e-palli

AMERICAN JOURNAL OF SMART TECHNOLOGY AND SOLUTION (AJSTS)

VOLUME 1 ISSUE 1 (2022)

Indexed in

American Journal of Smart Technology and Solutions (AJSTS)
Volume 1 Issue 1, Year 2022
https://journals.e-palli.com/home/index.php/ajsts

New Obstacles to Smart City Cybersecurity

Abdullah Alsaeed[1*]

Article Information

Received: October 06, 2022

Accepted: October 29, 2022

Published: November 03, 2022

Keywords

Cyber-attack, Cybersecurity, False Data Injection (FDI) , Resilience, Smart City, Smart Grid

ABSTRACT

This article provides a concise description of the criteria that may be evaluated to determine the adoption of smart grid approaches that improve cybersecurity. It is necessary, from a functional point of view, to establish the degree to which cyber resilience may be increased by implementing solutions that are efficient in terms of cost. The problem of cybersecurity for smart grids has been the focus of several research and initiatives. In this study, the detection and diagnosis of False Data Injection (FDI) attacks are investigated in detail concerning their accuracy, processing time, and resilience to outside influences. No one method can be applied to all power systems. Therefore, a comparison and statistical analysis of the newly reported approaches for detecting and recognizing cyberattacks are conducted here.

INTRODUCTION

One of the many advantages of the current power city's technological design, which is often referred to as the "smart city" in certain circles, is that it allows for more efficient integration of renewable energy sources (RESs). However, due to the vast quantity of data that has to be sent for the system to function correctly, the smart city relies on an improved communication infrastructure to function properly (Aoufi *et al.*, 2020; Mohammadi *et al.*, 2019b; Mohammadi & Neagoe, 2020). As a result, cyber-attacks on smart city have increased. Invasions of a company's communication networks may drive up operating expenses dramatically (Nikmehr & Moghadam, 2019) or could impede the efficient functioning of the system (Q. Wang *et al* 2019). For example, cyber-attacks on Ukraine's power infrastructure in 2015 caused several hours of extensive power outages (Aoufi *et al.*, 2020).

Smart city operators must immediately identify, detect, and respond to such assaults to guarantee the system's integrity and correct functioning. This procedure is referred regarded as having cyber resilience as its defining characteristic. Correctly identifying cyberattacks is reportedly the first step in bolstering resilience throughout the attack and post-attack phases. This is the opinion of those who operate power systems. This is because the strike cannot be predicted with any degree of accuracy. As a consequence of this, several research activities have been carried out over the last decade to effectively detect and identify intrusions as a component of the cyber-resistance of the smart city (Biggio & Roli, 2018; Otuoze *et al.*, 2018; Sharafeev *et al.*, 2018; Q. Wang, W. Tai, Y. Tang, & M. Ni, 2019; Wang & Lu, 2013).

LITERATURE REVIEW

Numerous research projects have been conducted to verify the precision of cyberattack identification and detection, help accelerate processing, and boost resistance from external influence. Malicious meters might be detected more precisely using an AI-based approach, as described by (Khanna *et al.*, 2018). Using machine learning, a strategy was published by (D. Wang *et al.*, 2019) that might better recognize different types of power city disruptions and cyber-attacks. Reinforcement Learning (RL) was proposed to cope with diverse Partially Observable Markov Decision Process POMDPs (Kurt *et al.*, 2018).

Training the defender with low-magnitude assaults and decreasing an attacker's attacking space increased the strategy's robustness (Kurt *et al.*, 2018). A multivariate Gaussian-based model was described for power distribution system cyber-attack detection (An & Liu, 2019). The isolation forest technique was introduced by (Ahmed *et al.*, 2019) to detect hidden data integrity breaches in the smart city, which is an unsupervised approach. To further speed up the detection of the assault, the suggested solution used minimal complexity.

A randomized trees-based machine learning approach was presented to identify stealthy cyberattacks in the smart city successfully (Acosta *et al.*, 2020). In addition, the recommended approach was faster to compute and more resilient to noisy input than previous machine learning-based attack detection techniques.

The distinction between data manipulation alterations and physical city adjustments was made by (Mohammadpourfard *et al.*, 2020), enabling the attack detection system to work successfully even when ideas moved. The unsupervised False Data Injection (FDI) attack technique (Mohammadpourfard *et al.*, 2017) effectively-recognized attacks under various scenarios. It showed resistance to the integration and reconfiguration

[1] Department of Computer Science, University of Manchester, Saudi Arabia
[*] Corresponding author's e-mail: alsaeed.866@gmail.com

of renewable energy sources (RESs) into power networks. It was discovered by (Moslemi *et al.*, 2017) that one of the most effective ways to identify assaults on the smart city is to use the Maximum Likelihood (ML) estimate.

