyer, S. Gulur, G. Gohil, and S. Bhattacharya, "An approach towards extreme fast charging station power delivery for electric vehicles with partial power processing," *IEEE Trans. Ind. Electron.*, vol. 67, no. 10, pp. 8076–8087, Oct. 2020, doi: 10.1109/TIE.2019.2945264.

[19] A. Blinov, D. Zinchenko, J. Rabkowski, G. Wrona, and D. Vinnikov, "Quasi single-stage three-phase filterless converter for EV charging applications," *IEEE Open J. Power Electron.*, vol. 3, pp. 51–60, Dec. 2022, doi: 10.1109/OJPEL.2021.3134460.

[20] N. M. M. Mohamed, H. M. Sharaf, D. K. Ibrahim, and A. El'gharably, "Proposed ranked strategy for technical and economical enhancement of EVs charging with high penetration level," *IEEE Access*, vol. 10, pp. 44738–44755, 2022, doi: 10.1109/ACCESS.2022.3169342.

[21] S. U. Jeon, J.-W. Park, B.-K. Kang, and H.-J. Lee, "Study on battery charging strategy of electric vehicles considering battery capacity," *IEEE Access*, vol. 9, pp. 89757–89767, 2021, doi: 10.1109/ACCESS.2021.3090763.

[22] D. Said and H. T. Mouftah, "A novel electric vehicles charging/discharging management protocol based on queuing model," *IEEE Trans. Intell. Vehicles*, vol. 5, no. 1, pp. 100–111, Mar. 2020, doi: 10.1109/TIV.2019.2955370.

[23] E. Braco, I. S. Martín, A. Berrueta, P. Sanchis, and A. Ursúa, "Experimental assessment of first- and second-life electric vehicle batteries: Performance, capacity dispersion, and aging," *IEEE Trans. Ind. Appl.*, vol. 57, no. 4, pp. 4107–4117, Jul./Aug. 2021, doi: 10.1109/TIA.2021.3075180.

DHAOU SAID (Member, IEEE) received the Diploma degree in engineering and the master's (research) degree in electric engineering and communication systems from the National Engineering School of Tunis, the Ph.D. degree (Hons.) in electrical and computer engineering from the University of Sherbrooke, Canada, in December 2014, and the Doctorate Diploma degree in network and computer science from the University of Technology of Troyes (UTT), France, in December 2014. He worked with the University of Ottawa as a Postdoctoral Researcher, a Software Developer, the Manager, and a Mentor. His research interests include cybersecurity, cyber-attacks (DoS, FDI, ransomware, and crypto-ransomware), decentralized models, power technology, smart grid, smart mobility, Fintech, game theoretic, autonomous connected electric vehicle (ACEV), renewable energy, smart micro-grids, net-zero, photovoltaic system, cloud computing, VANET communications, the IoT, big data, AI, ML, blockchain solutions, sustainable energy, data management, and smart cities. He is the founder of three start-ups, such as Accord Micro-Grid Corporation (AMgC), in November 2018, Decentralization of Electricity, ITooMove, in November 2018, Smart Transportation Platform, and SCIBDM Inc., in January 2018: Smart Cities Innovation Business Development and Management. He proposed and is currently co-supervising two doctoral subjects with the University of Ottawa. The first one is targeting "the interactions of EV connected to modern electricity grids in smart cities." The second subject proposes a "Community mobility traffic model based on the combination of several forms of transport in smart cities, such as electric buses, shared vehicles, and shared bicycles."

MAYSSA ELLOUMI (Student Member, IEEE) is currently pursuing the master's degree in data science with the National School of Computer Science of Tunisia (ENSI). She is also a Computer Science Engineer with two years of pre-engineering studies with the Preparatory Institute for Engineering Studies of Sfax. Her research interests include data science, data analytics, and machine learning.

LYES KHOUKHI (Senior Member, IEEE) received the Ph.D. degree in electrical and computer engineering from the University of Sherbrooke, Canada, in 2006. From 2007 to 2008, he was a Postdoctoral Researcher with the Department of Computer Science and Operations Research, University of Montreal. He is currently a Full Professor with the ENSICAEN, Normandie University, GREYC CNRS. His current research interests include the field of cybersecurity, attacks detection, and performance evaluation in advanced networks, such as cloud networking, 5G/SDN, IoT/V2X, and CPS.