In addition, the suggested strategy reduced the computing load by minimizing the complexity of the ML estimation issue. (Li *et al.*, 2018) looked into an exact and quick approach in computing for detecting FDI assaults on smart city. Noise-free data was not a problem for the proposed method. As reported by (Hao *et al.*, 2016), the Markov Decision Process (MDP) technique was used to identify and evaluate the susceptibility of power city to cyberattacks in a dynamic setting. (Zhao *et al.*, 2018) They have shown their method's robustness for detecting FDI assaults in noisy environments.

The resilience of the smart city and its ability to withstand cyberattacks take up a substantial portion of the attention of this essay. The most common types of cyberattacks, known as FDI assaults, are discussed in this section. The most current research publications to be published are compared to one another and are expounded.

The components of the paper are detailed below. Second, the principles of cyber-attack detection and identification in the smart city are discussed in Section 2, while Section 3 focuses on current quantitative methodologies for cyber-attack detection and identification. This is followed by Section 4, which concludes the paper. Finally, in the fourth part, we will evaluate several strategies based on their resilience.

The Smart City Cyber-Attack Detection and Identification Fundamentals

As one of the new cyber-physical systems, the smart city is built on the physical power infrastructure, which includes power generation, distribution, and consumption systems, and the dense integration of communication infrastructure with specialized hierarchical control structures (Mohammadi *et al.*, 2019c; Ostadijafari *et al.*, 2019). The physical power infrastructure, which consists of power generation, consumption systems, distribution, and the dense integration of communication infrastructure with specialized hierarchical control structures, forms the foundation of the smart city, as one of the new cyber-physical systems. Communication systems usually comprise actuation devices and smart sensors at the local control level. However, these systems also incorporate smart controllers, smart meters, automation units, Phase Measurement Units (PMUs), and distributed generations at the higher control levels, such as cyber layers (Mohammadi *et al.*, 2019a).

They are susceptible to cyberattacks due to the smart city's extensive penetration of communication infrastructure, which has led to the proliferation of connected devices. Most threats to the systems that distribute power originate from unfriendly outsiders, malicious insiders, non-malicious insiders, and mother nature herself. Most of these dangers originate from smart homes and businesses outfitted with smart meters. Malicious agents are a risk because they can infect everyone with malware and viruses or zero in on specific computer systems to break into them, disrupt their operation, or cause damage to them.

The most prevalent types of cyber-attacks in the smart city are Denial of Service (DoS) and FDI (Nguyen *et al.*, 2020). Most denial-of-service attacks are geared toward interrupting the data transfer process by focusing their attention on the communication infrastructure. It's possible that scam data streams could be continuously flooded into the network or that synchronized data flooding would be used to target control signals (Nguyen *et al.*, 2020). In contrast to DoS assaults, FDI assaults often take the form of data packet manipulation, which may occur at varying degrees of severity (Nguyen *et al.*, 2020).

In addition, FDI attacks may be designed to target several data packets included inside communication protocols (Nguyen *et al.*, 2020). These data packets can consist of sensor/actuator software calibrations and protective relays, feedback signals and commands. As a result, the smart city might experience poor performance, instability, and even blackouts due to attacks by FDI (Liu *et al.*, 2019). It is necessary to quickly and accurately detect and identify any hostile cyber-attacks to improve the cybersecurity of smart city. As well as reducing computation cost and complexity, defensive measures must be implemented to strengthen or restore the system's resistance against cyberattacks. The inability to differentiate between regular system interruptions and dynamics, such as changes in command signals and cyberattacks, connection/disconnection of power generating units, load switching, are barriers to detecting cyberattacks. Regular system interruptions and dynamics include these things.

Enhanced control mechanisms and careful evaluation of the system model's nonlinear character are necessary to deal with the nonlinearities, uncertainties, and disruptions inherent in the system.

One way of determining deviations and abnormalities is to estimate the system states under normal operating conditions and then compare those estimates to the actual system states. The steady-state states of the system were calculated using a Weighted Least Square (WLS) estimator, and the results are shown in (Xu *et al.*, 2017). In (Sreenath *et al.*, 2017), an attempt was made to solve the problem of WLS's inability to converge on a solution. This led to the development of recursive WLS.

Dynamic estimating techniques are required to do a quick study on power systems. These methods must take into consideration the system's initial states. The Kalman Filtering (KF) method is widely used non-static estimation approach that incorporates a corrective term to reduce the number of errors caused by state estimation (Manandhar *et al.*, 2014). Extended Kalman Filtering (EKF), which considers the system's nonlinearities, was examined by (Abbaspour *et al.*, 2019; Chakhchoukh *et al.*, 2019) to detect FDI assaults. In all of these model-dependent detection strategies, inaccuracies in the models

progressively degrade their effectiveness and potentially result in false positives.

The actual execution of the solution becomes more challenging when recursive techniques and exact models are used since they increase the bar for the amount of computing power required to estimate the system's state accurately. Data-driven solutions have been created so that the difficulties connected with model-dependent detection approaches may be addressed. In general, the data-driven methodology may be classified into one of three groups: supervised learning techniques, unsupervised learning techniques, and semi-supervised learning techniques. Each input is mapped to its one-of-a-kind output in the algorithms that use labels derived from the labeled dataset.

It is usual practice to use supervised learning techniques where various ranges of cyber-attack simulations may be produced to obtain the necessary training dataset (Ayad *et al.*, 2018; Fenza *et al.*, 2019). As opposed to that, it is feasible to identify a meaningful pattern in unlabeled data by using algorithms that do not need supervision. However, using such approaches to identify cyberattacks is far less common than supervised algorithms. In addition, you should only utilize them when cyberattacks are not found in any of the obtained datasets (Zanetti *et al.*, 2017). Therefore, acquiring the same training datasets under various operating settings is vital, are valid for supervised and unsupervised learning strategies.

Since the efficiency of detection algorithms is wholly dependent on the datasets they collect, there is a high risk that these algorithms may become overfit. Consequently, the system has difficulty recognizing instances of cyberattacks that were not included in the training data set. A data-driven and model-based detection technique was studied in the paper (Sargolzaei *et al.*, 2019) as a potential solution to the problem that had been found before. In addition, strategies based on semi-supervised learning may be used when a trial-and-error method must be utilized to rectify or change the following control action following the input from the control actions that came before (Chen *et al.*, 2018).

The main challenges in the way of the development of cybersecurity for the smart city are the detection accuracy, the processing complexity, and the resistance to external influences. These challenges apply to both data-driven and model-based detection systems.

Methods for the Detection and Identification of Cyber Attacks

Data-Driven Procedures

To effectively identify cyberattacks on the smart city, data-driven technologies, such as machine learning techniques, have seen widespread application in recent years (Apruzzese *et al.*, 2019).In (Khanna *et al.*, 2018), it was suggested to use a supervised AI-based load estimator to compare anticipated loads with actual meter data to identify which meters are vulnerable to FDI assaults. As a direct result of the model's capability to identify FDI assaults, the cumulative error rate for state variables was just 1%. In order to get more precise results for calculating the tampering meters, an extra load estimator has been included in the current model.

Neural Networks (NN) and Artificial Neural Networks (ANN) with a single hidden layer and forward connections were proposed to achieve an appropriate learning rate. Because these networks were trained using historical data, the suggested estimator could identify an FDI assault, even if it came from a small number of compromised meters. This was made possible because these networks were used to train the estimator. In the event of a widespread FDI attack, our technique ensures the correct identification of both the attack and the tempered meters. (D. Wang *et al.*, 2019) outlines a supervised learning method that may detect cyberattacks on the smart city using previous data and log information. With an accuracy of 93.9 percent and a detection rate of 93.6 percent, the presented strategy is superior to other previously proposed techniques, such as the Random Forest (RF) method, and the K-Nearest Neighbors (KNN) algorithm. Both of these techniques have a detection rate of 93.6 percent. In (Kurt *et al.*, 2018), the RL approach was used for the first time to detect internet assaults on the smart city. This form of cyberattack was categorized as a POMDP since the attacker could compromise the legitimate states of the smart city, which the system operator would not have been able to tell was compromised in the first place. The solution shown by (Kurt *et al.*, 2018) does not involve using a model, as was mentioned, and it also took much less time to accomplish. A person who acts alone.

The RL technique, which was presented from the perspective of a system defender, proved effective in detecting low-magnitude assaults. As a consequence, the defense may observe tiny variations in the states of the smart city independent of the method the attacker is using. The model-free strategy suggested showed evidence of resistance to the unknown system states. FDI assaults in the cyber-physical system of a power distribution city were detected using a multivariate Gaussian-based technique (An & Liu, 2019). This method was applied. It is possible to differentiate between transient and persistent assaults by examining the measurement data produced by micro-PMUs.

Power distribution systems are divided into zones with comparable voltage profiles using the K-Means clustering technique. In order to account for this shift, fewer micro-power management units (PMUs) were used. The accuracy and precision that were shown were sufficient for the identification of transient assaults. However, the technique suggested to be used in continuous assaults was based on the imprecision of prediction, which the circumstances of a smart city may influence.

Enhancing regression models may lower the proportion of erroneous predictions and boost attack detection accuracy. According to the information in reference 14, the smart city is now targeted by a covert data integrity attack. A technique for feature extraction based on

principal component analysis (PCA) was used to make the issue more manageable, and high-dimensional data was transformed into low-dimensional space. The "isolation forest" method, which may detect irregularities in state estimation measurement characteristics, is based on unsupervised machine learning. It exhibited a better accuracy rate when comparing the suggested method to more conventional machine learning-based tactics.

A shorter processing time was needed to detect cyberattacks due to the technique's lower computational complexity. In (Acosta *et al.*, 2020), the smart city's state estimation-measurement capabilities were used to detect stealthy cyberattacks by applying supervised learning.

Large-scale power systems have a high dimensional space. Hence it was chosen to use a Kernel Principal Component Analysis (KPCA) approach to reduce the complexity of the problem occurring in the system and accurately represent the information in a lower-dimensional space. Furthermore, the properties of KPCA were used to demonstrate that the proposed method is reliable in the presence of imbalanced datasets. It was also able to detect cyberattacks on the smart city with a high degree of accuracy, despite taking less computer time than other machine learning-based methods, such as classic PCA. (Mohammadpourfard *et al.*, 2020) conducted research on the cybersecurity of smart city to evaluate the effect of concept drift, also known as the detection of physical changes that are the consequence of variations in smart city data manipulation. The efficiency of this technique in spotting malicious cyber activity was subjected to extensive testing and analysis. Another study presented (Mohammadpourfard *et al.*, 2017) a technique for detecting cyberattacks that consider the system's reconfiguration and incorporation of RES.

The F-Test was applied to distinguish between the regular and attacked state vectors. It was found that more investigation is necessary for the suspect samples that defy the F-premise testing. As a result, the comparison index utilized to evaluate failed samples was the difference between suspected vectors and the average from comparable system state vectors. This was accomplished with the assistance of three outlier detection algorithms, including, Interquartile Range (IQR), Median Absolute Deviation (MAD), and Fuzzy C-Means (FCM) clustering, methods. According to the results, the proposed method could detect FDI assaults with a high degree of accuracy while unaffected by changes in the parameters.

Estimation Methods for the State

Correct state estimates may assist in keeping the smart city safe and fully controlled (Yong *et al.*, 2016). On the other hand, state estimators are open to assault by FDI. Such attacks may defeat Bad Data Detection (BDD) techniques and modify the state estimate.(Moslemi *et al.*, 2017) presented an example of a decentralized method for discovering smart city attacks based on ML estimates. ML estimate was used to identify attacks since it could be transformed into a chordal embedding space. With the help of the Kron reduction of the Markov network of phase angles, the approach that was provided was able to segment the ML estimation problem into a number of distinct local ML estimation problems. The suggested method is decentralized, which provides utilities with more anonymity. By minimizing the size of the problem, the quantity of labor required to solve it is also reduced. Furthermore, due to the properties of the attack matrix, which is sparsely, and the measurement matrix, which has a low rank, the FDI attack detection problem may be reframed as a matrix separation problem (Li *et al.*, 2018). This is possible because of the similarities between the two matrices.

The modern methods for separating matrices, such as the the Double-Noise-Dual-Problem (DNDP)-ALM, Augmented Lagrangian Method (ALM), the Low-Rank Matrix Factorization (LRMF), and, suffer from the increase in the amount of time needed for computing and a reduction in the amount of accuracy achieved. To successfully solve this issue, a strategy named Go-Decomposition was studied. The suggested approach displayed adequate accuracy in separating FDI attacks compared to the LRMF method and approximately similar accuracy compared to the ALM and DNDP-ALM methods when the environment was free of background noise. Furthermore, the solution offered to the issue had a fair calculation time and could protect the smart city against assaults on a broad scale.

An MDP that was designed to simulate the attack strategy of the attackers was published by (Hao *et al.*, 2016). Research on the knowledge and scenarios linked to the smart city was carried out in two phases. First, in an MDP with a short time horizon, it is conceivable for adversaries to determine the current state of the intelligent city over a relatively short amount of time. After investigating the probabilities of an assault, the most effective method from the viewpoint of the aggressor was found. According to the findings of the vulnerability analysis, the suggested method is resilient against the parametric uncertainties present in an MDP situation and the operators' dispatch strategy. An operator-perspective technique for assessing the susceptibility of nonlinear state estimators to FDI assaults is presented in reference (Zhao *et al.*, 2018).

A reliable approach for recognizing FDI assaults was developed, including using a subset of safe PMU measurements to investigate the measurement's statistical consistency.

These security approaches, unaffected by abnormalities and render the system completely transparent, may be used to determine whether or not an FDI attack has occurred. A dependable Huber M-estimator was also used to accomplish accurate FDI assault detection. The suggested approach was unaffected by secure measurements and insufficient and noisy data. It was stated by (Deng *et al.*, 2018) that FDI attacks might be carried out against power distribution networks since the statuses of these networks could be expected based on the data on power flow.

According to the simulation's findings, the FDI attack can be carried out without being discovered by the BDD approaches if the attacker correctly anticipates one state of the system. FDI attacks on the electrical city have been investigated (Margossian *et al.*, 2019), operating on the assumption that the attackers had some understanding of the system. After that, the demonstration FDI attack on the partial city was carried out to show how undetected FDI attacks may be. A strategy based on state estimates was later developed to protect power city against assaults carried out in the name of foreign direct investment (FDI) that go unreported. The Basic Measurement Set is a mechanism that was developed by (Sreeram & Krishna, 2019) to protect the smart city against FDI assaults by securing n-1 meter in n-bus power systems. This solution was given the moniker "the Basic Measurement Set" (BMS). The approach was then altered to determine a subset of the optimum BMS to reduce the level of vulnerability shown by the system if less than n - 1 meter could be safeguarded.

Various Other Approaches

As was said before, the primary objective of cyberattacks is to influence the condition that is expected to be present in the smart city. Therefore, in addition to the data-driven methodology and the state estimation technique, other methodologies, such as Game Theory, have been utilized to analyze the vulnerability of the smart city to the possibility of cyberattacks (Apruzzese *et al.*, 2019; Biggio & Roli, 2018).

In (Q. Wang, W. Tai, Y. Tang, M. Ni, *et al.*, 2019), the features of FDI assaults, as seen from the attacker's viewpoint, were described to reveal the vulnerabilities present in current BDD approaches. After that, a two-layer defensive paradigm that included detection and protection strategies was presented from the defender's point of view. A zero-sum, static Game Theory was used to identify the most effective defensive and attacking tactics. It was found that the minimax-regret technique could be used to design a cost-effective defense that could be used against an assault that used load redistribution (Abusorrah *et al.*, 2017).

There was an effort made to spread the load, and the algorithm's goal was to reduce the amount of economic damage caused. Because the protective strategy of the smart city is susceptible to time-varying loading situations, it is necessary to develop an algorithm that can account for these fluctuations. A Game-Theoretic model was developed and tested to meet this need under various loading scenarios. Subsequently, a multi-level insolvable problem was transformed into a bi-level solvable optimization issue. A greedy implicit enumeration method was also utilized to identify the optimal global solution. In (Pilz *et al.*, 2020), an investigation was conducted into how the influence of FDI assaults on compromising anticipated demand data.

A model based on Game Theory was devised to assist utilities in awarding against these kinds of assaults, and the Nash equilibrium was uncovered. The best kind of monitoring for low-impact cyberattacks is none; nevertheless, for all other types of assaults, a range of defense techniques should be devised. Researchers from (Hasan *et al.*, 2020) looked at a cyberattack game in which the attacker and the defense were fighting against one another to see who would emerge victoriously. The attacker chose and targeted critical power substations to do the most damage possible to the system while staying within the allotted spending limit.

The vast majority of important power substations were taken simultaneously to reduce the amount of damage done to the system from the standpoint of the defense. We used polynomial-time algorithms to determine the worst possible dynamic assault that could be launched and the most effective defensive plan. The strategy given was more effective, less challenging, and capable of attacking a wider range of target systems than the best practices already in place. It was also more efficient and less complex than those practices.

In (Gao & Shi, 2020), a method based on dynamic game theory was presented to determine the level of vulnerability posed by cyber-physical systems. Furthermore, a mathematical programming model consisting of three groups a defender, an attacker, and a defender was investigated in the context of a system recovery delay and a distributed denial-of-service attack.

To overcome the challenge of optimization, a cutting-edge technique known as Particle Swarm Optimization (PSO) was used. The developed strategy proved to be quite successful when it came to finding susceptible transmission lines in power networks.

Detection and identification of cyberattacks; A comparison

The many methods of detecting and identifying cyber-attacks discussed in this research are compared in Table 1. For this comparison, we will use our resilience criteria for accuracy, computational load, and resistance to external variables.

Table 1: Methods of detecting and identifying cyber-attacks

Author	Objective	Method Proposed	Criteria For Adaptability and Resurgence		
			Accuracy	Complexity	External robustness
(Gao & Shi, 2020)	detection and analysis of cyber-attacks and vulnerabilities	Dynamic Game Theory	✓		

(Hasan *et al.*, 2020)	detection of cyber attacks	Game Theory	✓		
(Pilz *et al.*, 2020)	detection and identification of cyber attacks.	Game Theory	✓	✓	✓
(Abusorrah *et al.*, 2017)	detection of cyber-attacks	Game Theory based on the Minimax-Regret Method	✓		
(Q. Wang, W. Tai, Y. Tang, M. Ni, *et al.*, 2019)	Detection and identification of cyber-attacks.	Zero-sum Static Game Theory	✓	✓	
(Sreeram & Krishna, 2019)	detection and analysis of cyber-attacks and vulnerabilities	State Estimation	✓	✓	✓
(Margossian *et al.*, 2019)	detection and analysis of cyber-attacks and vulnerabilities	State Estimation Based on power flow analysis	✓		✓
(Deng *et al.*, 2018)	detection and analysis of cyber-attacks and vulnerabilities	State Estimation	✓		✓
(Zhao *et al.*, 2018)	Vulnerability and intrusion detection	Huber M-Estimator	✓	✓	
(Hao *et al.*, 2016)	Vulnerability and intrusion detection	Markov Decision Process-Based Method			✓
(Li *et al.*, 2018)	Detection of Internet-based cyberattacks	Go-Decomposition Algorithm		✓	✓
(Moslemi *et al.*, 2017)	detection of cyber-attacks	Gaussian Markov Random Field Method	✓	✓	✓
(Mohammadpourfard *et al.*, 2017)	detection and identification of cyber-attacks.	Unsupervised Learning Algorithm	✓		✓
(Mohammadpourfard *et al.*, 2020)	detection of cyber-attacks	Isolation Forest Method	✓	✓	
(Acosta *et al.*, 2020)	detection of cyber attacks	KPCA-Based Method	✓		
(Acosta *et al.*, 2020)	detection of cyber attacks	Isolation Forest PCA-Based Method	✓		
(An & Liu, 2019)	detection of cyber attacks	Multivariate Gaussian-Based Method	✓	✓	✓
(Kurt *et al.*, 2018)	Detection of Internet-based cyberattacks	Reinforcement Learning-Based Algorithm	✓		✓
(D. Wang *et al.*, 2019)	Detection and identification of cyber-attacks.	Supervised Learning Algorithm	✓	✓	
(Khanna *et al.*, 2018)	Identification of Malicious Meters	AI-Based Algorithm	✓		

Recent research, as seen in this table, has emphasized precision as a primary priority. However, accuracy remains a significant barrier to adopting data-driven solutions in the energy industry. In most cases, the computational burden may be lowered by using more potent processors and computing methods, such as parallel or distributed computing, which incur costs. In addition, ensuring safe operations may incur an unwanted but unavoidable cost due to the computational burden.

There is also a great deal of literature about resilience. In several recent studies, the degree to which the smart city's security is enhanced remains unclear. According to Table 1 of the operational aims, detecting and identifying online cyberattacks should be the most significant. Due to the unexpected behavior of renewable energy sources, energy management systems are plagued by high uncertainty and stochasticity.

Smart meters and PMUs with IoT capabilities might

provide fraudsters with various attack surfaces. Finally, controlling and regulating smart city is made more difficult by the need for quick detection and diagnosis of cyberattacks. The application of AI models in dealing with small datasets for training and testing, as well as the complex behavior of attacker and defender models, is demonstrated by the fact that game theory and RL models fit all three criteria. These cutting-edge technologies for cyberattack detection in power city may be helpful in the future.

CONCLUSION

At the beginning of this article, we discussed improvements to the smart city's overall level of cybersecurity. Recent academic research has focused on investigating ways to defend the smart city from intrusions by digital hackers. The accuracy, computing complexity, and resistance to external influences of FDI attack detection and identification have been the focus of further research in this study. In addition, this study has looked at the resilience of FDI assaults. All of the criteria mentioned in this study can be quantified, enabling operators of the system to assess the degree to which the implementation of practical financial solutions may improve the system's resilience.

ACKNOWLEDGEMENT

The author is thankful to the University of Manchester, Saudi Arabia, for the continuous support of this research study.

Funding

No funding sources are reported.

Conflict of interest

The author does not have any conflict of interest.

REFERENCES

Abbaspour, A., Sargolzaei, A., Forouzannezhad, P., Yen, K. K., & Sarwat, A. I. (2019). Resilient control design for load frequency control system under false data injection attacks. *IEEE Transactions on Industrial Electronics, 67*(9), 7951-7962.

Abusorrah, A., Alabdulwahab, A., Li, Z., & Shahidehpour, M. (2017). Minimax-regret robust defensive strategy against false data injection attacks. *IEEE Transactions on Smart Grid, 10*(2), 2068-2079.

Acosta, M. R. C., Ahmed, S., Garcia, C. E., & Koo, I. (2020). Extremely randomized trees-based scheme for stealthy cyber-attack detection in smart grid networks. *IEEE Access, 8*, 19921-19933.

Ahmed, S., Lee, Y., Hyun, S.-H., & Koo, I. (2019). Unsupervised machine learning-based detection of covert data integrity assault in smart grid networks utilizing isolation forest. *IEEE Transactions on Information Forensics and Security, 14*(10), 2765-2777.

An, Y., & Liu, D. (2019). Multivariate Gaussian-based false data detection against cyber-attacks. *IEEE Access, 7,* 119804-119812.

Aoufi, S., Derhab, A., & Guerroumi, M. (2020). Survey of false data injection in smart power grid: Attacks, countermeasures and challenges. *Journal of Information Security and Applications, 54*, 102518.

Apruzzese, G., Colajanni, M., Ferretti, L., & Marchetti, M. (2019). Addressing adversarial attacks against security systems based on machine learning. 2019 *11th international conference on cyber conflict (CyCon).*

Ayad, A., Farag, H. E., Youssef, A., & El-Saadany, E. F. (2018). Detection of false data injection attacks in smart grids using recurrent neural networks. 2018 *IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT).*

Biggio, B., & Roli, F. (2018). Wild patterns: Ten years after the rise of adversarial machine learning. *Pattern Recognition, 84*, 317-331.

Chakhchoukh, Y., Lei, H., & Johnson, B. K. (2019). Diagnosis of outliers and cyber attacks in dynamic PMU-based power state estimation. *IEEE Transactions on Power Systems, 35*(2), 1188-1197.

Chen, Y., Huang, S., Liu, F., Wang, Z., & Sun, X. (2018). Evaluation of reinforcement learning-based false data injection attack to automatic voltage control. *IEEE Transactions on Smart Grid, 10*(2), 2158-2169.

Deng, R., Zhuang, P., & Liang, H. (2018). False data injection attacks against state estimation in power distribution systems. *IEEE Transactions on Smart Grid, 10*(3), 2871-2881.

Fenza, G., Gallo, M., & Loia, V. (2019). Drift-aware methodology for anomaly detection in smart grid. *IEEE Access, 7,* 9645-9657.

Gao, B., & Shi, L. (2020). Modeling an attack-mitigation dynamic game-theoretic scheme for security vulnerability analysis in a cyber-physical power system. *IEEE Access, 8*, 30322-30331.

Hao, Y., Wang, M., & Chow, J. H. (2016). Likelihood analysis of cyber data attacks to power systems with Markov decision processes. *IEEE Transactions on Smart Grid, 9*(4), 3191-3202.

Hasan, S., Dubey, A., Karsai, G., & Koutsoukos, X. (2020). A game-theoretic approach for power systems defense against dynamic cyber-attacks. *International Journal of Electrical Power & Energy Systems, 115,* 105432.

Khanna, K., Panigrahi, B. K., & Joshi, A. (2018). AI-based approach<? show [AQ="" ID=" Q1]"?> to identify compromised meters in data integrity attacks on smart grid. *IET Generation, Transmission & Distribution, 12*(5), 1052-1066.

Kurt, M. N., Ogundijo, O., Li, C., & Wang, X. (2018). Online cyber-attack detection in smart grid: A reinforcement learning approach. *IEEE Transactions on Smart Grid, 10*(5), 5174-5185.

Li, B., Ding, T., Huang, C., Zhao, J., Yang, Y., & Chen, Y. (2018). Detecting false data injection attacks against power system state estimation with fast go-decomposition approach. *IEEE Transactions on Industrial Informatics, 15*(5), 2892-2904.

Liu, C., Liang, H., Chen, T., Wu, J., & Long, C. (2019). Joint admittance perturbation and meter protection for mitigating stealthy FDI attacks against power system state estimation. *IEEE Transactions on Power Systems, 35*(2), 1468-1478.

Manandhar, K., Cao, X., Hu, F., & Liu, Y. (2014). Detection of faults and attacks including false data injection attack in smart grid using Kalman filter. *IEEE transactions on control of network systems, 1*(4), 370-379.

Margossian, H., Sayed, M. A., Fawaz, W., & Nakad, Z. (2019). Partial grid false data injection attacks against state estimation. *International Journal of Electrical Power & Energy Systems, 110*, 623-629.

Mohammadi, F., Nazri, G.-A., & Saif, M. (2019a). A bidirectional power charging control strategy for plug-in hybrid electric vehicles. *Sustainability, 11*(16), 4317.

Mohammadi, F., Nazri, G.-A., & Saif, M. (2019b). A fast fault detection and identification approach in power distribution systems. 2019 *International Conference on Power Generation Systems and Renewable Energy Technologies (PGSRET).*

Mohammadi, F., Nazri, G.-A., & Saif, M. (2019c). A real-time cloud-based intelligent car parking system for smart cities. 2019 *IEEE 2nd International Conference on Information Communication and Signal Processing (ICICSP).*

Mohammadi, F., & Neagoe, M. (2020). Emerging issues and challenges with the integration of solar power plants into power systems. In *Solar Energy Conversion in Communities* (pp. 157-173). Springer.

Mohammadpourfard, M., Sami, A., & Weng, Y. (2017). Identification of false data injection attacks with considering the impact of wind generation and topology reconfigurations. *IEEE Transactions on Sustainable Energy, 9*(3), 1349-1364.

Mohammadpourfard, M., Weng, Y., Pechenizkiy, M., Tajdinian, M., & Mohammadi-Ivatloo, B. (2020). Ensuring cybersecurity of smart grid against data integrity attacks under concept drift. International Journal of Electrical Power & Energy Systems, 119, 105947.

Moslemi, R., Mesbahi, A., & Velni, J. M. (2017). A fast, decentralized covariance selection-based approach to detect cyber attacks in smart grids. *IEEE Transactions on Smart Grid, 9*(5), 4930-4941.

Nguyen, T., Wang, S., Alhazmi, M., Nazemi, M., Estebsari, A., & Dehghanian, P. (2020). Electric power grid resilience to cyber adversaries: State of the art. *IEEE Access, 8*, 87592-87608.

Nikmehr, N., & Moghadam, S. M. (2019). Game-theoretic cybersecurity analysis for false data injection attack on networked microgrids. *IET Cyper-Phys. Syst.: Theory & Appl., 4*(4), 365-373.

Ostadijafari, M., Jha, R. R., & Dubey, A. (2019). Conservation voltage reduction by coordinating legacy devices, smart inverters and battery. 2019 *North American Power Symposium (NAPS).*

Otuoze, A. O., Mustafa, M. W., & Larik, R. M. (2018). Smart grids security challenges: Classification by sources of threats. *Journal of Electrical Systems and Information Technology, 5*(3), 468-483.

Pilz, M., Naeini, F. B., Grammont, K., Smagghe, C., Davis, M., Nebel, J.-C., Al-Fagih, L., & Pfluegel, E. (2020). Security attacks on smart grid scheduling and their defences: a game-theoretic approach. *International Journal of Information Security, 19*(4), 427-443.

Sargolzaei, A., Yazdani, K., Abbaspour, A., Crane III, C. D., & Dixon, W. E. (2019). Detection and mitigation of false data injection attacks in networked control systems. *IEEE Transactions on Industrial Informatics, 16*(6), 4281-4292.

Sharafeev, T., Ju, O. V., & Kulikov, A. (2018). Cyber-security problems in smart grid cyber attacks detecting methods and modelling attack scenarios on electric power systems. 2018 *International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM).*

Sreenath, J., Meghwani, A., Chakrabarti, S., Rajawat, K., & Srivastava, S. (2017). A recursive state estimation approach to mitigate false data injection attacks in power systems. 2017 *IEEE Power & Energy Society General Meeting.*

Sreeram, T., & Krishna, S. (2019). Managing false data injection attacks during contingency of secured meters. *IEEE Transactions on Smart Grid, 10*(6), 6945-6953.

Wang, D., Wang, X., Zhang, Y., & Jin, L. (2019). Detection of power grid disturbances and cyber-attacks based on machine learning. *Journal of Information Security and Applications, 46*, 42-52.

Wang, Q., Tai, W., Tang, Y., & Ni, M. (2019). Review of the false data injection attack against the cyber-physical power system. *IET Cyber-Physical Systems: Theory & Applications, 4*(2), 101-107.

Wang, Q., Tai, W., Tang, Y., Ni, M., & You, S. (2019). A two-layer game theoretical attack-defense model for a false data injection attack against power systems. *International Journal of Electrical Power & Energy Systems, 104*, 169-177.

Wang, W., & Lu, Z. (2013). Cyber security in the smart grid: Survey and challenges. *Computer networks, 57*(5), 1344-1371.

Xu, R., Wang, R., Guan, Z., Wu, L., Wu, J., & Du, X. (2017). Achieving efficient detection against false data injection attacks in smart grid. *IEEE Access, 5*, 13787-13798.

Yong, S. Z., Foo, M. Q., & Frazzoli, E. (2016). Robust and resilient estimation for cyber-physical systems under adversarial attacks. 2016 *American Control Conference (ACC).*

Zanetti, M., Jamhour, E., Pellenz, M., Penna, M., Zambenedetti, V., & Chueiri, I. (2017). A tunable fraud detection system for advanced metering infrastructure using short-lived patterns. *IEEE Transactions on Smart Grid, 10*(1), 830-840.

Zhao, J., Mili, L., & Wang, M. (2018). A generalized false data injection attacks against power system nonlinear state estimator and countermeasures. *IEEE Transactions on Power Systems, 33*(5), 4868-4877.